Knowledge Design in the Internet of Things: Blockchain and Connected Refrigerator

Samuel Szoniecky and Amri Toumia
Paragraphe Laboratory, University Paris VIII, 2 Rue de la Liberté, 93526 Saint-Denis, France

Keywords: Blockchain, Internet of Things, Power to Act, Modeling, Knowledge.

Abstract: The Internet of Things takes place in our daily life, but many users do not understand their relationships and interactions with these objects. We assume that dynamic and interactive representations of the power of action of users and objects are means to better understand what these devices are capable of. To do this, we design a secure and privacy-conscious design of knowledge in the connected object environment. We will analyze the example of a connected refrigerator to understand how to use the Blockchain to develop Digital Social Innovations.

1 INTRODUCTION

The Internet of Things (IoT) is witnessing a fast growth for few years now. A study done by the IDC consulting firm estimates that, by 2022, investments on the IoT sector should reach 1.200 billion dollars by 2022[1].

Economists consider these technologies as a new "growth driver" as long as the constraints that are preventing users from taking part in the IoT are solved. A French study done by Promotelec[2] reveals that these constraints are due to users' lack of trust in these technologies. Users wonder if they are harmful for the health and dangerous to vulnerable individuals (children, elderly people)and if they preserve the confidentiality of the collected data.

Beyond this desire to preserve the familiar space, interviewed users also question the simplicity of use, cost and usefulness. This last point is particularly important to us because the question of the usefulness of a digital device is undoubtedly the first question that should be asked because it places the individuals in a reflexive approach in relation to their own practices: do I need this product? This attitude of questioning is with no doubt the guarantee of a reasonable use of technologies (Lévy, 2017) (Citton, 2014) which counterbalances the fashion effects or the consumerist tendencies of our societies. But, how to evaluate the usefulness of a device like a connected refrigerator?

Manufacturers of connected refrigerators advertise devices capable of automatically recognizing food expiry date, reordering missing groceries and evaluating food compositions and their impact on consumers' health. However, the usefulness of these features is not obvious to all users. For example, automatically ordering food depends on the balance of the user's account or on the blood tests of the people in the household which conditions favoring one food over another. To be really useful, the refrigerator should continuously be aware of the users financial and serological state in order to adapt in real time to the changes of situations. Will we consent to give this information to a machine? How can we control the sharing of this information? Which responsibilities are we willing to give to algorithms?

The answers to these questions are not unique because each person can answer them differently and because the answers can vary depending on contexts. So, to answer the question of the usefulness of a connected refrigerator or any other smart object, we need to find ways to handle the different questions that arise from their use and their various possible answers, all this while ensuring the security of collected data and user privacy. Moreover, it is necessary that this data is interoperable and above all intelligible so that the experience of some benefits to the understanding of others.

From this perspective, it becomes fundamental to

[1] https://start.lesechos.fr/actu-entreprises/technologie-digital/comprendre-l-internet-des-objets-iot-en-5-questions-12253.php

[2] https://www.promotelec.com/wp-content/uploads/2018/06/Etude-Objets-connect%C3%A9s-pour-lhabitat-PROMOTELEC-21-juin.-pptx.pdf

Szoniecky, S. and Toumia, A.
Knowledge Design in the Internet of Things: Blockchain and Connected Refrigerator.
DOI: 10.5220/0007751703990407
In *Proceedings of the 4th International Conference on Internet of Things, Big Data and Security (IoTBDS 2019)*, pages 399-407
ISBN: 978-989-758-369-8

design knowledge management processes to measure interactions between humans and connected objects in order to evaluate the relationships between these two types of actors. The objective is to provide clear information about what these actors can do and for which purposes. To do this, we can model the power of action of these actors (Brun, 2017) to analyze how their interactions in a given situation and for a specific purpose, increases or decreases their power to act. Our hypothesis is that dynamic and interactive representations of this power to act are a way to better understand the capabilities of IoT devices: what are the offered services? Which difficulties can be encountered? What are the relationships between different objects? The main issue then becomes a question of knowledge design: how to manage the interactions between the knowledge of users and those of connected objects in a digital environment?

Alongside these knowledge management issues, the centralized architecture of IoT platforms raises many issues in terms of security and privacy protection. Due to its decentralized and distributed nature, Blockchain technology seems to address these issues (De Filippi, 2018). However, the characteristics of the IoT devices, for example their limited computing power, do not facilitate this adaptation. Similarly,understanding the complex mechanisms involved in the Blockchain makes this technology difficult to master for non-specialist users.

To illustrate and clarify how to conceive a secured knowledge design that respects users' privacy in the context of smart devices, we will begin by examining the Blockchain and its related technologies. In particular, we will focus on ”smart contracts” which give us a glimpse on a new way of contracting without a need for a trusted third party. In a second step, we will describe how to use the Blockchain in the IoT through the example of a dynamic and interactive device for collectively analyzing activities related to a connected refrigerator. Finally, we will discuss the advantages and drawbacks of this type of system.

2 WHAT IS THE Blockchain

In 2008, Satoshi Nakamoto (pseudonym) published a paper on Bitcoin (Nakamoto, 2008). In this article, the author describes a new cryptocurrency called Bitcoin. The latter is based on a technology called Blockchain. It is a public distributed and decentralized ledger in which transactions are recorded across multiple nodes of a peer-to-peer (P2P) network. The Blockchain is attack resistant, ubiquitous, verifiable and auditable.

To transfer virtual currency, Blockchain users, who are identified by their public keys,generate and broadcast transactions on the network. These transactions are grouped into blocks by users. When a block is filled, it is added to the Blockchain after a ”mining” process. To mine a block, nodes of the network, called ”miners”, try to solve a cryptographic puzzle called ”Proof-of-Work” (PoW). Once the block is validated, it is time stamped and added to the Blockchain. The transaction is then visible to the receiver as well as to the entire network (Saleh et al., 2018).

Since the invention of Bitcoin, other consensus mechanisms beside PoW have emerged. For example, we can talk about Proof-of-Stake (PoS) or Proof-of-Importance (PoI). In the first one, users who have more coins have the responsibility of validating transactions and protecting the system because they are the ones who invested the most in it and are therefore the most concerned about its good performance. Proof-of-Importance was introduced by NEM (Capstone, 2015). In this consensus mechanism, a reputation system is built for the network, based on an importance value associated with each account. The higher this value is, the greater the chance of being chosen to create the next block.

Based on the work of (Febin, 2018) (Shermin, 2017), we can distinguish three main types of Blockchain :

- Public Blockchain: as its name suggests, it is a large public ledger. No entity is in charge and all nodes of the network can read data from the Blockchain, participate in transaction validations and auditing. Having a computer with an internet connection in enough to become a node of the network and get a complete history of the Blockchain. The advantages of this system are transparency and anonymity, since each node is only identified by its public key. In addition, the redundancy of the public Blockchain and its replication over the network makes it very secure and immutable. However, transaction validations are slow and require significant computation power. This type of Blockchain is mainly used for cryptocurrencies such as Bitcoin or Ethereum.
- Private Blockchain: It is a kind of restricted Blockchain. It is under the management of an authority that oversees the creation, verification and validation of each transaction. The data is not open to the public and permissions are required to access it. Because of their nature, private Blockchains do not provide decentralized security, but offer increased efficiency for checking and validating transactions. Their use is destined for public or private companies.

- Consortium Blockchain or Public Blockchain with permission: It is a hybrid between public and private Blockchains. It operates under the supervision of a set of predetermined nodes that are allowed to verify and validate blocks or transactions. On the other hand, the data may be open to the public or restricted in the case of sensitive information. It is up to the nodes to choose this in advance. R3[3] and Energy Web Foundation[4] are examples of this type of Blockchain.

Given that the source code of Bitcoin is open source, many forks were possible and many new versions of peer-to-peer cryptocurrencies have emerged. However, the underlying protocol of Bitcoin, specifically the Blockchain technology, has attracted many new ideas. Researchers have been thinking of ways to use this decentralized distributed ledger for purposes other than virtual currencies. Thus, Blockchain got involved in any type of transaction or agreement between parties that previously required a trusted third party to regulate it.

In this context, Blockchain platforms, such as the Ethereum[5] , allow developers to create and execute ”smart contracts” within the Blockchain architecture.

The term ”smart contract” was introduced for the first time in 1994 by Nick Szabo (Szabo, 1994) as ” computerized transaction protocols that executes the terms of a contract ” . He gave the example of a vending machine through which a user could enter data or value and, in return, receive an item from that machine. While enforcing a standard contract is usually insured through laws and a trusted third party that guarantees its implementation (the State for example), enforcing and implementing a smart contract is done by an algorithm that is encrypted and added to the Blockchain. This smart contract can be automatically applied or executed taking into account a set of predefined conditions.

According to Gavin Wood (Wood, 2016) , cofounder of Ethereum, smart contracts have the following characteristics:

- Atomicity: the entire code of the contract must be executed or nothing is executed.
- Synchrony: operations cannot interfere with each other.
- Provenance: all messages can be inspected to determine the caller’s address.
- Permanence: the data of a contract are permanent.
- Immortality: a contract cannot be removed from the outside
- Immutability: the smart contract code cannot be changed.

Ethereum, introduced by Vatalik Buterin in 2013, is an example of a Blockchain platform specifically designed for the creation and application of smart contracts. Like Bitcoin, Ethereum is a public Blockchain network. While Bitcoin is designed for use cases involving transfer of virtual currency, Ethereum allows developers to create and deploy other decentralized applications based on Blockchain technology (Buterin, 2014). In Ethereum, miners work for a currency called Ether. That is what incentivize developers to write quality applications and ensure that the network works effectively. Thus, Ether, in addition to being an exchangeable cryptocurrency, is like the fuel that allows decentralized applications to run.

> *Contracts in Ethereum should not be seen as something that should be ”fulfilled” or ”complied with”; rather, they are more like ”autonomous agents” that live inside the Ethereum execution environment, always executing a specific piece of code when ”poked” by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables.* (Tsui, 2016)

Thus, from this definition we can understand that smart contracts are executed, as designed by their developers, when certain conditions are met, and without any human intervention. They are powered by the Ethereum Virtual Machine (EVM) and Ether.

According to Ethereum’s yellow paper (Wood, 2015) , the EVM is a quasi-complete Turing machine. Indeed, a Turing machine normally has infinite resources, while the EVM’s resources are deliberately limited. The qualification of ”quasi-complete” comes from the fact that the calculation is intrinsically linked to an amount of Ether allocated at the time of creation of a transaction, which limits the total amount of calculation that can be performed. This can be considered as equivalent to a fee. On the Ethereum network, each transaction requires the payment of an execution fee. To be able to program smart contracts, developers rely on ”Solidity”, the Ethereum programming language that is similar to Javascript.

[3] https://www.r3.com/
[4] http://energyweb.org/
[5] https://www.ethereum.org/

3 THE Blockchain IN THE IoT

The Internet of Things, or IoT, is a system of interconnected devices, sensors and digital machines that can communicate and share data over a network without the need for human intervention(Saleh, 2017). According to Gartner (Pettey, 2015), the number of smart devices connected to the Internet is expected to reach about 25 billion by 2020, generating an economic profit of 200 billion dollars.

Because of the generation of massive amounts of personal data, the IoT is facing issues such as the administration of these smart objects, safety and traceability , but also privacy protection and data access management...

Due to its distributed nature, its consensus mechanisms that reconcile divergent interests, and its distributed trust process that does not require third parties, the Blockchain can provide answers to these issues.

In their article (Atlam et al., 2018), Atlam et al. defend the idea that the shift of the IoT architecture toward a decentralized system could be a way to solve many problems, especially in terms of security. In addition, Brody et al. (Brody and Pureswaran, 2014) argue that in order to be profitable and sustainable, the ever-growing ecosystem of IoT devices should evolve into a decentralized architecture, reducing maintenance costs for manufacturers and increasing user trust in those products.

However, as mentioned by Dorri et al. (Dorri et al., 2016) , adapting Blockchain mechanisms to the IoT is not straightforward. In fact, the mining process requires a lot of computing power that IoT devices do not have. Moreover, it is a relatively slow process, while IoT applications require low latency. In addition, the Blockchain has scale-up problems and performance decreases as the number of nodes on the network increases, which may be problematic for IoT networks that involve a large number of devices interacting with one another. Finally, the underlying protocols of the Blockchain generate significant indirect traffic which may be undesirable for some IoT devices with limited bandwidth.

In this context, a lot of research is being done on how to use and adapt the Blockchain to the IoT environment. For example, we can cite Mettler (Mettler, 2016), who applied Blockchain in healthcare environment, whether for public health management, for medical research based on the personal information of patients or for quality insurance in medicine manufacturing. Dorri et al. (Dorri et al., 2017) presented an adaptation of the Blockchain to the case of smart homes. In their article, they show that it is possible to reduce the load on the network while ensuring data security and protection of users' privacy by grouping devices in clusters and using local Blockchain. In addition, Christidis et al. (Christidis and Devetsikiotis, 2016) demonstrated the benefits of Blockchain and smart contracts for sharing services or resources, as well as for task automation and verification. In (Huh et al., 2017) , Huh et al. showed a method to manage IoT devices using Ethereum. Using smart contracts and Ethereum accounts, an electricity meter was continuously sending electricity consumption to a smartphone, which in turn was sending instructions to a light bulb and an air conditioner to update their energy consumption modes. Finally, the authors of (Özyılmaz and Yurdakul, 2017) proposed a concept to facilitate Blockchain use for resource-limited IoT devices.

4 KNOWLEDGE DESIGN SYSTEM FOR A CONNECTED REFRIGERATOR

To understand and analyze the use of the Blockchain in the IoT, let us study the use of a connected refrigerator in a family of three people. To conduct this study, we use an activity modeling method based on an ecosystem approach that sees activity as a correlation between existence modeling (ontology) and knowledge experimentation (ethology). We adopt a global and evolving vision to analyze information-communication issues through the analogy of ecosystems in order to take advantage of an approach that includes the complexity of life in a field often analyzed with fixed models derived from engineering sciences. Following this analogical grid, we consider that the analysis of the activity goes through a double modeling, that of the existences which populate the ecosystems and that of the cognitive experiments that these existences maintain with each other.

To facilitate the modeling and make it accessible to as many people as possible, we propose to do this work using a graphic vocabulary that brings into play an analogy that is both simple and complex to give the user the means to invest already acquired knowledge and thus more easily understand the functioning of the device. The desktop analogy used by computer operating systems is a good example of a graphical vocabulary. However, in the case of the IoT, it is unsuitable for a context that we call an ecosystem (Roxin and Bouchereau, 2017). That is, an environment where a multitude of human and algorithmic actors evolve continuously in what they are, what they know and the relationships they have with each other.

Let us take the example of a connected refrigerator that has an automatic food inventory management feature which meets the needs and desires of family members. To implement this functionality with a desktop analogy, users should be asked to fill in ”lists” corresponding to their needs and desires, in ”folders” through ”forms” that will be sent to food suppliers and other companies that can access this data. In this case, the interactions with the refrigerator are similar to those of an ”accountant” and the story that the users co-construct with the connected object becomes only ”administrative”. Now, imagine the same refrigerator with the same functionality, but this time by setting up the analogy of the garden. In this case, the user is no longer facing lists, but gardening ”plants” that grow and play with ”animals” that interact with them. The user becomes a ”gardener” and ”cultivates” a living story with the digital environment to make a knowledge ecosystem their own.

4.1 Principles of Modeling Knowledge Ecosystems

The basic principles of modeling knowledge ecosystems (Szoniecky and Safin, 2017) are based on the description of the existences that compose them. They are defined by four distinct existential dimensions: physical, concept, actor, relation. These dimensions give the modeler an analytical grid to organize the chaos of ecosystems by distinguishing elements each possessing their own kind of knowledge accessible according to a dedicated metric:

- physical dimension = Euclidean metric ⇒ knowledge of shocks
- concept dimension = topological metric ⇒ experimentations of intuitions
- actor dimension = topographic metric ⇒ social knowledge
- relation dimension = temporal metric ⇒ pragmatic knowledge.

The diagram in figure 1 illustrates the organization of modeling by enriching it with a double translation. First, to each dimension is associated a pretopological element useful to formalize the informational transformations of the ecosystem:

- physical = outside,
- concept = interior,
- actor = edge,
- relation = stream.

Second, the dimensions of existence are translated according to the analogy of a plant:

- physical = branch,
- concept = root,
- actor = seed,
- relation = sap.

It is from this analog translation that we propose a dynamic and interactive representation of the power to act in the form of a semantic mapping that we define as dynamic and interactive interfaces composed of:

- a conceptual coordinate system to formalize an interoperable expression
- a projection of concepts in a graphic vocabulary to visualize expressions
- devices for interacting with the user (click, drag & drop, gesture capture, etc.) to manipulate expressions

This cartography takes as graphic vocabularies those of geographical cartography, housing plans or any other graphic forms like stars, icons, drawings, diagrams, etc. What matters is the ability of the mapping to make explicit the interactions of the users with the graphical vocabulary and the projection of these interactions in four coordinate systems:

- material spaces
- conceptual spaces
- networks of actors
- temporalities.

Passing through these coordinate systems allows to formalize the expression making it interoperable with other expressions. Thus the interpretation goes through the positioning of the user in these four coordinate systems. Positions that can be automatically calculated for example in the material space thanks to the GPS or in temporality thanks to the synchronization of the world clocks. On the other hand, positions in the network of actors and in the conceptual spaces require interactions with the user.

4.2 Modeling the Ecosystem of a Connected Refrigerator

To illustrate the use of this modeling method in the field of the IoT, here is the modeling of activities related to the use of a connected refrigerator. This diagram in figure 2 shows how Blockchain technologies are used to manage three types of activity. The first is a ”transfer of assets” corresponding to the purchase of

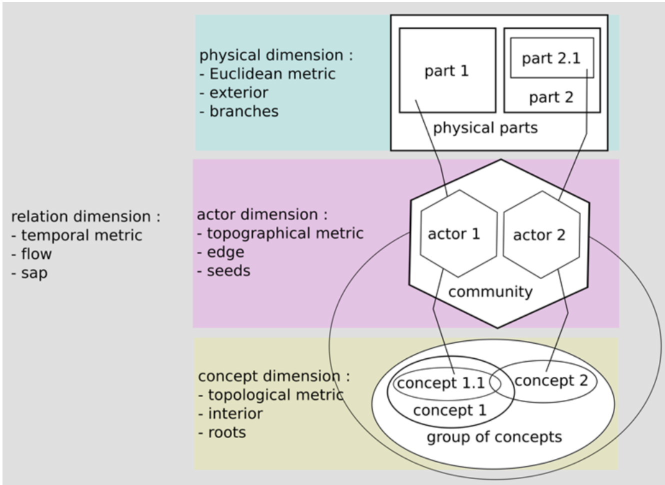

Figure 1: Modeling of existential dimensions in a knowledge ecosystem.

the refrigerator by a transaction between the "manufacturer", the "distributor" and the "family" who buys the product. This first act formalized by a "bill" initializes the chain and creates the second block in the form of a "smart contract" specifying the "guarantees" and their automatic application in case of "maintenance". This chain is replicated for these three actors which ensures its durability and immutability. The rest of the chain is composed of a register of interactions that each member of the family will operate with the refrigerator.

In this modeling, the interactions consist of evaluating the use of the refrigerator from semantic maps that feed a chain dedicated to the refrigerator that will have its own blockchain identified by the product reference (serial number). Activity data may also include the assessment of foods that are stored in the refrigerator. In this case, the data will be formalized in a blockchain corresponding to a food (barcode) and could enrich with new blocks a Blockchain dedicated to food traceability (for example a farm chicken).

The IoT ecosystem of the connected refrigerator thus consists of a multitude of blockchain each devoted to a particular product. Whatever the case, the blockchain ensures the security and durability of information through the protocol it uses. However, it is necessary to define who is authorized to consult this information. In the example we have modeled, should we make all blocks of the chain public? It is probably useful to analyze the blockchain to know what the children eat, how often and what they think. But is this information in the public domain freely available to all or only available to parents or companies willing to pay?

To answer these questions, we use the diagram above to specify whether relationships (color lines) between actors (hexagrams), documents (rectangles) and concepts (ovals) are open or closed and under which conditions. These relationships represent the "boundaries of trust" of the ecosystem, they define the rights of circulation of information. They can be formalized by "smart contracts" which will constitute a meta-blockchain used to manage the multiple Blockchains of the IoT ecosystem. At this meta level, users will define communication strategies at their household level. These will serve as a basis for discussing ecosystem development strategies at larger scale levels: cities, regions, nations, world.

4.3 Using the Blockchain in the Ecosystem of a Smart Refrigerator

Based on the previous diagram, we will analyze the possibilities of using the Blockchain in the context of the Internet of Things, specifically for the ecosystem of connected refrigerators. Let us start with the smart refrigerator manufacturer. The data on the product components and the place of manufacture could be stored on a public permissioned Blockchain that would be controlled by the manufacturer of the connected refrigerator. This Blockchain can also store data on the product's firmware, and updates could be done via the Blockchain, which would allow for better availability and traceability of these updates. Warranty data can also be stored in this Blockchain.

Blockchain can also be used in food monitoring and traceability systems. Indeed, traceability is crucial in the food supply chain to ensure food security for consumers. Blockchain technology allows you to save and share information about food products at each stage of production, throughout processing and distribution. This technology represents an opportu-

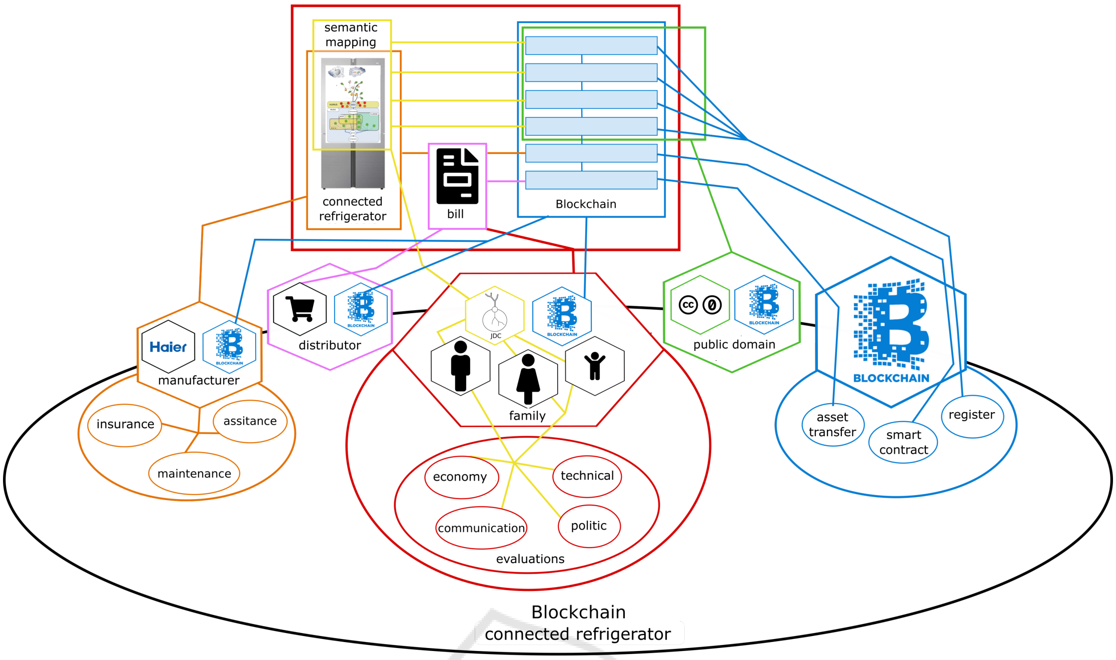

Figure 2: Ecosystem of the Blockchain for a connected refrigerator.

nity for the actors of the production chain, because it allows them to control more easily the supplies and the potential returns while providing quality information to the final consumer. It is also a way to avoid food scandals and ensure a rigorous transfer of responsibilities.

For end-users, the connected refrigerator is supposed to automate tasks such as purchasing and tracking products. To do this, it must store this information in a database. In addition, the connected refrigerator can generate recipes based on the preferences and health of the user. Management of access to all this stored information could be managed via the Blockchain, where each access to the data is recorded. Thus, users will not have to worry about their data and who has access to it. Moreover, the purchase process could be easily integrated into a blockchain network where cryptocurrency is exchanged providing an appropriate billing layer.

Finally, connected refrigerators could be used in businesses or school restaurants and blockchain could facilitate sharing (controlling access to a refrigerator, voting on menus and shopping lists ...)

5 DISCUSSION

Blockchain technology has revolutionized the reliability of information in a distributed and decentralized network. We believe this can be a way to build trust in distributed environments without the need for a trusted third-party. In addition, a system that guarantees data reliability would help secure and facilitate information sharing. Adapted to the specificities of the IoT environment, the Blockchain could solve some of the current issues of the Internet of Things.

The Blockchain can also be used to implement access control mechanisms through smart contracts, eliminating the need for a trusted third party while having an immutable log of all data access.

This technology could help transform the current architecture of IoT systems into a decentralized organization, reducing maintenance costs while ensuring security and reliability.

Research on the use of the Blockchain in an IoT environment is still in its infancy. Some problems persist and hinder this integration. Among them, we can talk about privacy protection issues. Since the details of all public keys are visible on the network, the risk of private information disclosure via data crossings is not insignificant. Indeed, cryptocurrency wallets, for example, have their public key displayed in plain view, particularly, in the block that recorded the transaction that transfered money to it. In addition, the Blockchain presents some scalability issues because the time to add a block increases with the number of nodes in the network.

In addition, the Blockchain does not comply with the GDPR. For example, the GDPR requires that data do not leave the EU, unless to jurisdictions with equivalent controls, which can be problematic in a decentralized global network. Similarly, the question of the "right to be forgotten" is not implemented in the Blockchain because it is immutable by nature and therefore, the data stored there cannot be erased.

The convergence between Blockchain technology and the emergence of collective intelligence projects is in line with our proposals of knowledge design in the IoT. They develop in the context of Digital Social Innovations (DSI) that can be described as:

> *"First, at the social level, the DSIs cover perimeters of collective use, involving a multitude of actors in order to co-create a societal value [...]. Secondly, at the technological level, they generate an open operating process based on an innovative hardware and software architecture as well as on specific functional mechanisms. Finally, at the ecological level, the DSIs focus on responsible innovation [...] and the desire to respond to social and environmental problems, improve the quality of life of citizens and create a sense of social justice"* (Boulesnane and Bouzidi, 2018).

In the case of the IoT, DSIs aim to develop a multi-agent architecture for ambient intelligence based on environmental modeling through representations of knowledge such as EKRL (Environment Knowledge Representation Language) (Dourlens, 2012). Designing these architectures with blockchain technologies would keep the history of interactions between agents and with users to build a representation of distributable and non-falsifiable knowledge. In addition, the blockchain would make it possible to contractualize certain actions such as purchase requests or access authorizations to private data and thus better manage the proliferation of this data in digital networks.

6 CONCLUSION AND FUTURE WORK

In this article, we looked at the Blockchain and related technologies. We have seen that it has characteristics that could benefit the Internet of Things. We used the example of a connected refrigerator to illustrate, with an example, the possible applications of the Blockchain. The integration of the Blockchain into the IoT ecosystem can provide solutions to some current issues.

However, there is still work to be done to reconcile an IoT environment with limited resources, with the requirements of Blockchain technology. Mainly, we plan to build a prototype to test the feasibility of an information and communication device using the blockchain in an IoT ecosystem, then, design an evaluation protocol for this device to analyze how the device increases or decreases the power to act of users in their interaction with the connected refrigerator. Finally, we want to test the prototype and the protocol in a real environment.

We have shown how a knowledge gardening device makes management of these ecosystems accessible and how Blockchain technologies ensure both security and sustainability of information. The combination of these two approaches gives the users of connected objects the means to define "boundaries of trust" and to think about strategies for developing ecosystems. This research reveals many issues such as those related to the ergonomics of augmented reality devices for gardening knowledge, or that of the efficiency of Blockchain technologies, particularly in terms of computing resources and availability of digital networks. It is probably illusory to think that these technologies can be conceived in all contexts. It will therefore be necessary to precisely define the resources needed to consider the conditions for the development of such a device. More generally, the collective intelligence platform that we are considering poses many technical, legal, political and ethical questions (Floridi, 2018) (Russo, 2018) that will have to explore in a concrete framework of experiments such as those of those of the Human At Home project[6].

REFERENCES

Atlam, H. F., Alenezi, A., Alassafi, M. O., and Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *International Journal of Intelligent Systems and Applications*, 10(6):40–48.

Boulesnane, S. and Bouzidi, L. (2018). Les innovations sociales numériques dédiées à l'e-participation citoyenne: quelle place pour la civictech? *Terminal. Technologie de l'information, culture & société*, (122).

Brody, P. and Pureswaran, V. (2014). Device democracy: Saving the future of the internet of things. *IBM, September*.

Brun, G. (2017). Pouvoir d'agir, en analyse de l'activité. Traces, usages et figures modernes de Spinoza. *Activités*, 14(14-1).

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Etherum*, (January):1–36.

Capstone (2015). NEM Technical Reference. *Capstone MicroTurbine User ' s Manual*, (February):1–23.

[6]http://hut.edu.umontpellier.fr/

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*.

Citton, Y. (2014). *Pour une écologie de l'attention*. Le Seuil.

De Filippi, P. (2018). *Blockchain et cryptomonnaies:≪Que sais-je?≫ n○ 4141*. Presses Universitaires de France.

Dorri, A., Kanhere, S. S., and Jurdak, R. (2016). Blockchain in internet of things: Challenges and Solutions.

Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P. (2017). Blockchain for IoT Security and Privacy : The Case Study of a Smart Home. *Ieee Percom Workshop on Security Privacy and Trust in the Internet of Thing*, (March).

Dourlens, S. (2012). Multimodal Interaction Semantic Architecture for Ambient Intelligence.

Febin, J. J. (2018). 3 Popular Types Of Blockchains You Need To Know – Hacker Noon.

Floridi, L. (2018). Soft Ethics: Its Application to the General Data Protection Regulation and Its Dual Advantage. *Philosophy & Technology*, pages 1–5.

Huh, S., Cho, S., and Kim, S. (2017). Managing IoT devices using blockchain platform. In *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pages 464–467. IEEE.

Lévy, P. (2017). La pyramide algorithmique. *Sens Public*.

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3. IEEE.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Özyılmaz, K. R. and Yurdakul, A. (2017). Integrating low-power IoT devices to a blockchain-based infrastructure. In *Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion - EMSOFT '17*, pages 1–2, New York, New York, USA. ACM Press.

Pettey, C. (2015). The Internet of Things and the Enterprise - Smarter With Gartner.

Roxin, I. and Bouchereau, A. (2017). Introduction to the Technologies of the Ecosystem of the Internet of Things. *Internet of Things: Evolutions and Innovations*, 4:51–95.

Russo, F. (2018). Digital Technologies, Ethical Questions, and the Need of an Informational Framework. *Philosophy & Technology*, pages 1–13.

Saleh, I. (2017). Les enjeux et les défis de l'internet des objets (ido). *Internet des objets*, 1(1).

Saleh, I., Ammi, M., and Szoniecky, S. (2018). *Challenges of the Internet of Things: Technique, Use, Ethics*. John Wiley & Sons.

Shermin, V. (2017). Types of Blockchains & DLTs (Distributed Ledger Technologies).

Szabo, N. (1994). Smart Contracts.

Szoniecky, S. and Safin, S. (2017). Modélisation éthique de l'Internet des Objets. *Internet des objets*, 17(2).

Tsui, D. (2016). Account Types, Gas, and Transactions — Ethereum Homestead 0.1 documentation.

Wood, G. (2015). Ethereum: A Secure Decentralised Generalised Transaction Ledger Final Draft - Under Review.

Wood, G. (2016). Blockchain what and why.