Blockchains et *Smart Contracts* : des perspectives pour l'Internet des objets (IoT) et pour l'e-santé

Par Philippe GENESTIER
Docteur en microélectronique chez Orange Labs
Loïc LETONDEUR
Ingénieur en Recherche et Développement, en fonction au sein d'Orange Labs
Sajida ZOUARHI
Ingénieure et doctorante en informatique et réseaux chez Orange Labs et au LIG (Laboratoire d'informatique de Grenoble INP)
Alain PROLA
Concepteur/développeur d'applications sur plateforme Androïd
et Jean-Marc TEMERSON
Ingénieur de recherche, responsable d'équipe et de projets au sein d'Orange Labs, aujourd'hui à la retraite

Du fait de l'utilisation croissante d'objets connectés (IoT) et de l'interconnexion de systèmes hétérogènes générant des myriades de données personnelles, notre société numérique se trouve confrontée à des défis nouveaux, qu'elle se doit de relever : administration décentralisée et composite de ces objets, résilience, respect de la vie privée dans l'accès aux données, traçabilité des usages...
La *blockchain* offre des réponses à ces défis :
- un fonctionnement décentralisé,
- des mécanismes de consensus permettant de concilier des intérêts divergents,
- une confiance répartie par la suppression du tiers de confiance unique.
De nouvelles opportunités émergeront au sein d'une nouvelle économie du partage basée sur des réseaux sociaux 2.0, dans lesquels humains et objets connectés interagiront de façon indifférenciée. La *blockchain* nous permet de créer des « ancres » entre le monde physique et le monde virtuel. C'est ainsi qu'une opération ou une transaction dans le monde réel pourra avoir son homologue dans le monde numérique.
Même si la *blockchain* ne répond pas à toutes les problématiques, ce type de solution est tout à fait pertinent dans des domaines où confiance, transparence et traçabilité sont indispensables. Néanmoins, il ne faut pas passer sous silence ce que la *blockchain* ne permet pas, notamment la vérification de l'authenticité des données enregistrées ou la vérification de la légitimité d'une opération « non électronique ».

Les possibilités offertes par la technologie *blockchain,* en particulier l'automatisation des transactions *via* des *smart contracts*, ouvrent un champ immense d'applications et de bouleversements organisationnels par la remise en question du rôle de certains acteurs, dans de nombreux domaines. Cela concerne en particulier des domaines comme l'Internet des objets (IoT, *Internet of Things*) ou la santé.

L'expansion rapide de l'Internet des objets dans notre monde numérique soulève des défis nouveaux. Tant pour leur gestion que pour la maîtrise des données qu'ils génèrent, ces objets connectés nécessitent des approches innovantes. Des technologies comme la *blockchain* permettent de relever tout ou partie de ces défis, tout en engendrant des usages novateurs : en témoignent des acteurs tels que Filament, IOTA ou IBM Watson IoT.

Les 26 milliards d'objets connectés pressentis à l'horizon 2020 constitueront une armada de taille inédite à administrer et à exploiter. Les aspects de garantie de sécurité, de confiance, de transparence, de qualité de service et de respect de la vie privée sont des questions clés pour le développement de l'IoT. Ces mêmes questions se posent également dans le domaine de la santé, avec le développement des solutions de télé-suivi (basées ou non sur des objets connectés) et de dossiers médicaux numérisés dans des systèmes hétérogènes, pour lesquels des exigences réglementaires fortes existent (notamment en ce qui concerne la prise en compte du consentement des patients à un accès à leurs données). Les approches traditionnelles basées sur des plateformes centralisées et/ou sur le postulat d'une gouvernance de bout-en-bout seront inadaptées. Pour dépasser ces approches, la technologie *blockchain* pourrait apporter des éléments de réponse.

Les défis de l'Internet des objets

L'IoT concerne un environnement à la fois massif et géo-distribué. Pourtant, les réseaux verticaux, à l'instar de celui de la santé, exigent des performances à la fois élevées et prédictibles, notamment en termes de bande passante et de latence réseau. Ces exigences requièrent une disponibilité aussi grande que possible des plateformes IoT malgré un environnement défavorable, que celui-ci soit dû à des risques de défaillance qui se retrouvent à tous les niveaux – des objets eux-mêmes jusqu'aux infrastructures de *datacenters,* en passant par les éléments réseau –, à des risques dus à la malveillance – illustrés par le récent exemple du *malware* Mirai [1] – ou encore aux aléas climatiques.

En conséquence, les plateformes IoT doivent posséder des propriétés de résistance (capacité à maintenir un état fonctionnel lors d'une occurrence de panne) et de résilience (mise en place de stratégies visant à recouvrer un état fonctionnel).

Par ailleurs, d'autres éléments doivent être pris en compte, comme la nécessité de pouvoir passer à l'échelle face au grand nombre d'objets connectés, le silotage (indépendance des constructeurs et absence de normes conduisant à des sous-ensembles isolés, parfois non interopérables), la gouvernance (éclatée entre de nombreux acteurs), l'hétérogénéité (des matériels, des protocoles, des environnements de programmation et des formats d'échange) et la découverte des objets connectés.

Face à de tels enjeux, seules répondront des plateformes distribuant des capacités de communication, de traitement des données (accès, filtrage, agrégation, stockage) et d'administration au plus près des objets, à l'instar des plateformes de *Fog Computing* [2]. La *blockchain* apporte des solutions de choix pour réaliser ces plateformes, qui seront des systèmes intelligents multi-agents.

Les problématiques du domaine de l'e-santé

L'informatisation croissante du domaine de la santé (avec le développement du télé-suivi, celui des dossiers patients dans tous les organismes de soins ou encore la mise en place de projets sur la médecine personnalisée) génère des préoccupations croissantes en termes de respect de la vie privée, de sécurité, en plus des contraintes réglementaires à prendre en compte par les acteurs du secteur. En outre, l'aspect très éclaté des systèmes d'information médicaux et les besoins croissants d'interconnexions ou d'échanges de données entre ceux-ci nécessitent de lourds processus de prise en compte du consentement des détenteurs de données au partage de celles-ci avec plusieurs tierces parties. Par ailleurs, ces mêmes usages soulèvent la question de l'authenticité des données et celle des moyens permettant de s'en assurer. Au niveau des assurances médicales, il est souvent difficile d'avoir une information à jour en ce qui concerne les droits d'un assuré.

La technologie *blockchain*

La *blockchain* est une innovation technologique en matière de stockage d'informations. Elle permet de stocker de façon sécurisée des informations (chaque écriture est authentifiée, irréversible et répliquée) avec un contrôle décentralisé (il n'y a pas d'autorité centrale qui contrôlerait le contenu de la base de données).

Elle s'appuie sur des techniques cryptographiques (fonction de *hash* [3] et cryptographie asymétrique) et sur l'utilisation d'un réseau informatique de nœuds indépendants.

Les technologies de la *blockchain* proviennent initialement de la crypto-monnaie bitcoin, pour laquelle elles ont été utilisées afin de créer un historique fiable des transactions financières.

Il existe des mises en œuvre alternatives autour du principe de la *blockchain*, avec des variantes dans les permissions de lecture et d'écriture des informations (privées, publiques ou semi-publiques), dans les types d'informations stockées (transactions financières, registre de propriété...) et en matière de performances (7 tps [4] pour bitcoin contre plus de 1000 tps avec d'autres *blockchains* sans mécanisme de preuve de travail).

La technologie *blockchain* voit aussi apparaître des évolutions qui ouvrent de nouvelles perspectives : les *smart contracts* qui réalisent des transactions conditionnelles automatisées s'exécutant sans intervention humaine ni tiers de confiance ; les applications décentralisées qui utilisent la *blockchain* comme infrastructure pour s'exécuter sans plateforme informatique centralisée.

---

(1) Une attaque de type déni de service via *des caméras connectées a été menée en 2016.*
(2) Le Fog Computing *est un prolongement des concepts du* cloud computing *au plus près des utilisateurs : déport d'une partie des traitements dans les objets connectés eux-mêmes (montres, capteurs…) ou dans les passerelles qu'ils utilisent (LiveBox ou téléphone mobile…).*
(3) Le hash *consiste à calculer une signature numérique de longueur fixe sur un ensemble de données, de sorte que toute modification de ces données entraîne une modification de la signature.*
(4) TPS : transactions par seconde. Il s'agit d'un indicateur de performance qui se base sur le nombre de transactions qui sont validées par le réseau en une seconde.

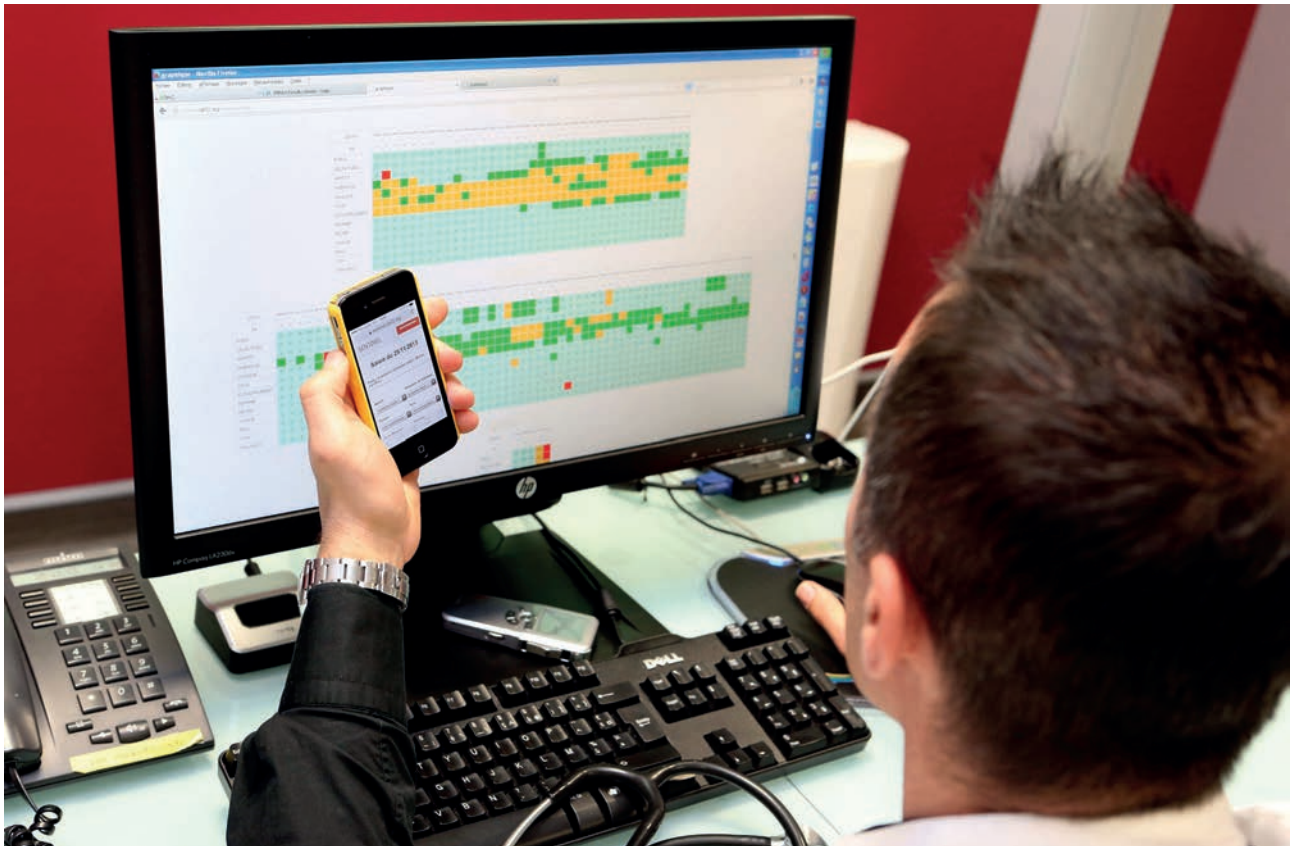

Photo © Bigot/ANDIA.fr

Recours au Centre Jean Bernard au Mans – Clinique Victor Hugo à une application utilisable sur *smartphone* inventée par Fabrice Denis, oncologue de l'établissement, pour dépister par anticipation les risques de récidive du cancer du poumon.

« L'informatisation croissante du domaine de la santé (avec le développement du télé-suivi, celui des dossiers patients dans tous les organismes de soins ou encore la mise en place de projets sur la médecine personnalisée) génère des préoccupations croissantes en termes de respect de la vie privée, de sécurité, en plus des contraintes réglementaires à prendre en compte par les acteurs du secteur. »

Les réponses apportées par la *blockchain* à l'Internet des objets

Si la *blockchain* ne fournit pas des réponses à tous les défis de l'IoT, elle apporte néanmoins un ensemble de fonctionnalités et de propriétés intéressantes qui pourraient constituer des éléments de choix pour les plateformes IoT.

L'IoT est par nature dynamique non seulement de par la mobilité des éléments qui le composent et de par les risques de défaillance, mais également en raison de son lien étroit avec la société de consommation mondialisée, où achats sporadiques de masse et obsolescence sont de règle. De ce lien découle une forte complexité liée à la découverte des objets connectés et des éléments d'infrastructure. Si tel objet s'avère légitime à un moment donné, il peut rapidement ne plus l'être, suite à sa revente ou à son vol, ou de par sa mise au rebut par les utilisateurs. Par ailleurs, il est nécessaire de protéger l'utilisateur contre des objets malveillants en interdisant la prise en compte. La solution *blockchain* permettra de légitimer les objets, de les répudier et de les bloquer en offrant un registre résistant et traçable d'autorisations liant le choix des utilisateurs finaux aux plateformes IoT. Une telle fonctionnalité est une extension de celle qui est connue sous l'expression de gestion de consentement et qui consiste à enregistrer les modalités de l'accès à ses données octroyé par un propriétaire à un tiers. Dans le cas présent, il s'agira pour le détenteur ou l'administrateur d'un objet de pouvoir en définir le statut (opérationnel, obsolète, en accès public…) d'une manière qui soit traçable et non répudiable.

Ces plateformes seront composées d'importants ensembles d'agents hiérarchisés capables d'exploiter et d'administrer des sous-ensembles de l'IoT. Du fait de la nature ultra-dynamique et hostile de l'IoT, ces agents entreront en conflit de décision et de responsabilité pour savoir qui est légitime pour décider d'actions sur les objets, l'infrastructure et les données, ou encore quelles sont les données et les fonctionnalités utilisables tout en préservant le respect du choix des utilisateurs et de leur vie privée.

La *blockchain* apportera par construction une solution de recherche de consensus à même de résoudre ces conflits en créant une autorité répartie, sécurisée, cohérente et traçable apte à vérifier toutes propriétés que les plateformes IoT devront posséder.

Plus généralement, la *blockchain* constitue une solution innovante en matière de délégation de droits pour rendre à un détenteur de données le contrôle de leur usage par des tiers, comme cela est imposé par la réglementation dans le domaine médical (en attestent les travaux en cours à ce sujet dans le cadre du Healthcare Data Institute et au sein d'Orange).

De cette communauté de besoins ont été identifiés plusieurs cas d'usage intéressant ces domaines et tirant parti des caractéristiques intrinsèques de la *blockchain* :

- la gestion du consentement [5], car celui-ci est au cœur des obligations réglementaires et des préoccupations pour le partage d'informations entre acteurs du monde de la santé : consentement du patient à la collecte et à la consultation de ses données par des soignants, ou encore à l'utilisation de ses données dans le cadre d'études cliniques. Dans le monde de l'Internet des objets, consentement du propriétaire d'un objet pour que les données issues de cet objet soient utilisées par des tiers (et définition des conditions d'utilisation), par exemple pour les diffuser ou les agréger avec d'autres ;
- la traçabilité des actions effectuées dans un système de collecte et de stockage de données ;
- la mise en œuvre de plateformes d'échange de données (par exemple, pour la mise en relation de donneurs et de receveurs d'organes[6]) ;
- le suivi de matériels tout au long de leur vie : production, transport, stockage et utilisation.

Rendre le pouvoir à l'utilisateur

Mise au service de l'IoT, et notamment dans des approches du type *Fog Computing*, la *blockchain* permet à l'utilisateur de gérer finement les droits d'accès à ses propres objets et données et leur utilisation par des tiers, ainsi que de journaliser les utilisations du patrimoine connecté des utilisateurs, tout en leur offrant une traçabilité ayant valeur de preuve en cas d'abus.

De ces deux atouts résulte une confiance renforcée des utilisateurs dans l'IoT face à l'aspect anxiogène de mythes errant de Big Brother en Skynet : la *blockchain* réaffirme leur gouvernance sur leur existence dans le monde numérique.

Au-delà de ses apports techniques, la *blockchain* pourra être le terreau d'une économie nouvelle laissant entrevoir de nouvelles sources de revenus. Par exemple, en facilitant l'émergence de réseaux sociaux 2.0, dans lesquels humains et objets connectés interagiront de façon indifférenciée au travers de transactions telles que l'achat de produits dont les deux types d'acteur auraient besoin (voir à ce sujet l'exemple développé par IBM et Samsung de machine à laver capable de commander de la lessive lorsque son stock est épuisé). Ces réseaux pourront être le support d'une économie collaborative rétribuant les possesseurs d'objets connectés en fonction de leur utilisation par d'autres membres du réseau, qu'ils soient humains ou objets. Cette économie s'inscrira pleinement dans le contexte actuel d'« ubérisation » et de déréglementation plaçant l'utilisateur comme fournisseur et « consommacteur » de biens et services. Par ailleurs, de tels réseaux sociaux seront une formidable source de création de valeur dans des perspectives de *Big data*.

La *blockchain* apparaît ainsi comme un facilitateur extraordinaire pour les plateformes IoT de demain (de type *Fog Computing,* par exemple), qui seront complètement décentralisées, offrant un service de qualité, fiable, traçable et maîtrisable par l'utilisateur final.

Les limites de la *blockchain*

Théoriquement apte à faciliter la transition en cours vers le monde IoT, la *blockchain* n'est cependant pas la solution miracle. Elle présente de fait quelques limites.

En premier lieu, elle n'assure ni la fiabilité des données remontées ni l'authentification des acteurs (qui consiste à s'assurer qu'une personne est bien celle qu'elle prétend être, par exemple à l'aide d'une solution comme Mobile Connect d'Orange), qui sont du ressort d'autres mécanismes. Une seconde limitation est relative au champ d'application de la *blockchain*, celle-ci ne concernant que des éléments (objets, événements…) ayant une « ancre » fiable dans le monde numérique, comme EverLedger a su le faire brillamment pour la traçabilité des diamants afin de lutter contre la contrefaçon. Un événement n'ayant pas de trace numérique ne pourra pas être pris en compte.

Ensuite, d'un point de vue technique, la *blockchain* fait un fort usage des technologies actuelles de *hash* et de chiffrement. Sachant que l'utilisation de certains registres créés au travers de la *blockchain* peut durer plusieurs dizaines d'années et que la fiabilité de la *blockchain* est basée sur celle de ses mécanismes intrinsèques, se pose donc une véritable problématique de pérennité de la protection des informations stockées face à la vulnérabilité future des algorithmes utilisés. En effet, un rapport du NIST (*National Institute of Standards and Technology*) pointe la vulnérabilité de ces algorithmes face à un ordinateur quantique (celui-ci pourrait exister dès 2030). Un tel ordinateur aura une puissance suffisante pour casser les protections mises en place aujourd'hui, et donc, en particulier, pour revenir sur des transactions passées.

Enfin, sur le plan juridique, la *blockchain* constitue une preuve « de fait » qui, en l'absence actuelle de qualification légale, n'est pas une preuve d'acte juridique.

Conclusion

Face aux nombreux défis posés par l'IoT et l'e-santé, et face aux besoins suscités en termes de décentralisation, de traçabilité et de confiance, la *blockchain* offre des réponses. Sans avoir la prétention de résoudre tous les problèmes, elle ouvre également la porte vers de nouveaux horizons. De ce fait, elle présente des champs d'investigation inédits aux acteurs du domaine, qui ne pourront faire l'économie de s'y intéresser.

---

(5) Blockchain for Consent Management in the eHealth Environment: A Nugget for Privacy and Security Challenges, *par GENESTIER Ph., ZOUARHI S., LIMEUX P., EXCOFFIER D., PROLA A., SANDON S. & TEMERSON J.-M. Publié dans* Journal of the International Society for Telemedicine and eHealth *(2017).*

(6) Plus d'informations sur le site officiel du projet Kidner : www.kidner-project.com