Blockchains and smart contracts:
Prospects for the Internet of things and e-health

Philippe Genestier,
PhD in microelectronics, Orange Labs;
Loïc Letondeur,
R&D engineer, Orange Labs;
Sajida Zouarhi,
engineer and doctoral student in information sciences and networks at Orange Labs and Laboratoire d'Informatique de Grenoble (LIG, INP);
Alain Prola,
inventor/developer of applications for Androïd;
& **Jean-Marc Temerson**,
research engineer, head of projects at Orange Labs, now retired.

In J.P. Dardayrol, editor of the special issue *Blockchains and smart contracts: The technology of trust?* of *Réalités industrielles*, 2017

Abstract:
Given the growing use of devices connected through the Internet of things and the increasing interconnection of disparate systems producing myriads of personal data, our digital society faces new questions about: the decentralized, "mixed" administration of these "things", resilience, the respect of confidentiality when accessing data, traceability of uses, etc. In response, blockchain technology is proposing: a decentralized organization, a consensus procedure that satisfies diverging interests and "distributed trust" — since the trusted third party is eliminated. New opportunities will arise in a sharing economy based on social networks 2.0, where connected human beings and devices will interact without any difference being made between the two. Blockchains can help link the physical and virtual worlds: an operation (or "transaction") in the real world will have a counterpart in the digital realm. Though not answering all questions, blockchain technology is appropriate whenever trust, transparency and traceability are indispensable. Let us not fail to mention, however, what blockchains cannot do: they cannot verify the authenticity of recorded data or the legitimacy of "nonelectronic" operations.

The possibilities offered by blockchain technology, in particular the automation of transactions via smart contracts, opens a vast field of applications and of organizational turmoil as roles come under question in many areas, in particular, the Internet of things (IoT) and health.[1]

The IoT's rapid expansion comes with new issues. These connected devices call for innovative approaches both for managing them and controlling the data they generate. A technology such as blockchains can address some or all of these issues while generating novel uses, as attested by Filament, IOTA or IBM Watson IoT.

The 26 billion connected devices foreseen by 2020 will represent a fleet of an unprecedented size that will have to be administered and operated. Guaranteeing security, confidence, transparency, privacy and the quality of services are key questions for the IoT's prospects. These same issues arise in the field of health as telemonitoring (whether or not via connected devices) develops and as medical records in quite diverse information systems are being digitized. For these records, tight regulations exist, in particular concerning patients' consent for access to their data. To move beyond the unadapted traditional approaches based on a centralized platform or the postulate of end-to-end governance, blockchain technology could be of help.

Issues surrounding the Internet of things

The IoT is an environment that is both massive and geo-distributed. Vertical networks, as in health, require a high, predictable level of performance, especially in terms of network bandwidth and latency. Given these requirements, IoT platforms should be as available as possible despite an environment that might be unfavorable, whether due to the weather, technical failures (at any level ranging from the devices themselves through points in the network to the data centers) or malevolent actions (a recent example being Mirai, the malware used to launch a denial-of-service attack via connected cameras in 2016). As a consequence, IoT platforms have to have properties such as resistance (the ability to remain operational during a breakdown) and resilience (strategies for recovering an operational state).

Other issues must also come under consideration, such as: the need for scalability (given the huge number of connected devices); problems of storage (given the independence of the manufacturers of electronic devices and the absence of standards with, as a consequence, isolated subsets of data that might not be interoperable); governance (splintered between several parties); the heterogeneity of devices, protocols, programing environments and exchange formats; and the invention of connected devices.

Given all these issues, the only response can come from platforms that distribute the functions of communications, data-processing (access, filters, aggregation, storage) and administration as closely as possible to connected devices, as on fog computing platforms, which have moved the concepts of cloud computing in the direction of users. Part of the work of data-processing is shifted onto the connected devices themselves (watches, sensors, etc.) or onto the gateways used by these devices (LiveBox, mobile telephones, etc.). Blockchain technology bears first-rate solutions for creating these platforms, which will be multi-agent intelligent systems.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

Problem areas in e-health

Digitization is advancing in the health field: telemonitoring, computerized patient records in all health organizations, and plans for a personalized or precision medicine. These advances are stirring up concern about privacy and security, not to mention the rules and regulations that care-givers must take into account. Furthermore, the fracturing of medical information systems and the growing need for interconnections and exchanges of data between systems entail lengthy procedures for obtaining the consent of data-keepers to share their data with multiple third parties. The question also crops up about how to authenticate data. As for medical insurance, it is often hard to have up-to-date information on the coverage provided to insurees.

Blockchain technology

Blockchains are a technological innovation in the storage of information. Each entry is authenticated and recopied; it is irreversible. A blockchain thus safely stores data under decentralized control, since no central authority controls the database's contents. It relies on cryptographic techniques (asymmetry, the hash function) and on using a network made up of independent nodes. Hashing is the process of calculating a digital signature of a fixed length for a data set such that any modification of the data entails modifying the signature. Blockchain technology originated with the cryptocurrency bitcoins, for which it was used to create a reliable chronological ledger of financial transactions.

Alternative forms of the blockchain principle have been implemented that vary with respect to: the granting of reading and writing permissions (private, public or semi-public), the type of information stored on the blockchain (a ledger for financial transactions, a real estate registry, etc.) and performance (7 transactions validated per second on Bitcoin vs. 1000 tps for blockchains without a proof-of-work system).

Blockchain technology has come along with new prospects: smart contracts for automated conditional transactions to be executed without human intervention and without a trusted third party; and decentralized applications using a blockchain as an infrastructure for their execution (without a centralized platform).

Blockchains and the Internet of things

Although blockchain technology does not address all issues raised by the IoT, it does have several interesting features and properties that could determine the choices made by IoT platforms.

By nature, the IoT is dynamic not only because of the mobility of devices in the network and the risks of failure but also owing to its close association with the now global consumer society, where product obsolescence and sporadic mass purchases are run of the mill. This association entails, in turn, a high degree of complexity related to the infrastructure and the invention of connected devices. The connection of a given device, now legitimate, might soon no longer be so, once the device is resold or stolen or discarded. In addition, users have to be protected from malevolent devices by preventing the latter from being connected. By offering a robust registry with traceable authorizations linking the end-user's choices to IoT platforms, blockchains will provide a solution for legitimating, rejecting or blocking devices. This would extend what is known as consent management. The blockchain would be a record of the conditions that the owner of data grants to a third party for accessing them. In other words, the person equipped with a connected device (or its administrator) may make a traceable, attested declaration of the device's status (operational, obsolete, public access, etc.).

An IoT platform will consist of large sets of hierarchically ranked “agents” capable of running and administering subsets of the IoT. Given the IoT’s highly dynamic but hostile environment, these agents will come into conflict when making decisions. There will be conflicts about who is responsible and legitimate for deciding the actions that target a device (its data or hardware) or for making a decision about the data and features that may be used in compliance with the user’s choices and privacy.

Blockchain technology has been designed to solve the problem of reaching a consensus. It does this by creating a distributed authority that, secure, coherent and traceable, is capable of verifying whether an IoT platform measures up to specifications.

In general, blockchain technology is an innovative solution for delegating rights to data-keepers to control the use of data by third parties, as required in the medical field (See the work under way in the Healthcare Data Institute and the Orange Group).

Several use cases for a blockchain have been identified that take advantage of its inherent characteristics:

- consent management.[2] It lies at the center of the obligations imposed by regulations and of concerns about sharing information among stakeholders in the health field: the patient’s consent for care-givers to collect and consult his/her data, or to use these data in clinical studies. With regard to the IoT: the management of the consent given by a device’s owner so that a third party may use the data from the device (a stipulation of the conditions for use, for example whether the data can be diffused or aggregated with other data).
- the traceability of the actions for collecting and storing data.
- the operation of platforms that exchange data (for example, for matching organ donors and transplant recipients).[3]
- the monitoring of devices for as long as they last (production, transportation, storage and use).

Returning power to users

When placed at the service of the IoT (especially through methods similar to fog computing), a blockchain will enable users to manage in detail the rights to access their devices and data and the permissions for third parties to use them. It will keep a journal of the uses of an owner’s connected devices while providing a traceability that will serve as proof in case of misuse. These two advantages will reinforce users’ confidence in the IoT despite the anxiety aroused by the stories told about Big Brother or Skynet. A blockchain reasserts the user’s control over his/her existence in the digital realm.

Beyond its technical advantages, blockchain technology could serve as the grounds for a new economy with new sources of income. For example, it will facilitate the development of social media 2.0, where human beings and connected devices interact without distinction and engage in transactions, such as the purchase of products needed by both. On this, see the example provided by IBM and Samsung of a washing machine that orders its own detergent when its stock is exhausted. These networks will form the foundation of a “sharing” economy that remunerates the owners of connected devices for letting other members of the network, whether human or not, use their devices. This economy follows on the current ”uberization” and deregulation, which are turning users into both suppliers and “consumactors” of goods and services. Given the prospects of big data, social networks of this sort will be a tremendous source of value.

[2] GENESTIER P., ZOUARHI S., LIMEUX P., EXCOFFIER D., PROLA A., SANDON S. & TEMERSON J.M., “Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges”, *Journal of the International Society for Telemedicine and eHealth*, 5, 2017.

[3] For more information, see: www.kidner-project.com.

Blockchain technology thus appears to be an extraordinary facilitator for the IoT platforms of tomorrow. These fully decentralized platforms (of a fog computing type, for example) will offer a quality of service that is reliable, traceable and controllable by end users.

The limitations of blockchains

Though theoretically capable of advancing the transition under way toward the IoT, blockchain technology is not a miracle solution. It has a few limitations.

First of all, blockchains do not guarantee the reliability of uploaded data; nor do they authenticate persons (*i.e.*, verify whether the person connected is who he/she claims to be, by using Orange's Mobile Connect, for example). Guarantees of this type require other procedures.

A second limitation comes from the blockchain's scope of application. It only applies to "things" (devices, events…) with sound mooring in the digital realm. EverLedger has brilliantly managed to do this for the tracking of diamonds, the aim being to fight against fraud. An event without a digital trail cannot be taken into account.

From a technical viewpoint, a blockchain heavily relies on hashing and deciphering techniques. Since certain blockchain registers (or ledgers) will be used for several decades and since a blockchain's reliability stems from its inherent procedures, a serious problem must be solved: how long will the information stored on a blockchain be protected? After all, current algorithms will become vulnerable. A report by the National Institute of Standards and Technology (NIST) has pointed out that they will are unlikely to withstand quantum computing, which could exist by 2030. A quantum computer will have enough computational power to breach current systems of protection; and it could, therefore, alter past transactions on the ledger.

In a court of law, a blockchain constitutes *de facto* evidence. But given that laws do not currently recognize it, a blockchain is not proof like a notarial act.

Conclusion

Blockchain technology provides responses to many issues (decentralization, traceability and confidence) raised by the IoT and e-health. Without claiming to settle all problems, it does open onto new prospects — an unprecedented possibility to be explored by stakeholders who cannot afford to hold aloof from taking an interest in this new technology.