# Living Things

## Traçabilité, sécurité, collaboration : ce que peut la blockchain pour l'IoT

**Compte-rendu.** Evénement du 10 juillet 2018

Ces dernières années, les technologies blockchain et de registre distribués ont émergées comme des innovations contribuant au développement de systèmes d'informations plus transparents, sûrs et résilients. Leur impact se profile dans de multiples domaines, de la relation client à la supply chain en passant par le microtrading d'énergie. Devant l'un des défis majeurs de l'IoT, la sécurité des objets connectés, ces technologies pourraient apporter une réponse.

Le marché est relativement jeune, mais il génère de fortes attentes. Plusieurs startups développent des solutions appliquées à des cas tels que la gestion des réseaux électriques intelligents, la traçabilité des produits et bien sur l'identification sécurisée d'utilisateurs.

Par ailleurs, la blockchain et des technologies de registres distribués proposent des modèles économiques nouveaux, basés sur les «  coin  » et les crypto monnaies.

Quelles solutions existent aujourd'hui et quel est leur degré de maturité ? Ont-elles trouvé leur place dans la chaîne de valeur de l'IoT? Quels sont les premiers retours d'expérience des startups, des PMEs, des industriels ? Bouleversent-elles les modèles économiques? Quelles en sont les limites et les alternatives ?

Avec **Xavier Lavayssière**, fondateur d'ECAN, **Sara Tucci-Piergiovanni**, Head of Laboratory at CEA LIST, **Emmanuel Moyrand**, Président et co-fondateur de Monuma, **Philippe Nguyen**, Directeur technique de SECURE IC, **Nicolas Bacca**, CTO de Ledger.

cap-digital Paris Region

Systematic Paris Region Digital Ecosystem

# Introduction

## Par Xavier Lavayssière, fondateur et directeur d'ECAN

La popularisation du Bitcoin et des cryptomonnaies a  entrainé depuis 2014 des tentatives d'utilisation des technologies sous-jacentes, notamment pour résoudre certaines des difficultés auxquelles était confronté l'écosystème des objets connectés.

### Les "technologies blockchains"

Le mot blockchain est apparu dans le document décrivant le fonctionnement du Bitcoin en 2008 pour décrire l'historique des transactions organisé sous la forme de blocs. Chaque bloc, constitué des transactions émises dans un intervalle de temps, est validé et ajouté à la suite des blocs précédents de façon décentralisée par un algorithme de consensus. Blockchain désigne la suite de blocs, puisque chaque bloc comporte une référence cryptographique au précédent, et, par synecdoque, l'ensemble du procédé.

La raison d'être de ce système est d'assurer la transmission d'unités de valeur de façon numérique, sans risque de double dépense par un utilisateur ou de saisie des fonds par une autorité. Une composante technique et une composante idéologique sont à l'origine du projet Bitcoin. Le procédé garantit à tous les utilisateurs du réseau, sous certaines conditions, l'intégrité des paiements dans cette unité de valeur.

Comme il s'agit d'un réseau pair à pair, sans serveur central, dont l'intégrité de l'information est en partie assurée, l'idée est apparue d'utiliser ce type de procédés pour valider des paiements mais aussi d'autres informations dans des environnements complexes.

### Expérimentations et limitations

Ainsi ont fleuries les expérimentations associant IoT et blockchain. Une des premières du genre, entre RWE, énergéticien allemand (devenu Innogy), et Slock.it, startup positionnée sur des solutions à base d'Ethereum[1] et d'IoT, vise à fournir une solution efficace pour l'authentification et le paiement de bornes de recharge de véhicules électriques.

La mise en œuvre technique de ces projets a fait apparaître des défis issus de la rencontre de ces technologies. En premier lieu, la sécurité : les blockchains reposent sur une sécurité aux abords, où chaque nœud est responsable du contrôle des clés cryptographiques qui lui permettent de contrôler des fonds, ou d'inscrire des informations. Dans le contexte IoT où les appareils sont répartis physiquement, garantir ce contrôle demande des architectures et technologies rigoureuses.

Pour la protection de la vie privée, ces technologies offrent aussi une solution paradoxale. Bien que basés sur de la cryptographie, les procédés de validation des transactions reposent sur leur transparence. Les solutions dépendent autant de la conception de l'architecture des projets utilisant la blockchain dans l'univers IoT que du développement de la recherche fondamentale en cryptographie et architectures distribuées.

[1] Ethereum est un protocole blockchain permettant la création par les utilisateurs de programmes autonomes  (smart contracts)

Enfin, la conception de systèmes autonomes soulève des questions juridiques notamment de responsabilité, de valeur légale des inscriptions[2] et de gouvernance entre les participants.

## La blockchain comme catalyseur

Loin d'une solution prête à l'emploi pour l'IoT, les technologies blockchain apportent aujourd'hui une nouvelle dynamique à la recherche fondamentale et à l'industrie. Des champs anciens ou relativement plus récents, comme les *secure elements*, les preuves formelles ou les *zero knowledge proof,* voient ainsi leur intérêt et financement renouvelés.

Il y sans doute aujourd'hui une part une part d'agitation et d'effets d'annonces. Mais il y a aussi des efforts substantiels destinés au développement et l'adoption d'une nouvelle génération d'architectures. A terme, l'efficacité et la sécurité seront juges des solutions développées.

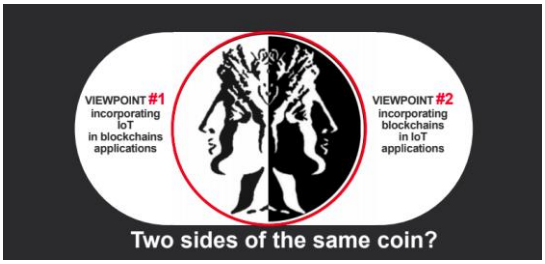
[2] voir Smart Contract: Etudes de cas et analyses juridiques : http://ecan.fr/Smart-Contracts-Etudes.pdf

# Keynote

## Par **Sara Tucci**, Head of Laboratory at CEA List

Le CEA fait de la recherche pointue avec des académiques et s'applique à opérer le passage des innovations vers l'industrie.

### Qu'est-ce que la blockchain peut apporter à l'IoT ?




Des applications blockchain sont développées avec des industriels, et il n'est pas possible, dans ce contexte, de ne pas considérer l'IoT : traçabilité alimentaire, énergie à l'échelle d'un écoquartier, … Il faut toujours remonter des données.

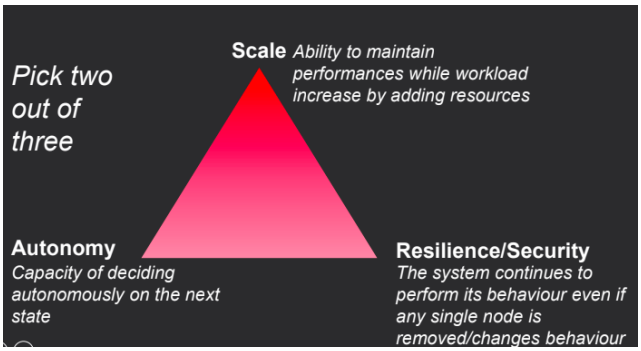
De l'autre point de vue, la blockchain peut servir les systèmes IoT. Elle peut répondre aux problèmes de sécurité, de privacy, à la contamination par des malware. La blockchain peut renforcer la sécurité de ces appareils en permettant l'établissement et la gestion des règles d'accès sur ces appareils.
La blockchain offre une approche décentralisée et permet de détecter des anomalies, donc des intrusions.

Les applications industrielles sont nombreuses : les enregistrements dans le domaine du notariat, les micropaiements par exemple pour des recharges de voitures électriques et le trading d'énergie entre voiture et acheteur (*machine economy*).

De nombreux problèmes qu'on retrouve de manière récurrente dans l'innovation sont reportés sur la blockchain ; par exemple la scalabilité ou encore la sécurité pour laquelle la question reste l'enregistrement effectif des droits et la sécurisation de la politique d'accès.

C'est la théorie du « triangle conjecture » : sur les trois propriétés, on ne peut en choisir que deux.

- Autonomie : les participants ont l'autonomie de décider et de valider les blocs.
- Scalabilité : plus le volume de transactions augmente, plus la charge augmente et donc plus il faut ajouter de ressource de calcul.
- Résilience : le système peut continuer à fonctionner même s'il y a des attaques, il y a différents niveaux de résilience.




La recherche académique étudie ces liens : le committee consensus, le sharding (plus de scalabilité mais moins d'autonomie).
Il faut combiner les technologies, avec le *2nd layer blockchain*. Les protocoles *off chain* ont besoin de se synchroniser.
La recherche montre qu'il faut fédérer les blockchains car elles sont toutes intéressantes et hétérogènes. Il existe

des initiatives : certaines sont plus orientées sur l'intéropérabilité, d'autres sur la sécurité, ...

**Pour le moment, la blockchain n'est pas encore opérationnelle.** Il y a des codes sur github mais il est encore difficile de proposer ces solutions à un industriel. Elles sont opérationnelles pour un POC au maximum.

**Comment faire des applications qui servent le monde industriel ?**
Il faut imaginer un système complet donc faire de l'ingénierie système. Par exemple pour un système smart home, il faut définir une architecture : un ledger privé centralisé, et le *overlay network* (ou réseau superposé) qui permet à des smart home d'interagir ensemble ; à chaque fois on retrouve la question du compromis ou trade off.

Le CEA a travaillé avec Véolia sur les Contrats de Performance Energétique. Les données sont collectées par des capteurs et les données de Météo France. Dans cette architecture il faut qualifier les données, établir des smart contracts, utiliser des algorithmes de voting très spécifiques pour calculer une valeur de confiance aux données. L'utilisateur a la possibilité de voter pour établir la valeur de confiance. Il fallait trouver un trade off acceptable : un smart contract avec un modèle prédictif. Le machine learning a permis d'arriver à un modèle bilinéaire mais ça n'était pas ce que voulait Véolia.

Pour finir, l'IoT et Blockchain ne peuvent pas résoudre tous les problèmes : il faut penser système et trouver les bons arbitrages (*tradeoffs)*. La R&D peut encore progresser. Mais ce qui est certain, c'est la tendance à aller vers des blockchains fédérées et donc interopérables, donc des principes d'architectures. Un domaine de recherche a émergé : l'économie des machines (ou machine economy). Celles-ci prendront des décisions donc il faut changer la manière dont on conçoit les systèmes.

# La blockchain au service de l'IoT (et inversement)

Table-ronde avec **Emmanuel Moyrand**, co-fondateur et Président de Monuma, **Nicolas Bacca**, CTO chez Ledger, **Philippe Nguyen**, Secure IC, **et Sara Tucci**, Head of Lab at CEA List

*Animée par Xavier Lavayssière*

**Monuma**
Monuma a développé une expertise pour certifier toutes les données. La blockchain rempli le rôle de tiers de confiance. Nous utilisons notamment des photos, datées et géolocalisées, qui sont sont ainsi « scellées ». L. La solution repose sur un système blockchain Bitcoin et au bout de la chaîne, un expert agréé réalise un certificat.

Il n'y a plus d'huissier de justice. Les biens peuvent désormais être expertisés et assurés grâce à des photos mais le rôle de l'expert reste essentiel pour faire des rapports d'expertise. Ce que permet Monuma, c'est l'automatisation de l'expertise et le remboursement à 100% en cas de sinistre. Un cas d'usage est par exemple l'état des lieux.

## Secure IC

Secure IC est une société d'une cinquantaine de personnes réparties entre Rennes, Paris et Singapour. La blockchain est l'une des configurations de réseaux possibles pour sécuriser l'IoT.

## Ledger

Il est important de mettre l'accent sur les parties économiques des protocoles, les tokennomics.
Ledger développe des transfuges de la carte à puce. L'objectif est de redonner des possibilités aux utilisateurs.
L'utilisateur est au centre et est capable de vérifier ce qu'il se passe. Le mot d'ordre est « *don't trust, verify* ».
La cryptomonnaie est une occasion de redéfinir l'utilisation de la carte à puces. La blockchain est un ensemble d'écosystèmes complètement ouverts car il faut pouvoir vérifier ce qui se passe.

## Discussion

Au départ de ces sujets on trouve la résolution des problèmes de sécurité. La blockchain est un élément de sécurité, dans son cœur, mais pas en entrée et sortie.. Quelles conséquences est-ce que cet IoT va avoir sur la vie privée et comment la blockchain intervient-elle ?

Beaucoup de choses se développent mais sans prise de conscience des problèmes de privacy. Ceux qui ont des solutions doivent proposer une compatibilité avec les primitives. On doit regarder les cryptoprocesseurs asymétriques. L'enjeu est de comprendre les grandes tendances en termes de contraintes.

Le problème de cœur est la traçabilité de l'information. Qu'en est-il des données personnelles ?
Monuma ne stocke pas la donnée, c'est le client final qui la garde et lui qui gère son dossier.
Ledger réfléchit aux fonctionnalités cryptographiques nouvelles : des algorithmes qui permettent de manipuler les données en préservant l'intégrité du système. Ledger réfléchit à l'implémentation de ces primitives cryptographiques et pour que les techniques arrivent le plus rapidement possible : par exemple des blockchains rattachées à bitcoin, comme Liquid, déployé sur du hardware sécurisé.
Les systèmes de consensus permettent de garantir un certain degré de sécurisation de la blockchain.

Pour autant, il est prouvé que dans certaines situations, on évoque souvent la possession de 51% de la puissance de calcul, alors il est possible de falsifier le système.

Il très difficile de définir la blockchain : « autonomie », « scalabilité » ou encore « publique », « privée », … il n'y a pas de consensus sur la définition de ces termes, ce sont des hypothèses. Le Bitcoin est bien un objet défini mais le reste est un océan de technologies qui se définissent comme « blockchain ».

La question de la protection des dispositifs embarqués contre les attaques physiques n'est pas encore résolue. Comment s'assurer de l'intégrité du fonctionnement du système, notamment de la confidentialité des clés privées, en cas d'attaque physique sur les dispositifs ?

Le passage de ces technologies sur le marché est un premier pas, qui permet de valider le fonctionnement. Le code

est public ; quelqu'un qui casse un code peut partir avec la valeur. Mais dans ce cas, les failles sont identifiées très vite car il y a de l'argent en jeu. Le niveau des attaquants augmente en permanence et sur une blockchain, tout le monde est impacté. Les fabricants sont donc incités à développer des systèmes robustes.

**Est-ce que ça permet de mieux financer la recherche ?**
On a un fort incitatif à créer des blockchains rapidement : un nouvel algorithme intérêt à faire une ICO[3] et récupérer des fonds avant de s'assurer de la rigueur de son fonctionnement ou de sa pertinence.

A l'intersection entre blockchain et IoT, il y a les données de confiance, sur lesquelles il faut un consensus. On arrive à recréer des oracles en associant plusieurs technologies. Par exemple, pour récupérer une donnée externe (comme le prix d'un actif), on peut croiser plusieurs sources. La meilleure façon de prouver des données c'est d'aller chercher des données externes.

**Est-il possible de faire de la cryptographie « légère » c'est-à-dire peu consommatrice de mémoire sur les objets connectés ?**
Le capteur peut décider d'envoyer des informations sur une blockchain et récupérer des droits, une licence et avec une clé représentant l'identité, ... C'est assez simple d'adapter un objet existant pour intégrer ces technologies. Si on le fait dans le capteur lui-même, tout dépend du type de blockchain choisi et des compromis. La synchronisation d'un nœud par exemple dépend de la puissance de calcul disponible. Des compromis peuvent aussi être réalisés en déléguant la partie consensus à des concentrateurs.

Le NIST a publié cette année un rapport sur les mécanismes de cryptographie légère : certains protocoles sont validés pour certaines transactions mais aucun protocole n'a été totalement validé.

Les *secure element* sont déjà très simples et on des déclencheurs cryptographiques. En termes de consommation de batterie et de chauffe, il existe des possibilités très légères, sur les cartes sim des téléphones. Les mécanismes cryptographiques sont abordables à ce niveau.

**Où y'a-t-il le plus de valeur ?** Le marché en est à des cas d'usage très simples. Certains secteurs d'activité comme les vols d'avion sont encore très compliqués : ce sont des marchés très important mais sur lesquels ces solutions sont difficiles à démocratiser.

**Les modèles économiques des services reposant sur la blockchain** suivent ceux du marché du numérique : paiement à l'acte et systèmes d'abonnement.
Dans le cas de Monuma, il s'agit d'un passage vers la prévention dans la garantie des biens de valeur. Les compagnies d'assurance travaillent depuis des années à partir de photos, et Monuma propose une sécurisation grâce à l'horodatage et la géolocalisation de la photo. L'usage principal de la blockchain est d'ailleurs l'horodatage.

[3] Une ICO (Initial Coin Offering) est une méthode de levée de fonds consistant en la vente d'actifs numériques qui représentent un droit ( d'utilisation, financier ...) sur une future plateforme en développement.

Il n'y a pas de modèle économique spécifique à la blockchain, en revanche celle-ci porte une expansion des cryptomonnaies.


La blockchain a du sens lorsque beaucoup d'acteurs sont impliqués : la traçabilité alimentaire pour limiter les fraudes (pas les éliminer, car la blockchain n'est pas un détecteur de mensonge, en revanche elle peut avoir un effet levier sur la qualité de chacun), les voitures avec des processeurs qui doivent s'identifier les uns et l'autres, le trading, le textile,...
Un exemple dans le secteur du textile : des producteurs en Inde font un travail de très bonne qualité du point de vue environnemental mais ils ne peuvent pas procéder à une certification bio. S'ils rentrent sur la blockchain, le modèle économique peut rendre cette certification plus accessible.

Ledger

list
cea tech

Lectures conseillées

- Le white paper du Bitcoin: https://bitcoin.org/bitcoin.pdf
- Mastering Bitcoin d'Andreas Antonopolous, dont une version en Français téléchargeable librement et ses vidéos sur Youtube.

monyma

SECURE IC®
THE TRUSTED COMPUTING COMPANY