CHAIRE AgroTIC

BLOCKCHAIN ET AGRICULTURE

> COMPRENDRE,
> EXPLORER,
> S'INTERROGER

Une étude de la Chaire AgroTIC - Octobre 2017

SOMMAIRE

REMERCIEMENTS

Nous tenons à remercier sincèrement les personnes qui ont accepté de consacrer du temps pour répondre à nos questions :

> **Emmanuel Delerm,** Directeur de projets, Carrefour, Paris
> **Christine Hennebert,** Chercheuse au CEA-LETI, Grenoble
> **Bruno Lauga,** Chef de projet, Service Systèmes d'Information et Méthodologies, ARVALIS - Institut du végétal, Boigneville
> **Nicolas Pauvre,** Chef de projet, et **Paul Bounaud,** Manager Senior Vin Spiritueux et RHD, GS1 France, Paris
> **Nicolas Philippe,** Responsable UT Big Data, Simulation & Blockchain, CATIE, Bordeaux
> **Cyrille Sauvignac,** Responsable Lab Innovation Aquitaine, Atos, Bordeaux
> **Florent Saucède,** Maitre de Conférences Montpellier SupAgro, Montpellier

INTRODUCTION

Blockchain. Pas une semaine sans que ce mot ne fasse l'objet d'un article dans la presse. Le moins que l'on puisse dire, c'est que cela fait le buzz ! Cette technologie permettant la tenue d'un registre de transactions infalsifiable et distribué est même annoncée comme une « révolution » susceptible d'intéresser de nombreux secteurs. Cependant, malgré cette explosion d'intérêt, force est de constater que la blockchain reste une technologie difficile à appréhender...

Cela a en tout cas été le sentiment des membres de la Chaire AgroTIC, chaire d'entreprises dédiée au numérique pour l'Agriculture, curieux de savoir si et comment cette technologie pouvait concerner le secteur agricole. C'est la raison pour laquelle la Chaire AgroTIC a choisi de consacrer sa première étude d'opportunité à la blockchain.

Mais le problème avec la blockchain est que lorsque l'on tire un fil pour en savoir plus, on se retrouve vite avec une pelote ! Aussi, il nous a semblé important de repartir des principes fondamentaux afin de comprendre sur quoi repose la technologie et ce qui la rend si innovante. Notre objectif est toutefois modeste : proposer une synthèse de ce qui se dit et se fait afin de mieux comprendre la technologie et les pistes déjà en cours d'exploration. Mieux informés, nous serons ainsi plus à même de nous projeter dans l'avenir : soit en tant qu'utilisateurs, soit en tant qu'initiateurs de solutions. Des expérimentations et des retours d'expérience devront prolonger cette synthèse afin d'avoir une vision complète de l'opportunité de la technologie.

NOUS PROPOSONS DONC UN DOCUMENT ARTICULÉ EN 3 PARTIES :

« COMPRENDRE »

reprendra les principes fondamentaux de la blockchain, notamment d'un point de vue technique, ce qui nous permettra d'en préciser les propriétés principales.

« EXPLORER LE POTENTIEL »

présentera plusieurs cas d'usage, en portant bien sûr une attention particulière aux applications envisagées dans le secteur agricole.

« S'INTERROGER »

permettra d'aborder des questions qui se posent actuellement par rapport à la blockchain afin de comprendre les éventuels freins et limites et envisager les perspectives d'avenir avec cette technologie.

PARTIE I : Comprendre

1 | La blockchain, de quoi s'agit-il ?

Lorsque l'on cherche la signification de blockchain, on arrive facilement sur ce type de définition :

> « Une blockchain est **un registre de transactions sécurisé** partagé par tous les utilisateurs par Internet ou par un autre réseau **distribué** d'ordinateurs » (Pillington, 2015). **(5)**

> « La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Par extension, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne. » (Blockchain France / Blockchain Partner). **(6)**

Cela est très précis mais... cela mérite néanmoins quelques explications complémentaires...

A LIRE AUSSI :

> La blockchain décryptée les clés d'une révolution - Blockchain France **(1)**

> Comprendre la blockchain - livre blanc Uchange **(2)**

> La blockchain pour les entreprises - MEDEF **(3)**

> Réalités industrielles - Blockchain et smart contracts : des technologies de la confiance ? - Annales des Mines **(4)**

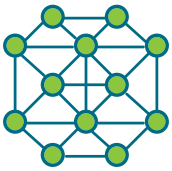
Distinguons d'abord deux nuances par rapport au terme « blockchain » : (2)

> quand on parle de « LA » blockchain, on évoque un type de technologie (en fait **un mix innovant de technologies pré-éxistantes**), fruit des travaux d'un certain Natoshi Sakamoto révélés en 2008, basé entre autres sur la cryptographie.

> quand on parle d'« UNE » blockchain spécifique, on évoque un protocole et un réseau donnés qu'un individu ou une organisation peut utiliser. Bitcoin est une blockchain. Ethereum en est une autre.

REPRENONS MAINTENANT LES TERMES DES DÉFINITIONS POUR BIEN COMPRENDRE CE QUE RECOUVRE « LA » TECHNOLOGIE :

REGISTRE



DISTRIBUÉ, SANS ORGANE CENTRAL DE CONTRÔLE

SÉCURISÉ

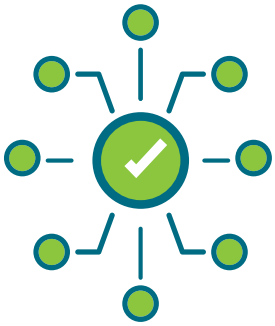
Registre

> Un grand livre (ledger en anglais)

Blockchain : une technologie de « registre », c'est-à-dire qui conserve un historique de transactions

Littéralement, blockchain signifie « chaine de blocs » où les blocs sont des groupes de transactions. En informatique, une transaction est une suite indivisible d'opérations qui permettent de passer d'un état A à un état B. Par exemple, un achat, un paiement, l'envoi d'un message... Une blockchain est donc une base de données dans laquelle sont ajoutées chronologiquement des transactions groupées par blocs. Elle peut être comparée à un registre ou un grand livre de compte, où chaque ligne est une transaction. **La particularité de ce livre est qu'il est écrit à l'encre indélébile :** toutes les pages sont accessibles pour consultation, on peut ajouter des lignes, mais il n'est pas possible d'effacer ou modifier une information précédemment consignée. De plus, ce grand livre est dupliqué à l'identique chez les différents utilisateurs du réseau d'échange.

Blockchain : une technologie basée sur une architecture et une gouvernance distribuées



Centralisée

Décentralisée

UN RÉSEAU PAIR-A-PAIR (P2P OU PEER-TO-PEER)...

Une architecture distribuée est une architecture informatique où les ressources sont réparties en différents endroits. Elles ne s'organisent pas autour d'un serveur central. Une blockchain correspond donc à un réseau d'ordinateurs (où chacun a un rôle de serveur et de client) qui échangent des données entre eux de façon directe, sans passer par un serveur central (c'est le même principe que les outils d'échanges pair-à-pair de contenus multimédia, type eMule par exemple). La blockchain permet donc de se passer **d'organe centralisateur**. Les postes qui constituent le réseau sont appelés des **nœuds.** C'est au niveau de ces nœuds que le registre est répliqué.

...QUI FONCTIONNE SELON UN CONSENSUS DISTRIBUÉ.

Dans un système classique, centralisé, les organes centralisateurs assurent un rôle de tiers de confiance. Ce sont eux qui vérifient que les conditions sont réunies pour assurer les transactions puis qui les exécutent. Mais la centralisation implique une vraie confiance vis-à-vis de l'acteur centralisateur et peut-être source de risques (les attaques sont plus faciles en un seul point), de coûts d'infrastructure et de délais de traitement. Dans un système blockchain, ces intermédiaires n'existent pas. Ce sont les nœuds du réseau qui assurent ce travail de validation et d'exécution. Ils doivent pour cela être d'accord entre eux, au moins pour une majorité, alors qu'a priori ils ne se connaissent pas et ne se font pas confiance. Pour cela, la blockchain fonctionne autour de règles communes reposant sur des mécanismes de consensus (exécutés par des algorithmes). On parle de **consensus distribué :** grâce à eux, la confiance n'est pas détenue par un seul tiers mais répartie au sein du réseau. Il existe différents mécanismes de consensus. Nous y reviendrons.

Blockchain : une technologie sécurisée (notamment) par l'utilisation de principes de cryptographie

Le grand registre qu'est la blockchain est accessible à tous les utilisateurs. Ce qui signifie que la liste des transactions est visible par tous. Cependant, la cryptographie est utilisée pour :

> rendre la chaine inviolable en liant chaque bloc de transactions au précédent => utilisation de fonctions de hachage.

> garantir la signature des transactions => principe d'authentification par cryptographie asymétrique

Voyons ensemble ces 2 principes :

» LES FONCTIONS DE HACHAGE

Les fonctions de hachage, ou hash, sont des algorithmes qui créent une empreinte numérique à partir d'une donnée d'entrée (qui peut être un document entier) : tout comme une empreinte digitale correspond à un unique individu, une empreinte numérique identifie de façon unique une donnée. Le moindre changement dans la donnée d'entrée donnera une empreinte totalement différente.

Exemple : *Comparaison des hash (fonction SHA-256) pour le mot AgroTIC avec et sans point d'exclamation*

AgroTIC => 842ef466771f1af6ea4c24824512cde129bf4c6281674424f0b0254b27d054ea
AgroTIC! => 5792a4c098aa14eac06d640fa333fe2a9ec719203bd8392e6851bec55acdf622

Cette fonction de hachage fonctionne en sens unique. A partir du hash obtenu, il n'est pas possible de remonter à la donnée d'origine.

C'est grâce à ces fonctions que le « grand livre » n'est pas modifiable.
En effet, chaque bloc de la chaîne est constitué d'un en-tête et des nouvelles transactions. Dans **l'en-tête** du bloc est stockée une **empreinte numérique** constituant un « condensé » des transactions du bloc (la racine de l' « arbre des transactions » ou arbre de Merkle). Chaque bloc est lié au précédent grâce à un hash calculé à partir de l'en-tête du bloc précédent : ainsi, chaque bloc contient une empreinte d'une partie du bloc précédent, de telle sorte qu'une modification même infime de l'une des transactions après son inscription, entraîne une modification de l'ensemble de la chaîne. Or cette chaîne étant dupliquée en de multiples copies, tout changement peut être remarqué. Et compte tenu du nombre de copies et du principe de consensus distribué, il est difficile de reporter l'anomalie sur tous les exemplaires de la chaîne. Chaque bloc ajouté sécurise ainsi un peu plus la chaîne. C'est ce qui fait qu'une blockchain apparaît comme infalsifiable.

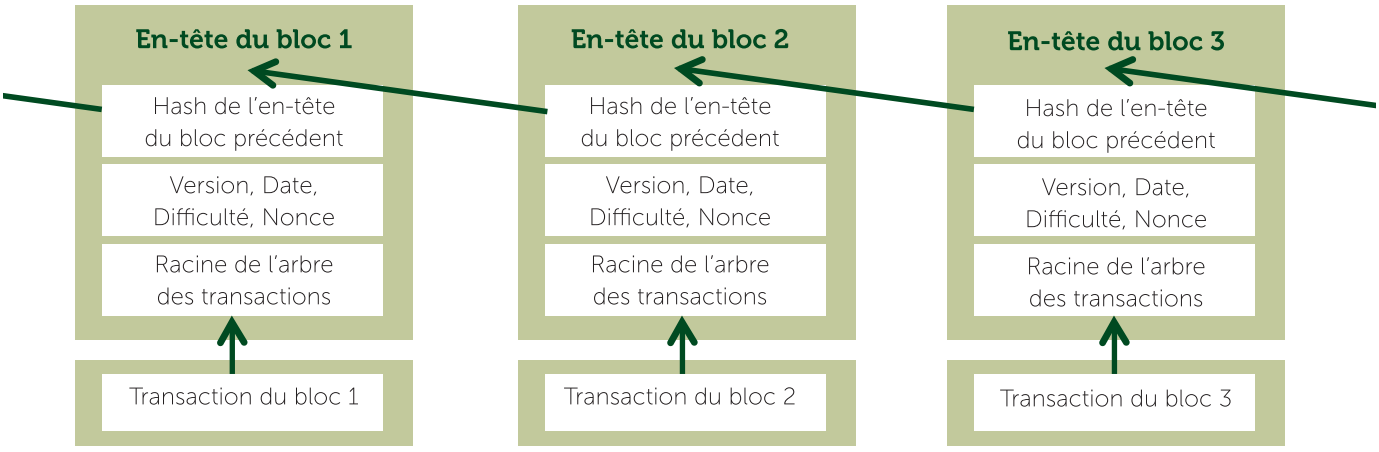
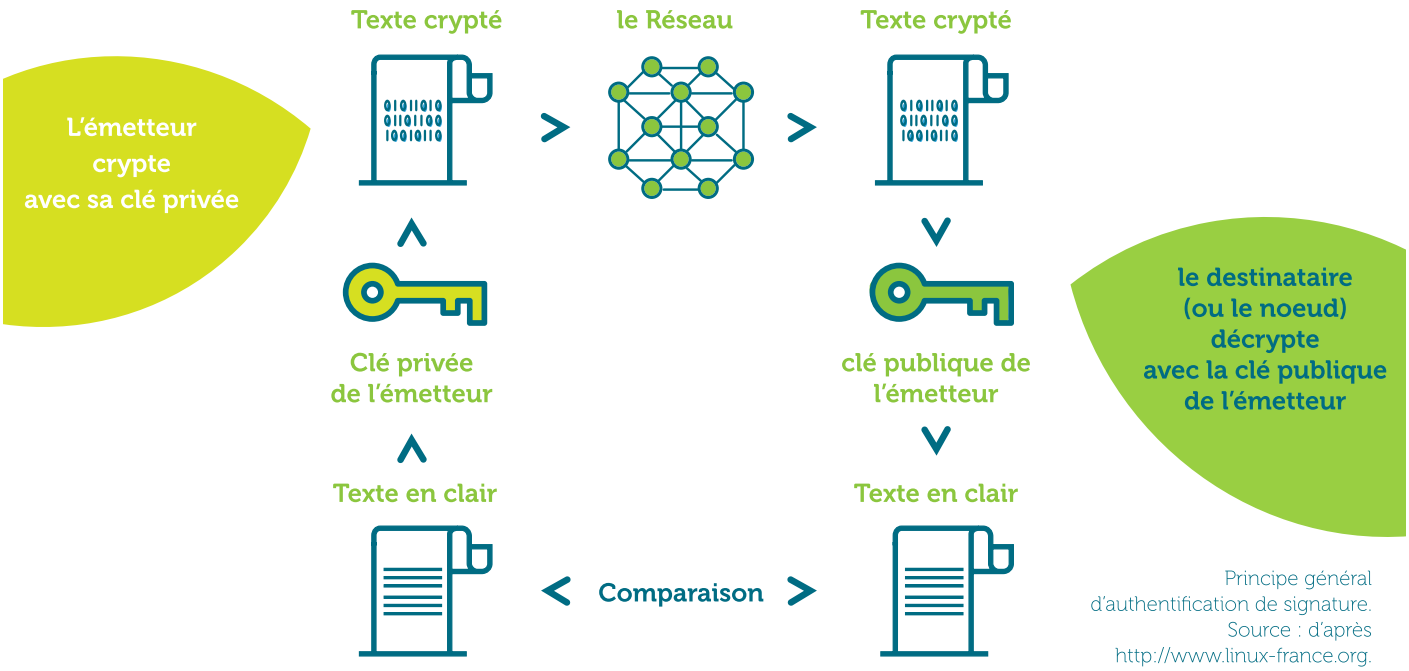


Schéma simplifié d'une blockchain (type Bitcoin) (Source : www.ethereum-france.com)

LA CRYPTOGRAPHIE ASYMÉTRIQUE

Il s'agit d'une méthode de chiffrement permettant soit de garantir la confidentialité d'une transmission de donnée entre 2 utilisateurs, soit de garantir l'authenticité d'une signature d'un message sans qu'un code secret ne soit partagé par ces 2 utilisateurs. Elle repose sur l'utilisation de 2 clés liées entre elles, l'une privée et l'autre publique. La clé privée est une clé personnelle qui ne doit être communiquée à personne. La clé publique est celle qui est communiquée à l'ensemble du réseau (l'« adresse » d'un utilisateur à laquelle on peut envoyer des transactions est d'ailleurs calculée à partir de sa clé publique).



Principe général d'authentification de signature. Source : d'après http://www.linux-france.org.

Dans le cas de la blockchain, ce mécanisme vise à garantir l'authenticité d'une signature.
Ainsi, pour pouvoir initier une transaction entre Alice et Bob, Alice doit utiliser sa clé privée pour « signer numériquement » son message (lequel peut correspondre par exemple à « je donne 200 unités monétaires à Bob ») :

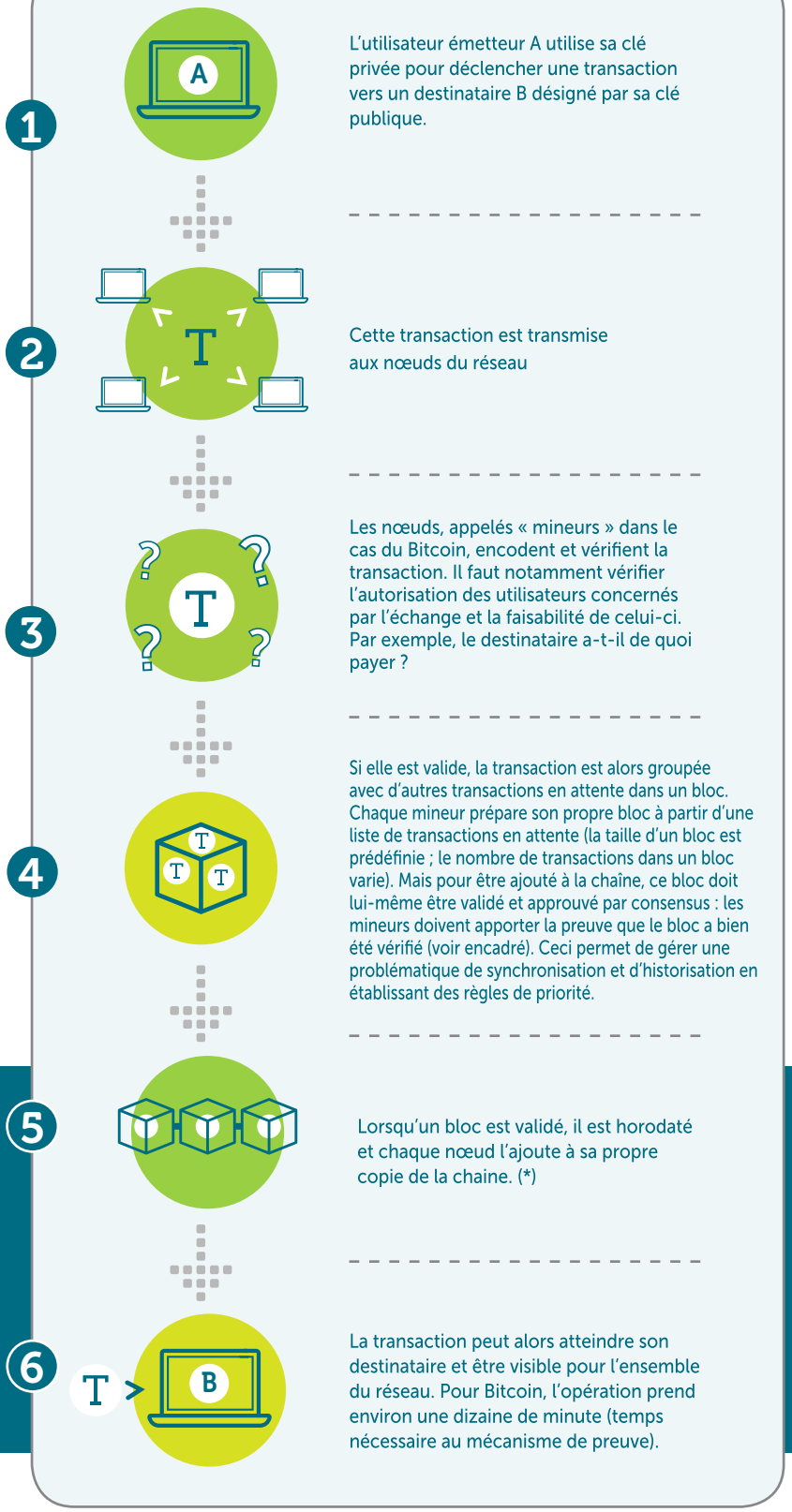
> *Elle associe en fait à son message en clair une signature correspondant à « l'empreinte numérique » du message en clair, empreinte ensuite cryptée par une fonction de chiffrement utilisant sa clé privée.*

Les nœuds du réseau seront sûrs que le message a bien été produit par Alice s'ils réussissent à déchiffrer la signature grâce à sa clé publique.

> *Plus précisément, la transaction sera authentifiée si les utilisateurs parviennent à décrypter la signature numérique d'Alice à l'aide de sa clé publique et à établir une égalité entre cette signature décryptée et l'empreinte du message en clair.*

2 | Comment ça marche ?

Afin de comprendre comment tout cela s'articule concrètement, prenons l'exemple de la première blockchain réellement mise en œuvre à l'échelle mondiale : **le Bitcoin**.



Créé en 2009, Bitcoin est une monnaie numérique ou « crypto-monnaie » qui permet des paiements de pair à pair (achats de biens et services mais, aujourd'hui, également échanges contre des devises monétaires physiques...). Bitcoin fonctionne selon un protocole libre (code source ouvert) qui permet aux utilisateurs d'émettre des bitcoins et de gérer des transactions de façon collective et automatique, avec une interopérabilité des logiciels et services qui l'utilisent. Le bitcoin est à la fois un intermédiaire de paiement et une réserve de valeur limitée à 21 millions d'unités (le bitcoin est également le nom de l'unité) **(7)**. La Blockchain Bitcoin retrace l'intégralité des transactions depuis sa création. Comme toutes les crypto-monnaies, Bitcoin n'a pas de valeur réelle sous-jacente : elle n'a de valeur que sur Internet et repose donc sur un mécanisme spéculatif.

(*) A noter : il arrive que du fait du temps de synchronisation entre les nœuds, deux nœuds diffusent leur version de bloc simultanément. Dans ce cas, la chaîne peut temporairement compter deux branches différentes. Chaque nœud continue alors à travailler sur la base du bloc reçu en premier mais garde l'autre en attente. Dès qu'un bloc suivant est ajouté, c'est la branche devenue la plus longue qui devient légitime et l'autre est abandonnée.

PREUVE DE TRAVAIL ET AUTRES MÉCANISMES DE CONSENSUS

Dans un système décentralisé, sans tiers de confiance, où il n'existe donc pas a priori de confiance entre chaque individu, les mécanismes de **consensus** sont indispensables. Pour fonctionner ensemble, les utilisateurs du réseau doivent utiliser des règles acceptées par tous, permettant de mettre d'accord le plus grand nombre tout en s'assurant que ceux qui participent aux choix sont bien légitimes (et non animés d'intentions malveillantes).

Dans le réseau bitcoin, le consensus utilisé pour la validation des blocs est basé sur **la preuve de travail « Proof-of-work »** : il s'agit d'apporter la preuve que l'on se donne du mal pour vérifier les transactions **(8)**. Ce mécanisme réclame une telle puissance de calcul pour la validation de chaque bloc qu'il dissuade des attaques malveillantes et rend quasiment impossible la réécriture de l'historique de la chaîne.

Comme chaque mineur prépare son bloc, il est nécessaire de sélectionner celui qui sera ajouté à la chaîne. La règle est donc la suivante : le mineur qui pourra ajouter le bloc est le premier qui aura résolu un problème mathématique complexe. Par exemple, il peut s'agir de trouver une valeur aléatoire à ajouter à (ou plutôt à concaténer avec) l'en-tête de bloc précédent pour obtenir un hash inférieur à un certain seuil (le hash doit commencer pour cela par une série de 0, ce qui nécessite de nombreux essais). Les problèmes sont de plus en plus complexes au fil de l'évolution de la blockchain mais la solution, elle, est toujours facilement contrôlable. Ainsi, le bloc sera validé si plus de 50% des nœuds agréent le résultat.

Compte tenu de l'importante puissance de calcul requise, il s'agit plutôt aujourd'hui d'une affaire de spécialistes. Les mineurs sont rémunérés pour ce travail en recevant des **tokens** (jetons correspondant à une fraction de la crypto-monnaie), ce qui les incite à entretenir le réseau. D'où le terme « **minage** » faisant référence aux chercheurs d'or qui pouvaient s'enrichir par leur travail...

Ce mécanisme de preuve de travail est propre aux premières blockchains mais d'autres processus de consensus sont également utilisés **(voir (9))**. On parle notamment beaucoup de **Preuve d'enjeu « Proof-of-state »**, processus bien moins consommateur en calcul, donc en énergie, où les mineurs (alors appelés **Minters**) obtiennent le droit de validation des blocs en mettant en jeu des unités de crypto-monnaies. Plus ils en possèdent, plus ils ont de chance d'être désignés par les algorithmes.

Mais notons bien que toutes les blockchains n'ont pas besoin de ces mécanismes relativement complexes. Ainsi, nous verrons que certaines blockchains sont privées ou contrôlées par un nombre restreint d'opérateurs. Le problème de confiance étant alors moindre, les mécanismes de validation sont bien plus simples et de coût énergétique faible. Il suffit parfois simplement que le bloc soit approuvé par X des N nœuds pour qu'il soit considéré valide (par exemple par un simple système de vote). Ou bien encore que certains nœuds soient désignés contractuellement responsables de la validation.

Grâce à tout cela, la blockchain présente donc les caractéristiques suivantes :

☑ L'HISTORISATION

Les transactions sont ajoutées chronologiquement : elles sont horodatées et liées entre elles.

☑ L'IMMUABILITÉ DES DONNÉES INSCRITES

La base est répliquée en de multiples copies et la moindre modification modifie l'intégralité de la chaine.

☑ LA DÉSINTERMÉDIATION ET LA DÉCENTRALISATION

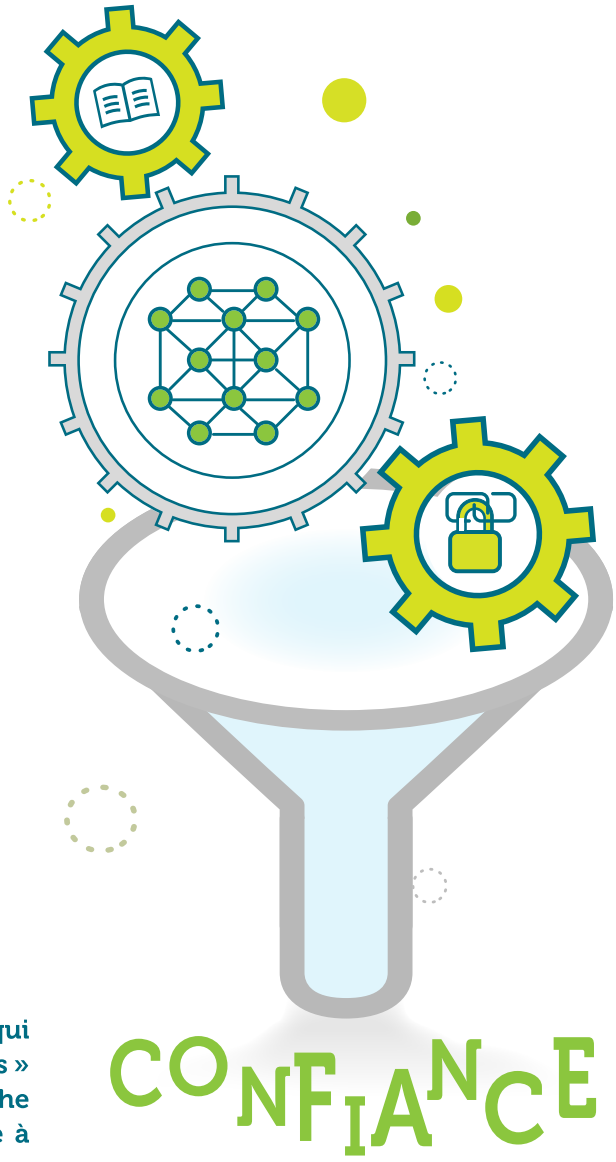
Le fonctionnement en réseau pair-à-pair permet de se passer d'un organe central.

☑ LA SÉCURITÉ

Le caractère distribué et les mécanismes de consensus rendent les attaques plus difficiles. La signature numérique garantit l'origine des transactions.

☑ LA TRANSPARENCE

Les nœuds possèdent l'intégralité de la chaine et peuvent accéder aux transactions.



La blockchain est donc avant tout une technologie qui « garantit la sincérité et la validité de tout type d'échanges » (10). Pour reprendre l'expression du magazine The Economist (31 oct/6 nov 2015), elle est une « machine à confiance ».

On retient :

- La blockchain permet la tenue d'un registre sécurisé et distribué de transactions. Elle repose sur deux piliers technologiques, la cryptographie et une architecture pair-à-pair, qui lui permettent de garantir un haut niveau de sécurité et le caractère infalsifiable des données.
- Elle repose également sur un mode de gouvernance collaboratif impliquant des mécanismes de consensus. Elle promet ainsi la désintermédiation c'est-à-dire l'absence d'autorité centrale.
- Par les mécanismes qu'elle met en œuvre, basés sur le partage et la transparence des informations, la blockchain est vue comme une machine à créer de la confiance.

3 | De la blockchain aux blockchains (ou technologies de registres distribués)

Nous l'avons vu, au départ, la blockchain correspond à une base de données distribuée et sécurisée. A ce titre, elle peut assurer un stockage (registre) et des échanges de données (comme des paiements). Mais rapidement, d'autres protocoles ont fait leur apparition pour répondre à de nouveaux besoins. Ils ont apporté de nouvelles fonctionnalités mais aussi d'autres façons d'appréhender la gouvernance.

Ainsi, on est passé de « la blockchain » à « des blockchains ». Les puristes vis-à-vis du concept originel de blockchain parlent alors de façon plus générique des technologies de registres distribués : « Ditributed Ledger Technologies » (DLT).

» UNE ÉVOLUTION DE FONCTIONNALITÉ MAJEURE : LES SMART CONTRACTS.

Les smart contracts sont des programmes autonomes (donc des codes informatiques) qui exécutent automatiquement les conditions et termes d'un contrat, en fonction de paramètres déterminés à l'avance, sans nécessiter d'intervention humaine une fois démarrés (Blockchain France, 2015). Les conditions et les modalités d'exécution du contrat sont inscrites dans la blockchain : elles sont donc immuables.

Là encore, il ne s'agit pas d'une notion nouvelle (le terme a été utilisé dès 1993 par l'informaticien Nick Szabo) mais c'est le développement du réseau Ethereum qui lui a donné une bien plus grande ampleur en l'associant à une crypto-monnaie (l'Ether dans le cas d'Ethereum) permettant par exemple le transfert entièrement automatisé et sécurisé d'actifs.

Ces smart contracts ouvrent de nouvelles perspectives : **en effet, associés aux objets connectés, ils peuvent établir un lien sécurisé entre virtuel et réel.** Ainsi, un capteur peut collecter une information qui, une fois transmise, constitue le déclencheur d'une série d'actions automatiques, prévues à l'avance dans un smart contract (par exemple un paiement est déclenché dès qu'il est prouvé par géolocalisation qu'un colis a atteint une destination).

» DES ÉVOLUTIONS DE GOUVERNANCE : VERS DES BLOCKCHAINS PRIVÉES

Le caractère totalement ouvert et transparent tel qu'appliqué dans Bitcoin fait la grande originalité de la blockchain. Toutefois, ce principe a vite rencontré ses détracteurs peu enclins à tout partager et à devoir tout décider en commun. Très vite, des blockchains moins ouvertes sont apparues.

Schématiquement, 3 grands types de blockchain sont distinguées **(11)**

> Les Blockchains publiques (ou « non permissionnées ») :

Tout le monde peut valider des transactions et participer au processus de consensus.
Tout le monde peut envoyer des transactions afin qu'elles soient validées et intégrées à la blockchain si elles sont correctes.
Tout le monde peut accéder à la consultation des transactions.
Ce type de blockchain est réellement décentralisé, ce qui permet des coûts d'infrastructure réduits pour un utilisateur donné puisque partagés par l'ensemble du réseau (il n'y a pas de serveurs à maintenir par exemple). Une crypto-monnaie y est étroitement liée de façon à entretenir le réseau par incitation économique. Par contre, ce type de blockchain est difficile à faire évoluer car il faut que tous les acteurs soient d'accord.

Exemples : Bitcoin, Ethereum, Litecoin...

> Les Blockchains de consortium

Le processus de consensus est assuré par des nœuds pré-sélectionnés (comme un consortium d'établissements bancaires qui se mettent d'accord sur des règles communes). Les transactions peuvent être accessibles à tous ou restreintes aux participants du réseau ou encore accessibles partiellement.

Ces blockchains sont considérées comme partiellement décentralisées.

> Les blockchain privées (ou « permissionnées »)

Elles sont détenues par une organisation donnée qui en régit totalement les droits d'écriture et de consultation. De fait, elles sont régulées et règlementées, ce qui va à l'encontre de l'idée originelle de Bitcoin et amènent les puristes à leur refuser l'appellation « blockchain ». Elles ne nécessitent pas de crypto-monnaie associée ni de mécanismes de type preuve de travail ou d'enjeu. Des caractéristiques de la blockchain, elles gardent essentiellement l'immuabilité par le caractère distribué et les principes d'authentification cryptographiques.

Chaque type a ses avantages et inconvénients. Elles peuvent s'adresser à des contextes différents. Par exemple, les blockchains publiques s'adaptent bien aux usages consommateurs à consommateurs (CtoC) tandis que les privées vont plus facilement concerner des usages d'entreprise à entreprise (BtoB : business to business).
Les blockchains privées sont encore souvent le moyen pour les entreprises d'expérimenter la technologie à moindre impact mais il est probable qu'à terme les blockchains des différents types cohabiteront et interopèreront. Ceci existe d'ailleurs déjà : **des sideschains** permettent d'établir des passerelles entre différentes blockchains.

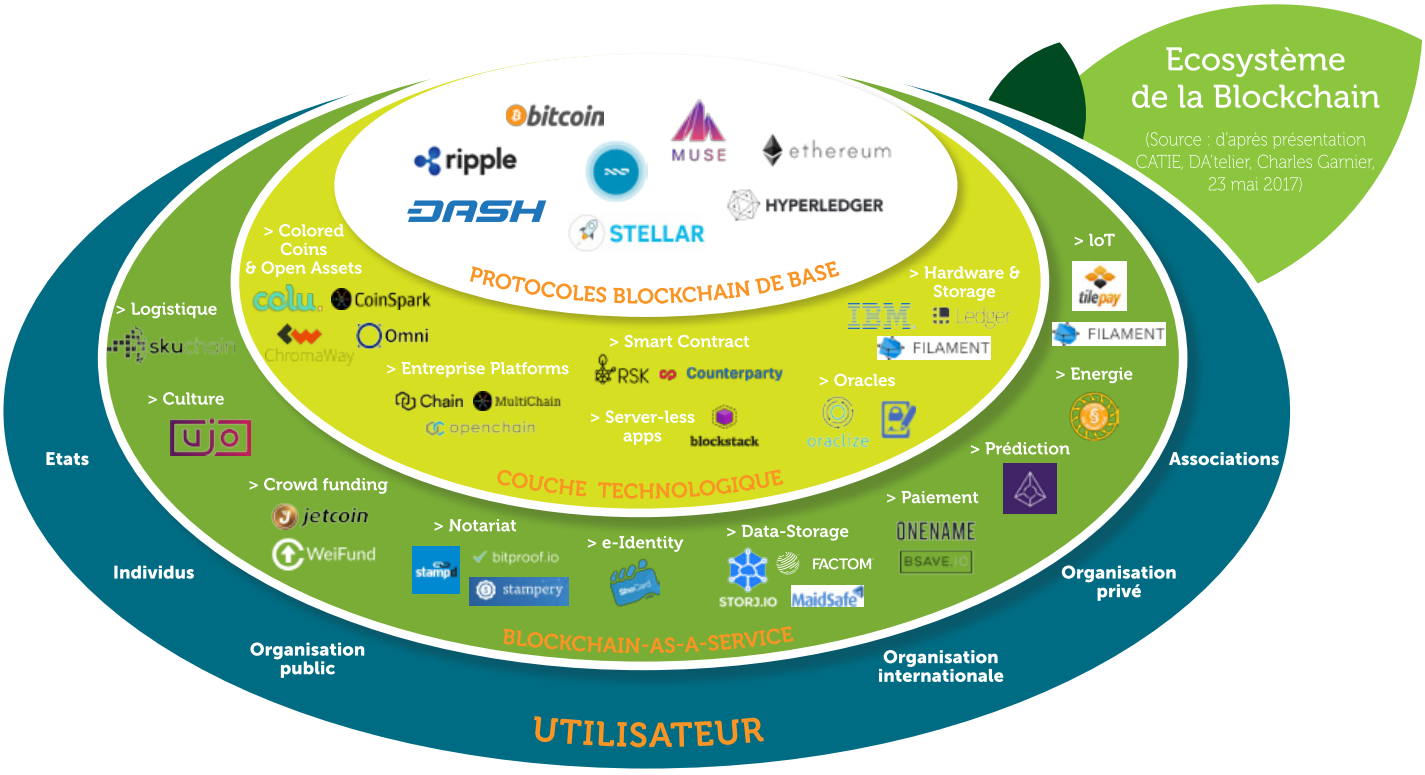
DES ÉVOLUTIONS EN TERMES DE DÉVELOPPEMENT DE SERVICES : VERS UN ÉCOSYSTÈME BLOCKCHAIN

> La blockchain s'organise sur une architecture en couches, exactement comme internet :

Une **couche d' « infrastucture »** : c'est la « base de donnée » distribuée, la chaîne de blocs elle-même, et le réseau dans lequel elle est répliquée.
Cette couche d'infrastructure est surmontée d'un niveau de **« protocole »** : un ensemble de règles que suit la blockchain, telles les règles de vérification et de validation des transactions...

Une **couche « technologique »** : c'est la couche intermédiaire qui propose des services permettant de traiter les informations de la blockchain pour les mettre à disposition d'applications.

Une **couche applicative** : ce sont les applications qui interagissent avec les utilisateurs. A ce niveau, la blockchain est transparente pour l'utilisateur. C'est le niveau : « Blockchain-as-a-service » (Baas).



Selon son besoin, une entreprise a le choix entre différentes options pour mettre en œuvre une technologie blockchain (**voir (12), figure ci-dessous**) dont celle consistant à utiliser une plateforme de développement.

APPROCHE	COMMENT CELA EST FAIT	EXEMPLE
Services informatiques	Nous faisons pour vous	Grandes Entreprises de Services Numériques
Blockchain d'abord	Vous travaillez directement avec les outils et les services des blockchains	Bitcoin, Ethereum
Plateformes de développement	Outils pour les professionnels de l'informatique	BlockApps, Blockstream, Eris, EthCore, Hyperledger, Tendermint
Solutions verticales	Destinées à l'industrie	Axoni, Chain, Cleamatics, DAH, itBit, R3
API et surcouches spécifiques	Briques de construction « pour faire soi-même »	Blockstack, Factom, open Assets, Tierion

Source : William Mougayar, 2016, www.coindesk.com (traduit de l'anglais)

A terme, l'écosystème va probablement se structurer autour des sociétés de services développant la couche technologique d'une part et les entreprises développant les applications métiers d'autre part.

Pour les premières, comme les gros opérateurs tels IBM ou Microsoft, l'enjeu est de réussir à imposer leur environnement de services permettant aux entreprises de créer, déployer, faire fonctionner et assurer la surveillance d'applications basées sur des blockchains. Ainsi, IBM développe ses services autour d'*HyperLedger* de Linux Fondation. Microsoft mise sur sa plateforme *Azure* et Orange sur *Chain*.

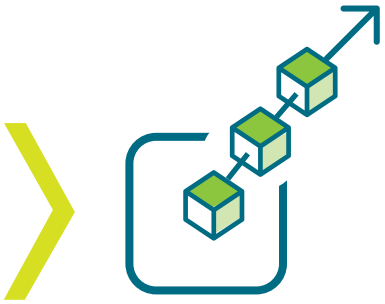
Pour les entreprises développant les applications métiers, l'enjeu est d'être celle qui pourra proposer la « killer app », l'application qui permettra l'adoption massive de la technologie blockchain.

On retient :

- Il n'existe pas un type de blockchain mais des blockchains dont les caractéristiques et les fonctionnalités varient.
- Les smart contracts, codes informatiques s'exécutant de façon autonome, apportent une valeur ajoutée par rapport au seul principe de base de données distribuée : ils laissent envisager de connecter le réel et le virtuel.
- Des blockchains privées existent aujourd'hui. Elles s'éloignent de la philosophie originelle d'un système entièrement géré par ses utilisateurs.
- La blockchain nourrit déjà un véritable écosystème d'acteurs et de solutions.

4 | Pourquoi la blockchain suscite-t-elle tant d'intérêt ?

LA BLOCKCHAIN SUSCITE UNE ATTENTION PARTICULIÈRE CAR IL S'AGIT D'UNE TECHNOLOGIE QUE L'ON ANNONCE **DISRUPTIVE**.



La blockchain, en particulier la blockchain publique, porte un grand potentiel de transformation et implique des changements de paradigmes :

> **Elle réinvente la confiance.** En permettant de s'affranchir d'un organe centralisateur et en reposant sur la transparence et le consensus distribué, elle change la façon d'accorder sa confiance (voir le « talk pédagogique » de Claire Balva au TEDxLyon à ce sujet **(13)**).
Jusqu'ici nos modes de fonctionnement sont régis par le fait de déléguer sa confiance à un tiers : un banquier, un notaire, un organisme de certification, un état... Mais ces tiers sont faillibles, peuvent subir des attaques de sécurité, peuvent décider du jour au lendemain de changer les règles... La blockchain « réinvente la confiance » en la distribuant : ce n'est pas qu'un organe qui valide et exécute, c'est tout un collectif. Au lieu de faire confiance à un organisme, on reporte la confiance sur une technologie (et sur les mathématiques !).

> **Elle permet une mutualisation du risque :** là encore parce qu'elle permet que le risque ne soit pas concentré sur un intermédiaire mais partagé par tous.

> Parce qu'elle implique mutualisation des moyens, transparence, décentralisation, elle pose des fonctionnements **d'économie collaborative ou de partage.** Les cryptomonnaies qui existent indépendamment des états et des banques sont l'une des manifestations mais ce ne sont pas les seules. Par son fonctionnement basé sur un réseau peer-to-peer, la blockchain laisse envisager de pousser encore un cran plus loin l' « ubérisation », ce phénomène qui permettait déjà de mettre en contact direct des professionnels et des clients. En effet, la blockchain permet de se passer de la plateforme de mise à disposition des services. Elle permet d'échanger de façon sécurisée avec son voisin n'importe quelle unité de valeur : c'est le phénomène de « tokenisation », du terme « token » ou jeton (un token peut correspondre à un actif, à une unité de production mais également à des choses immatérielles comme du temps, un droit de vote, une réputation...).**(14)**

> Dès lors, **elle réinvente les jeux d'acteurs et donc de pouvoir...** Dans les blockchains privées ou de consortium, les « rapports de force » entre les acteurs qui vont proposer l'adoption de la technologie et les partenaires qui vont y adhérer devront probablement respecter un équilibre subtil. « Il faut un mode de coordination mixte, fait de pouvoir sans abus et de confiance sans aveuglement. Ce genre de dispositif est complexe à mettre en œuvre». **(15)** Dans les blockchains publiques, les membres de la communauté ont un pouvoir énorme mais également des responsabilités. « S'il n'y a pas d'autorité centrale capable d'appliquer la loi, la communauté blockchain a l'obligation morale ou la responsabilité d'intervenir pour faire respecter l'intention de la loi (ou du code, en l'occurrence) de façon à préserver l'ordre public et la morale. C'est exactement ce qu'implique la ''gouvernance distribuée''. » (Primavera de Filippi, citée par Blockchain France, 2016) **(16)**

Evidemment cela suscite beaucoup de questions, qui font travailler actuellement les chercheurs de multiples disciplines : des questions technologiques bien sûr, mais également juridiques (de responsabilité et de réglementation), politiques (rôle des états), sociétales, écologiques, etc.

Si la blockchain a rapidement intéressé les milieux financiers du fait de la notion de cryptomonnaie et la possibilité de transferts d'actifs, elle est en fait susceptible d'intéresser tous les secteurs d'activité.

Aussi, après ce premier aperçu de la technologie, intéressons-nous maintenant aux cas d'usage et aux applications, en particulier pour le monde agricole.

On retient :

- La technologie blockchain est dite disruptive par les changements de paradigmes qu'elle implique en termes de confiance, de jeux d'acteurs et de pouvoir.
- Elle pose des questions, notamment des questions de recherche, dans de nombreux domaines : technologie, économie, société, politique, juridique, écologie...

PARTIE II :
Explorer le potentiel

1 Des promesses aux cas d'usage

Nous l'avons vu précédemment, les principales caractéristiques de la blockchain sont :

- L'HISTORISATION
- L'IMMUABILITÉ DES DONNÉES INSCRITES
- LA DÉSINTERMÉDIATION ET LA DÉCENTRALISATION
- LA SÉCURITÉ
- LA TRANSPARENCE

La blockchain peut donc être synonyme de valeur ajoutée dès lors qu'il s'agit de gagner :

> de la confiance par la fiabilité des données, la sécurisation du système ou sa transparence,

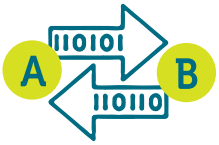
> du temps et de l'argent par la décentralisation de l'infrastructure*, l'automatisation et la simplification des procédures.

* Associée à une cryptomonnaie, une blockchain présente une autonomie de fonctionnement : en effet, comme pour le Bitcoin, les coûts sont répartis sur les nœuds du réseau et les acteurs rémunérés par création de valeur en interne. Ceci laisse envisager des réductions de coûts d'infrastructure.

Actuellement, les cas d'usage peuvent être classés en 3 grandes familles (6) (17) :

Tenues de registre

Stockage de données, d'information dont on souhaite garantir la preuve d'existence, l'historique, la propriété, l'origine, etc.



Transactions digitales

Transfert d'unités de valeur : cryptomonnaies, transactions immobilières, cofinancement, achats/ventes, votes, etc.

Smart-contracts

Développement et stockage de smart-contracts qui permettent d'exécuter automatiquement des conditions inscrites de façon non modifiable dans la blockchain.

Mais cette vision est déjà probablement réductrice et en vérité, il serait dommage de brider son imagination...

2 | Des exemples tous secteurs

Le secteur financier a vite été attiré par le potentiel de la blockchain et il est sans doute celui qui a le plus massivement investi sur des preuves de concept (ce stade est encore rarement dépassé) pour la gestion des titres, le financement du commerce international ou le financement privé. Mais il n'est pas le seul : d'après un sondage réalisé par le MEDEF en mai 2017 auprès de 302 entreprises françaises de toutes tailles et de tous secteurs d'activité, 66 % des décideurs s'intéressent au sujet blockchain **(3)**. En 2016, les investissements mondiaux sur le sujet ont représenté 694 millions de $ (Source : baromètre blockchain, TNP & Largillière Finance). Nous proposons ci-après un rapide tour d'horizon de cas d'usage destiné à montrer la variété des domaines d'application...

CERTIFICATION DE DIPLÔMES

L'école Supérieure d'Ingénieurs Léonard de Vinci (Paris) et l'Ecole Supérieure des Sciences Economiques et Sociales (ESSEC) ont mis en place un partenariat avec la société Paymium pour proposer le service diploma.report permettant de certifier les diplômes qu'elles délivrent. L'école numérise le diplôme, une empreinte numérique du diplôme est produite, une transaction est inscrite dans la blockchain en guise d'attestation de la délivrance du diplôme par l'école. Une entreprise peut ainsi recevoir la version numérique du diplôme, vérifier qu'elle n'a pas été modifiée grâce à la comparaison du hash, et vérifier grâce à l'exploration de la blockchain que l'école est bien à l'origine du diplôme.

PRODUCTION D'ÉLECTRICITÉ

SolarCoin, est une cryptomonaie qui permet aux auto-producteurs d'électricité de recevoir des SolarCoin en fonction de l'électricité que l'installation photovoltaïque génère. Par exemple, 1 SolarCoin récompense la production d'1 MWh et est convertible dans la plupart des devises. En France, ekWateur, fournisseur d'énergie verte, accepte les SolarCoin en échange d'énergie.

En matière d'échanges plus directs d'énergie solaire entre voisins, des expérimentations sont en cours à l'échelle de quartier : comme avec le projet TransActiveGrid à Brooklyn ou le projet de Bouygues Immobilier avec Microsoft, Energisme et Stratum, dans le quartier Confluences à Lyon.

DROITS D'AUTEURS / PROPRIÉTÉ INTELLECTUELLE

Plusieurs applications utilisent la blockchain pour protéger la paternité d'une œuvre et/ou rémunérer les auteurs directement (Monegraph, Verisart, Muse Blockchain). En mai 2017, la plateforme de streaming musical Spotify, régulièrement prise en faute pour des problèmes de mauvaise rémunération des ayant-droit, a annoncé le rachat de la start-up Mediachain, spécialisée dans le développement de solutions de protection des contenus numeriques en ligne. Mediachain utilise la blockchain Ethereum pour authentifier l'auteur des œuvres.

COOPÉRATIVE DE DÉVELOPPEMENT D'APPLICATIONS

Les Digiculteurs sont un groupement coopératif d'entreprises de la filière numérique initié par le Crédit Agricole. Le Crédit Agricole ouvre ses données, forcément sensibles puisque bancaires, aux entreprises de ce groupement pour favoriser les créations d'applications innovantes. Les digiculteurs sont rémunérés selon un système original puisque la rémunération dépend de l'utilisation mensuelle des applications. Ceci permet un revenu sur le long terme aux digiculteurs et les incitent à améliorer en continu les applications. Etant donné qu'il s'agit de petites sommes, le système s'appuie sur un paiement en bitcoins, ce qui permet au Crédit Agricole de monter en compétence

COVOITURAGE

LaZooz propose un service de réservation de covoiturage basé sur une plateforme autogérée. Les chauffeurs sont rémunérés grâce à une cryptomonnaie (le Zooz basé sur Bitcoin).

VOTE ÉLECTRONIQUE

FollowMyVote, start-up américaine, propose un service qui permet d'enregistrer les votes et grâce au registre et au travail de vérification des nœuds, de vérifier que les votants ont le droit de voter et n'ont pas voté plusieurs fois.

STOCKAGE CLOUD

Filecoin propose une alternative au stockage de type DropBox utilisant des datacenters. Elle propose un stockage de fichiers décentralisé : les données sont cryptées et distribuées sur les différents nœuds du réseau. Des mineurs gagnent des Filecoin en fournissant de l'espace disque. Chaque client peut adapter les paramètres de réplication des données en fonction du niveau de sécurité, de la rapidité d'accès et du coût souhaités.

INTERNET DES OBJETS

Slock-it : Leur slogan: « louez, vendez ou partagez tout ce que vous voulez ». Il s'agit de lier les objets physiques avec la blockchain Ethereum, pour que des smart contracts puissent interagir avec eux. L'entreprise donne l'exemple de la location d'appartement : la serrure de la porte d'entrée pourrait être liée à la blockchain et un smart contract pourrait permettre l'ouverture si les conditions de paiement de la location sont remplies. Slock-it met en avant la plus-value de la blockchain par le fait que contrairement à d'autres systèmes, la blockchain ne peut pas tomber en panne ou être soumise à la volonté d'un tiers. La réduction des coûts est également avancée **(19)**

Filament : travaille sur un réseau sans-fil longue portée pour les objets connectés basé sur le principe de blockchain. L'idée est de proposer un protocole (Blocklet) permettant aux objets connectés d'interagir entre eux, la blockchain permettant seulement de vérifier les entrées et sorties.

Iota : cette application promettant une solution pour relier les objets connectés est en fait déjà une extension du principe de blockchain (une vision 2.0) puisque les blocs de transactions ne sont pas liés en chaine mais plutôt en arbre. Le système ne repose pas sur une incitation économique (ce qui permet d'alléger les coûts). Les nœuds ne sont pas rémunérés pour leur travail de validation de transaction : ils doivent en valider deux avant de pouvoir en initier une.

3 | Des exemples dans le secteur agricole

Nous présentons ici un panorama (non exhaustif) des cas d'usage agricoles illustrés dans la presse ou des articles scientifiques. Ces cas constituent une illustration des pistes de réflexion, des domaines où la blockchain peut être une technologie d'intérêt en réponse à certains enjeux. Cela nous permettra d'appréhender différentes questions associées. Cependant, précisons qu'à l'heure actuelle, ces exemples ne sont probablement pas exempts d'un certain effet d'annonce et relèvent tous ou presque de projets pilotes ou de simples preuves de concept (Proof-Of-Concept ou POC)...

A LIRE AUSSI :

« Agriculture, agroalimentaire et blockchain », une étude réalisée par Blockchain Partner - **(20)**

CAS D'USAGE 1 : TRAÇABILITÉ ET TRANSPARENCE DE LA CHAÎNE D'APPROVISIONNEMENT (SUPPLY CHAIN)

LE CONTEXTE :

Les scandales alimentaires et crises sanitaires qui ont jalonné l'actualité depuis les années 80 ainsi que l'augmentation de certains problèmes de santé tels que ceux liés à l'obésité ont mis à mal la relation de confiance entre consommateurs d'une part et producteurs et industries agro-alimentaires d'autre part. Les consommateurs se plaignent d'un manque de transparence, sur les produits alimentaires, leur provenance, leur composition, mais également et de plus en plus sur les conditions sociales et environnementales de leur production **(21)**. Il y a donc un enjeu pour les entreprises à rassurer les consommateurs.

Par ailleurs, les producteurs et industriels sont soumis à des normes strictes pour lesquelles ils doivent être en mesure de fournir les preuves de traçabilité du champ à l'assiette. Ce sont des procédures lourdes et coûteuses. Malgré cela, il faut parfois des semaines pour remonter à la source d'un problème en croisant les systèmes d'information hétérogènes (parfois basés sur des documents papier) - au moins 3 mois dans le cas des œufs contaminés au Fipronil cet été **(22)**. L'enjeu se situe cette fois au niveau de l'efficience de la traçabilité.

CE QUE LA TECHNOLOGIE BLOCKCHAIN PEUT APPORTER :

- **Remonter à l'origine d'un problème :** la blockchain peut permettre de tracer dans un registre toutes les étapes de la chaîne de production d'un produit. Elle doit ainsi permettre de remonter rapidement à une source de dysfonctionnement. Les données étant infalsifiables, elle permet de garantir que nul ne modifiera ses enregistrements pour éviter une mise en cause.
- **Signaler un dysfonctionnement :** par l'association avec des objets connectés et des smart contracts, elle peut permettre l'alerte en temps réel quand des problèmes surviennent (non respect d'une température par exemple).
- **Restaurer une confiance par la transparence :** la traçabilité via une blockchain peut apporter au consommateur final la preuve d'une provenance, d'une origine, le respect d'un cahier des charges ou des conditions de fabrication (tant sur des aspects liés à la santé, qu'à l'éthique ou l'environnement). Le caractère distribué et décentralisé permet l'accès à l'information par tous les maillons de la chaîne qui peuvent ainsi travailler en synergie.
- **Faciliter les audits et contrôles :** par la tenue du registre et/ou le recours de smart contracts qui vérifient de façon autonome que des critères sont respectés, la blockchain peut permettre de réduire les délais et coûts des procédures d'audits et de contrôles et permettre de concerner plus de produits. La blockchain peut ainsi intervenir dans une démarche de certification.
- **Réduire le gaspillage alimentaire :** en accélérant les procédures administratives et en identifiant plus sûrement l'origine d'un dysfonctionnement, elle peut permettre d'éviter que des lots entiers de denrées soient perdus par péremption ou destruction.

DES EXEMPLES :

> LA TRAÇABILITÉ DANS LES GRANDS GROUPES ALIMENTAIRES VIA LES SOLUTIONS IBM :

La nouvelle a été annoncée à large échelle dans la presse : des géants de l'alimentaire (Dole, Driscoll's, Golden State Foods, Kroger, McCormick and Company, McLane Company, Nestlé, Tyson Foods, Unilever et Walmart) se sont associés à IBM pour explorer le potentiel de la blockchain dans le cadre de solutions de traçabilité. Ce consortium fait suite à deux preuves de concept estimées concluantes menées par Walmart et IBM et basées sur la technologie Hyperledger : l'une pour la traçabilité du porc en Chine **(23)** et l'autre, pour celle des mangues au Mexique **(24)** .

Pour les industries alimentaires, l'objectif est de stocker et tracer de façon infalsifiable des informations de type lieu d'élevage ou de production, lieu d'abattage, numéro de lot, données d'usine, dates d'expiration, températures de stockage, détails de transport et de livraison... Une traçabilité totale est visée. L'offre « Blockchain as a service » proposée par IBM, valorisant notamment les innovations HyperLedger de Linux Fondation **(25),** permet à chaque acteur du réseau d'alimenter les données le concernant (son maillon de la chaîne d'approvisionnement) et d'avoir accès aux informations des autres membres, sans qu'il soit possible que l'un des membres détienne une exclusivité. Les rôles et les accès de chacun sont donc soumis à contrôle.

> CARREFOUR ET SES FILIÈRES QUALITÉ ANIMALES

En France, **Carrefour** a également annoncé en février 2017 la mise en œuvre de la technologie blockchain pour la traçabilité de ses filières animales **(26).** Cette démarche s'inscrit dans le cadre des filières qualité Carrefour (en l'occurrence celle des poulets IGP, certifiés Label Rouge, céréales françaises, sans OGM, sans antibiotiques). La chaîne trace les évènements de la naissance à la commercialisation (soit environ 90 jours).

« Ce n'est pas la blockchain qui fait la traçabilité. Nous avons mené un travail d'analyse important sur le process de traçabilité, pour identifier ce qu'il faut stocker dans la blockchain et à quel moment. »

Emmanuel Delerm,
Directeur de projets Carrefour

Le groupe a choisi de travailler sur une blockchain privée, de technologie Ethereum (même si d'autre technologies sont « observées »), où tous les acteurs de la chaîne de production et de commercialisation sont les membres du réseau : préparateurs des lots de poussins, éleveurs, fournisseurs des céréales, abattoirs, ... Les nœuds du réseau sont hébergés par Carrefour au sein d'un Cloud privé ou par les partenaires disposant des moyens informatiques suffisants.

Cela suppose bien sûr que chaque acteur contribue effectivement. L'ordre n'est pas tant important que le fait qu'il y ait bien des enregistrements à chaque étape. Au besoin, des dispositifs (de type smarts contracts) signalent les manques.

Le choix du caractère privé du réseau a été raisonné en fonction de la facilité de mise en place du modèle économique et de gouvernance (dotation initiale de chaque acteur en fonction d'un nombre d'Ether déterminé par le consortium) et de la volonté de pouvoir maîtriser la diffusion ou non de certaines informations, notamment des informations de « savoir-faire » ou des données utiles pour les producteurs (suivi du poids des poulets par exemple) mais non requises aujourd'hui pour la traçabilité. Certaines des informations enregistrées dans la chaine pourront être mises à disposition du consommateur par le biais de QR Code sur les produits. Une communication ascendante vers les éleveurs est également envisagée afin de les tenir plus informés du devenir de leurs productions.

A ce stade, la phase expérimentale est terminée et une mise en place opérationnelle pourrait avoir lieu d'ici la fin de l'année. Pour Emmanuel Delerm, directeur de projets à Carrefour, l'intérêt principal de cette technologie est la mise en commun des informations au sein d'un groupe d'acteurs engagés sur des objectifs communs de qualité.

Il estime que cela se justifie essentiellement sur des produits à forte valeur ajoutée (ou lorsqu'il s'agit d'attester de bonnes pratiques, comme dans le cas de la pêche au thon, filière également explorée par Carrefour).

Il souligne deux points de vigilance :

// Veiller à la « qualité des informations enregistrées (du fait que l'enregistrement n'est pas modifiable mais amendable par un autre enregistrement) » ; à ce titre, il estime que les tiers de confiance vont garder un rôle important, même si ce rôle va évoluer du fait de la technologie.

// Accompagner le changement en « expliquant les plus, les droits et devoirs liés à la blockchain (partagée, infalsifiable, engageante, publiable, etc.) ».

« L'utilisation de la blockchain n'a de sens que si on travaille à plusieurs. C'est son caractère distribué et décentralisé qui est essentiel. »

> LA TRAÇABILITÉ JUSQU'AU CONSOMMATEUR PAR LES TAGS SUR LES PRODUITS

L'entreprise **Provenance** a développé une plateforme des services permettant de savoir d'où vient un produit et s'il a été élaboré dans des conditions éthiques et/ou écologiques. Une de ses preuves de concept utilisant la technologie blockchain a porté sur le suivi de la pêche du thon en Indonésie, selon des méthodes traditionnelles à la ligne et non au filet. L'ensemble de la procédure est bien décrite sur le site internet de Provenance (www.provenance.org) **(27).** Les messages envoyés par sms par les pêcheurs avec le détail de chaque prise alimentent la blockchain de Provenance, une blockchain Ethereum. Chaque poisson est identifié par un numéro de série unique, un « tag » digital qui le suit tout au long de la chaîne d'approvisionnement. Le cas d'utilisation est intéressant car il soulève une difficulté à l'entrée dans la chaine de transformation : celle de pouvoir interfacer la blockchain avec les progiciels de gestion intégrée en place dans les usines (les ERP). Ainsi, dans ce cas d'utilisation, il est décrit que seuls les ERP compatibles avec des standards d'interopérabilité (normes GS1) ont permis de continuer à enregistrer les étapes de transformation dans la blockchain.

En fin de chaîne, un tag NFC (une étiquette électronique) placé sur le produit permet à l'utilisateur d'accéder à l'histoire du produit via son smartphone. Reste évidemment à ce que le tag lui-même ne soit pas copié, falsifié ou déplacé, ce qui constitue là aussi un enjeu pour que la solution soit fiable, bien que basée sur une blockchain...

La **filière viti-vinicole** n'est pas en reste puisque **Dartess**, filiale du groupe Tesson spécialisée dans la logistique du vin, a également annoncé la réalisation d'un POC. L'objectif visé est de pouvoir « reconstituer l'histoire d'une bouteille et de lutter plus efficacement contre la fraude et le vol, de fluidifier les échanges et les traitements douaniers » **(28).** Là encore, le lien entre physique et digital est établi au moyen d' « étiquettes intelligentes ». D'autres initiatives du même type sont engagées dans d'autres pays (comme l'Italie)**. (29)**

> LA CERTIFICATION : CONNECTING FOOD ET AUTRES

Connecting Food est une start-up française qui a une approche un peu différente de la traçabilité puisqu'elle axe son service plus sur une notion de « certification en temps réel ». Elle part ainsi du constat que les marques qui ont recours à des fournisseurs ne peuvent pas procéder à des audits et des contrôles de respect de leur cahier des charges autrement que ponctuellement. *« Les marques et les distributeurs qui font produire à des tiers auditent leurs producteurs une ou deux fois par an en moyenne. Cela signifie que seulement environ 10 % des produits mis sur le marché sont vérifiés et certifiés » (Stefano Volpi, cofondateur de ConnectingFood)* **(30)**. Or, c'est l'image de la marque du produit fini qui peut pâtir des problèmes. La solution de la start-up propose, à chaque étape de la production, de comparer en temps réel le cahier des charges du client avec ce qui est réellement proposé par le fournisseur, de façon à ne pas poursuivre les étapes de production avec un

produit intermédiaire qui ne convient pas. La solution repose sur un ensemble de technologies mises en œuvre avec l'appui d'IBM et de CEA Tech LIST : blockchain mais aussi objets connectés, cloud, cryptographie et intelligence artificielle... Le modèle économique est fondé sur une approche de type service (« Software-as-a-Service » ou SaaS) avec un abonnement payé par le propriétaire du cahier des charges **(31)**. L'entreprise propose aussi de valoriser le travail des agriculteurs en rémunérant leur participation au système Connecting Food.

Toujours dans le domaine de la certification, **un cas d'utilisation pilote a été mené par des chercheurs néerlandais** et présenté lors du congrès EFITA qui s'est tenu à Montpellier SupAgro du 3 au 5 Juillet 2017. Basé sur une technologie Hyperledger, le démonstrateur correspond à une blockchain privée permettant de gérer l'émission, le suivi et la validation des certificats de conformité en temps réel par rapport à un cahier des charges de production de raisin de table. Ce cas a été précédemment présenté via le blog Agrotic : **voir**. Là encore, la décentralisation des informations, c'est-à-dire le non monopole de l'information, et la transparence des informations ont été relevées comme les points les plus intéressants de l'expérience tandis que des problèmes d'évolutivité ont été soulignés en tant que limites techniques.

D'autres expérimentations sont en cours y compris par les acteurs centraux actuels de la certification, les tiers de confiance, tel **Bureau Véritas** qui a lancé un POC sur la certification de la chaîne logistique du thon, utilisant « Proof of Process » une technologie de la start-up Stratumn qui allie blockchain et cryptographie pour sécuriser des échanges entre entreprises.**(32) (33)**

On retient :

En matière de traçabilité, un partage de données fiables est jugé comme une vraie plus-value pour travailler efficacement et en confiance entre partenaires. Mais :

- La blockchain ne fonctionne que si tous les maillons l'alimentent ;
- Les informations en entrée et en sortie de chaîne ne sont pas sécurisées par la blockchain ;
- La notion de tiers de confiance peut subsister quand il s'agit de garantir la validité des informations entrées dans le système ou la conformité de pratiques ;
- La question de l'interopérabilité se pose pour l'intégration de la blockchain dans les systèmes d'information en place.

CAS D'USAGE 2 : **BLOCKCHAIN ET ASSURANCES AGRICOLES (ALÉAS CLIMATIQUES)**

LE CONTEXTE :

> D'une manière générale, les agriculteurs sont relativement mal couverts en termes d'assurance pour les risques liés aux aléas climatiques.

> En France, 25% seulement des cultures de vente (grandes cultures et viticulture) sont assurées contre les risques climatiques. Les agriculteurs jugent les couvertures inadaptées à leurs besoins et n'acceptent de s'assurer que s'ils pensent récupérer au moins l'équivalent de la prime versée **(36).** Dans le cas de gros incidents, l'état doit alors intervenir pour compenser les pertes. Il y a donc un enjeu pour l'état et les groupes d'assurances pour que la couverture des risques soit mieux anticipée.

A LIRE AUSSI :

« Blockchain et assurances » sur le site de Blockchain France **(34)**

« La blockchain dans le secteur de l'assurance » sur le site de Wolters Kluwer France, Actualités du droit **(35)**

> Dans les pays en voie de développement, 357 millions de petits exploitants de moins d'un hectare sont non assurés. Or, près de 80% de la nourriture consommée [...] est produite par ces exploitants. Tout accident de production peut engendrer une pénurie alimentaire. **(37)** Pour les assureurs, l'éparpillement des zones de risques dans le monde ou au contraire, la concentration du risque sur un même type de culture dans une zone géographique soumise aux mêmes aléas est source de coûts administratifs et opérationnels. Le coût de l'assurance restant élevé, peu d'agriculteurs y accèdent ou y sont même sensibilisés.

CE QUE LA TECHNOLOGIE BLOCKCHAIN PEUT APPORTER :

- **Réduire les tarifs :** un système décentralisé et automatisé pourrait permettre une diminution des coûts de gestion et de structure pour les organismes d'assurance donc potentiellement une diminution des tarifs d'assurance pour les assurés, notamment dans les pays où l'assurance agricole est peu développée.
- **Anticiper et mieux évaluer le risque :** l'accès partagé à des informations fiables peut permettre une meilleure connaissance des situations et donc permettre d'élaborer des offres plus adaptées voire personnalisées (principe « Know Your Customer »).
- **Accélérer les procédures :** la remontée automatique d'information en temps réel par des objets connectés ou par recherche dans des bases de données partagées peut constituer un élément déclencheur de programmes autonomes (smart contracts) gérés par la technologie blockchain. Ceci peut, par exemple, permettre l'exécution d'un contrat d'assurance pour régler un sinistre, sans déclaration ni constatation par un expert. Les processus d'indemnisation peuvent être accélérés. Des traitements « de masse » peuvent être facilités.
- **Appréhender l'assurance autrement :** par exemple de façon collaborative en exploitant la possibilité de réseau « peer-to-peer » (s'assurer de particulier à particulier ou dans des groupes d'intérêt commun).

DES EXEMPLES :

Si des exemples d'application sont déjà mis en œuvre dans d'autres secteurs (par exemple, AXA propose « Fizzy » une assurance voyage qui se déclenche automatiquement en cas de retard ou d'annulation de vol **(38)**), ils semblent encore rares en agriculture.

> ASSURANCE INDICIELLE

Notons un cas d'usage proposé dans le cadre d'un challenge (Hackathon Swiss Re 2017, **(39)**) qui, s'il reste fictif, nous aide à percevoir le rôle de la blockchain en matière d'**assurance dite indicielle** (c'est-à-dire basée sur des indices ou indicateurs objectifs, tels qu'une moyenne de températures, une pluviométrie...) et de **micro-assurance**.

Le cas présenté est à destination des agriculteurs kenyans et décrit une mise en collaboration au sein d'une blockchain des petits producteurs, des organismes qui leur apportent une aide (coopératives, organisme de micro-crédits ou d'aide technique), des organismes assureurs, des fournisseurs d'indices météorologiques basés sur des données satellites et des organismes de ré-assurance (organismes auxquels les organismes d'assurance initiaux cèdent une partie du risque). Le service d'assurance serait mis à disposition des agriculteurs grâce au téléphone portable dont ils sont majoritairement équipés. Il serait basé sur le principe de contrats de micro-assurance sur indice prévoyant la prise en compte de paramètres précis pour une zone géographique, une période, et un type de culture spécifiques. Ces conditions et leurs effets seraient inscrits dans un smart contract. Ainsi, dès que le seuil du paramètre serait atteint (par exemple une somme de degrés ou une somme des millimètres de précipitations issues de données météorologiques satellitaires), les assurés seraient automatiquement indemnisés. Tous les titulaires de polices dans une zone géographique définie recevraient des paiements sur la base du même contrat, sans nécessité d'une constatation sur le terrain.

> ASSURANCE COLLABORATIVE

Le principe n'est pas nouveau et des plateformes sans blockchain existent déjà, telles **Otherwise** en France ou **Friendsurance** en Allemagne **(40)** : ① des assurés se regroupent au sein d'une communauté, ② ils déclarent des biens et payent une cotisation pour les assurer ; l'argent est placé pour la plus grande partie sur un compte de séquestre et le reste est investi dans un contrat d'assurance (réassureur) ; ③ en cas de sinistre, l'assuré est payé avec l'argent placé sur le compte de séquestre, puis par le contrat d'assurance lorsque le compte de séquestre est vide ④ l'année suivante, les membres de la communauté ne paient que la somme permettant de reconstituer le montant du séquestre et de payer la police de réassurance. Le but est de redonner du sens à l'assurance en responsabilisant les assurés et en évitant le sentiment de payer sans jamais récupérer.

La start-up Wekeep promettait un « outil permettant de stocker de l'argent numériquement dans des séquestres en smart contract sur la blockchain », basée sur Bitcoin et Ethereum, mais ne semble plus active aujourd'hui **(41)**. L'idée demeure : un syndicat agricole ou autre groupement pourrait par exemple programmer une indemnisation qui serait déclenchée automatiquement en fonction de paramètres comme des données météorologiques. On rejoint le principe de micro-assurance mais en pair-à-pair cette fois.

A NOTER :

Si peu d'exemples sont spécifiquement liés au domaine agricole, le secteur des assurances est actif en ce qui concerne l'exploration du potentiel de la blockchain. Mais comme pour le secteur financier, des questions juridiques particulières seront à considérer. Le rapport Norton Rose Fulbright et R3 fait état de :

- « la nécessité de prévoir des contrats-cadres pour encadrer les relations entre les participants d'une blockchain ;
- la nécessaire conformité des nouveaux systèmes avec les règlementations applicables,
- l'identification du responsable légal d'une blockchain ;
- les risques de discrimination liés au stockage et partage d'informations des assurés ;
- la collecte et la gestion des données personnelles, notamment des données sensibles. »

CAS D'USAGE 3 : **GESTION DE CONSENTEMENT POUR L'UTILISATION DES DONNÉES D'EXPLOITATION (SMART FARMS).**

LE CONTEXTE

Pour piloter leurs exploitations, les exploitants peuvent s'appuyer sur des outils d'aide à décision (OAD). Basés sur des modèles agronomiques, ces outils se nourrissent de plus en plus des apports du numérique, que ce soit pour la collecte, le traitement ou la valorisation des données. Les capteurs et autres objets connectés se développent sur les exploitations et augmentent la quantité de données produites, créant désormais un « Big Data » agricole. « Dans le secteur de l'agriculture et de l'environnement on compte déjà plus de 12 millions d'objets connectés en 2014. Dans 8 ans, on en comptera presque 100 millions. » **(42).** Pour plus d'efficacité, les outils et systèmes doivent communiquer entre eux, être interopérables. La Mission Agriculture Innovation 2025 recommande d'ailleurs de créer un portail de données agricoles, pour faciliter l'accès à ces données hétérogènes et issues de sources multiples. Mais tout ceci pose de véritables questions quant à la propriété et l'usage des données : les agriculteurs s'inquiètent de ne pas pouvoir maitriser l'usage de leurs données, et les fournisseurs d'outils et services numériques peinent à déterminer les droits de mise à disposition et de réutilisation des données qu'ils hébergent. C'est notamment une question de confiance qui est posée : que deviennent mes données, qui les utilise et pour quoi faire ? Peuvent-elles être utilisées contre moi (par des concurrents par exemple). Peuvent-elles être vendues ? Peuvent-elles être modifiées ?

CE QUE LA TECHNOLOGIE BLOCKCHAIN PEUT APPORTER :

- une solution pour renforcer la confiance sur la conservation de l'intégrité des données confiées (en l'occurrence le consentement pour l'utilisation de données) et la préservation de l'anonymat ou la confidentialité des données
- une solution décentralisée et sécurisée évitant que des intermédiaires, tels Google ou Facebook, ne conservent les données pour leur propre usage

DES EXEMPLES :

Ce cas d'utilisation sera exploré dans le cadre du projet « Multipass », projet CASDAR, débutant en Novembre 2017 et réunissant 7 partenaires : **ARVALIS - Institut du végétal** (pilotage du projet), **l'ACTA**, **l'IDELE**, **ORANGE** (partenaire technologique), **SMAG**, **FIEA** (acteur des échanges de données agricoles), **IRSTEA**.

« L'objectif est de mettre à disposition des producteurs une solution "passeport de données" pour protéger le partage des informations collectées sur leurs exploitations ».

Dossier Projet « Multipass »

Ce projet vise à faire émerger de nouveaux services pour l'agriculteur dans une chaine de confiance gérant les consentements d'accès aux données des exploitations. Le projet commencera par identifier les attentes des exploitants vis-à-vis d'un outil de gestion des consentements (facteurs d'établissement de la confiance, freins à lever en matière de partage des données, réponses aux obligations légales...), attentes qui seront traduites en spécifications fonctionnelles pour adapter des outils de gestion des consentements existants puis des cas concrets seront explorés en grandes cultures et en élevage. Ceci permettra de s'interroger sur les conditions de l'interopérabilité entre ces outils et les systèmes existants ou à venir et d'explorer les modalités d'une gouvernance pérenne.

La blockchain ne sera que l'une des voies techniques explorées, et comparée avec une solution centralisée passant par un tiers de confiance. Pour cette partie, « le développement sera confié aux équipes d'Orange et visera principalement à transposer un prototype d'Orange au contexte de l'agriculture [...]. Ce prototype conçu par la Direction de l'Innovation du groupe Orange visait à gérer le consentement d'accès aux données médicales de patients ». **(42)**

Concrètement, ce prototype médical en question illustre la possibilité pour un patient de décider à qui et pourquoi il souhaite ouvrir son dossier médical. Par un formulaire, le patient précise le type de données qu'il ouvre, pour qui (quel type de professionnel), la durée du consentement et le type de droit donné (lecture ou écriture). Ces données sont alors inscrites dans la blockchain. Ainsi, si lors d'un déplacement, il doit avoir affaire à un autre médecin que son médecin traitant, le praticien peut accéder à son dossier. Le patient peut ensuite révoquer ce droit à son retour - Cas décrit par Sajida Zouarhi, doctorante Orange Labs : **(43)**.

« La solution technique utilisée pour la réalisation est basée sur la solution open source Hyperledger qui fournit une Blockchain de type consortium [...] dans laquelle ne peuvent intervenir que des acteurs (utilisateurs ou valideurs de transactions) autorisés au préalable. Une telle solution n'a pas besoin de mettre en œuvre un mécanisme de consensus gourmand en ressources (la preuve de travail), mais un consensus majoritaire, ce qui permet aussi d'offrir de bonnes performances en termes de nombre de transactions validées. Arvalis, FIEA et SMAG hébergeront chacun un nœud du réseau blockchain, avec le support des équipes d'Orange. Les nœuds seront donc dans un premier temps contrôlés par les partenaires du projet mais devront l'être par le consortium à terme. » **(42)**

« La blockchain n'est pas une fin en soi. Elle sera abordée comme l'un des moyens d'instaurer la confiance. »

Bruno Lauga, Arvalis, Chef de projet Multipass

A LIRE AUSSI :

(article en anglais) :

"How blockchain will finally convert you: Control over your own data"**(44)**

CAS D'USAGE 4 :

VENTES DE DENRÉES ET PAIEMENT AUX PRODUCTEURS

LE CONTEXTE :

> Dans le domaine agricole, il existe souvent des délais significatifs entre la vente des denrées par les producteurs et le règlement par les acheteurs. Des délais de paiement allongés peuvent entrainer des situations de dépendance du producteur vis-à-vis du client. Les rapports de force peuvent être déséquilibrés entre des producteurs atomisés et des entreprises clientes puissantes.

> Dans les pays en développement, les coopératives aident les agriculteurs à conserver une plus grande part de la valeur de leurs cultures mais elles s'appuient souvent sur des documents papier ou des promesses verbales. Des problèmes critiques et des situations de corruption peuvent apparaître du fait du manque de transparence et de l'accès restreint aux données sur les prix **(45).**

> Dans les pays en développement, des récoltes sont parfois vendues trop tôt par crainte de non-vente ce qui entraîne une baisse significative de la qualité des denrées et peut être source de gaspillage **(46).**

CE QUE LA TECHNOLOGIE BLOCKCHAIN PEUT APPORTER :

- **Créer la confiance** entre acheteurs et vendeurs sur la base d'un registre ouvert permettant de tracer qui vend quoi, qui achète quoi, à quel prix.
- Permettre l'**accès à une information qualifiée**, y compris pour les très petits producteurs, afin de mieux connaître les valeurs des denrées sur les marchés locaux et internationaux et ainsi être en mesure de planifier.
- Par les **smarts contracts**, les conditions et modalités de règlement peuvent être inscrites de façon immuable et exécutées automatiquement.
- Le réseau peer-to-peer peut permettre des **ventes directes de producteurs à acheteurs,** sans passer par des intermédiaires et donc sans frais de commission.

DES EXEMPLES :

> BEXT360 : POUR UNE RÉMUNÉRATION PLUS JUSTE DES PRODUCTEURS DE CAFÉ

La société **Bext360** a pour objectif d'utiliser la technologie pour améliorer la vie des producteurs de café. La société a mis au point un robot qui utilise la vision et l'intelligence artificielles pour filtrer les grains de café et les séparer en trois catégories - Qualités A, B et C. Les notes sont révélées aux acheteurs et aux agriculteurs qui peuvent alors négocier un juste prix via l'application mobile de bext360. L'application et les logiciels basés sur le cloud utilisent la technologie blockchain de Stellar. org pour créer un enregistrement de l'origine des grains, et qui a payé quoi pour eux. La plate-forme permet également aux usines de transformation, aux distributeurs, aux grossistes et aux autres parties prenantes de la chaîne d'approvisionnement d'utiliser la fonction de traçabilité. Cela permettra à terme aux clients finaux de savoir d'où vient le produit et les étapes qu'il a suivies.

> AGRILEDGER : POUR AIDER LES PETITS AGRICULTEURS ET LEURS COOPÉRATIVES

AgriLedger est une initiative philanthropique appliquant la technologie blockchain pour créer un cercle de confiance pour les coopératives de petits agriculteurs. L'entreprise propose une application mobile liée à la blockchain permettant d'enregistrer les transactions (des partenariats avec des entreprises de télécommunication pour fournir les smartphones), un pack de services permettant de planifier plus efficacement la distribution des produits par une meilleure connaissance des marchés, ainsi qu'une gestion d'identité sécurisée et un coffre-fort de valeur, ce qui permet aux petits producteurs d'entrer dans le monde des services bancaires, des micro-paiements et des prêts.

> AGRIDIGITAL : POUR LA GESTION INTÉGRÉE DE LA FILIÈRE CÉRÉALES

L'entreprise australienne **Fullprofile** teste l'utilisation de blockchain Ethereum pour la solution AgriDigital, plateforme intégrée pour la filière céréalière réunissant les producteurs, les acheteurs, les opérateurs gérants les contrats, les factures, les paiements etc. La solution s'appuie sur les smart contracts pour assurer le règlement immédiat du vendeur dès la livraison à l'acheteur. Après vérification de la transaction, le paiement s'effectue par les mécanismes bancaires classiques (par envoi automatisé d'un ordre de règlement à la banque) ce qui évite le paiement en cryptomonnaie.

AUTRES CAS D'USAGE **ASSOCIÉS À L'AGRICULTURE...**

> Garantir la propriété des terres agricoles :

// En Afrique, 90 % des zones rurales ne sont pas répertoriées dans un cadastre, ce qui est un vrai frein au développement économique. En effet, difficile de faire fonctionner une entreprise lorsque l'on n'a même pas une adresse pour recevoir des approvisionnements. Pour répondre à cette problématique, au Ghana, la start-up *Bitland* propose d'enregistrer les actes fonciers sur une blockchain. De même, en 2015, le gouvernement du Honduras a fait répertorier l'intégralité de son territoire sur une blockchain grâce aux entreprises Epigraph et Factom afin de remédier à de nombreux problèmes de fraudes : certaines personnes s'introduisaient en effet dans les bases de données pour s'octroyer la propriété de terres.

> Assurer un financement participatif :

// En agriculture, le financement participatif (ou crowdfunding), c'est-à-dire la possibilité de faire appel à une communauté pour financer un projet, se développe. Voir par exemple ce que proposent **Miimosa** ou **Blues Bees**. La blockchain peut prolonger (ou transformer ?) cette mouvance en proposant une solution sécurisée pour un transfert direct de fonds au porteur de projet, en utilisant une crypto-monnaie.

Notons que la blockchain fait beaucoup parler d'elle dans le cadre des levées de fonds en soutien au lancement d'entreprises. Ce phénomène porte même un nom : les ICO (Initial Coin Offering). Des actifs numériques (les fameux « tokens ») sont émis par l'entreprise à l'origine de l'ICO, et peuvent être acquis par chacun en échange de cryptomonnaie. Ces tokens correspondent alors à des droits d'utilisation des futurs services développés par l'entreprise. Ils peuvent être revendus mais leur valeur dépend de la valeur accordée au service ou produit (elle est donc basée sur la spéculation).

> De façon beaucoup plus indirecte :

// L'entreprise **Pur Projet** fait intervenir la blockchain pour soutenir des projets d'Agroforesterie dans les pays en développement. Ainsi, Nespresso s'est engagé à planter 10 millions d'arbres dans des modèles agroforestiers en partenariat avec les producteurs de café Nespresso en Colombie, Guatemela et Éthiopie. L'agroforesterie est en effet vue comme un moyen d'assurer un mode de production plus durable pour les populations locales. En contrepartie, la trace de cet engagement de l'entreprise, correspondant à une compensation carbone, est certifiée et l'entreprise peut l'intégrer dans sa chaine de valeurs. « Grâce à la blockchain [...] tous les engagements des entreprises pour les écosystèmes peuvent désormais être certifiés et enregistrés de façon transparente, décentralisée et inviolable. Le tout à moindre coût, car sans intermédiaire bancaire », explique Tristan Lecomte, fondateur de Pur Projet et de la plateforme IPI (International Platform for Insetting). **(47)**

On retient :

- L'utilisation de la blockchain dans le cadre de la traçabilité et de la gestion de la chaîne d'approvisionnement est l'un des cas d'usage les plus évidents et probablement l'un des plus explorés.
- La blockchain est source de promesses en agriculture, notamment par la perspective d'apport de solutions collaboratives aux petits producteurs.
- De la traçabilité, aux solutions de paiements des denrées produites en passant par le pilotage de l'exploitation connectée, les cas d'usage en agriculture sont divers. Bien d'autres restent à imaginer.

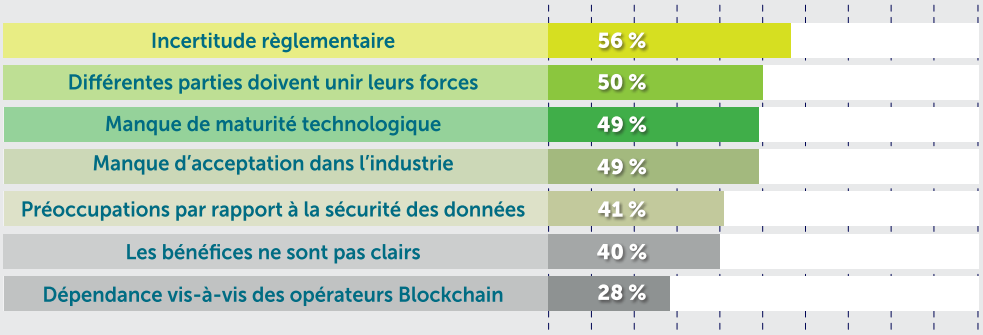
PARTIE III : S'interroger

On l'a vu, les technologies de registres distribués sont porteuses de bien des promesses, en agriculture comme ailleurs. Cependant des promesses à la réalité, il reste de nombreuses marches... La plupart des cas d'usage décrits sont encore à l'état de preuves de concept et il n'est pas toujours facile de recueillir un retour d'expérience de la part de ceux qui les ont mises en œuvre.

Dès lors, il nous semble intéressant de faire le point sur les différentes questions qui se posent quant à la blockchain et les réponses apportées à l'heure actuelle, afin de comprendre ce qui peut (ou non) constituer des freins, et ainsi permettre de mieux se positionner par rapport à ses propres intérêts.

Dans un article de conférence en date d'Octobre 2017 *(« Blockchain in Logistics and Supply chain : trick or treat ? »)* **(48)**, les chercheurs Niels Hackius et Moritz Petersen communiquent les résultats d'une enquête réalisée via les réseaux sociaux entre avril et juin 2017 et destinée à recueillir un avis général sur les bénéficiaires de la blockchain dans un contexte de chaine logistique et sur les obstacles probables à l'adoption. 152 réponses ont permis d'obtenir les réponses suivantes à la question « Quelles sont les barrières probables à l'adoption de la blockchain dans l'industrie logistique ? » :

Quelles sont les barrières probables à l'adoption de la Blockchain dans l'industrie logistique ?



Même s'ils ne portaient que sur les des cas d'usage liés à la logistique, ces résultats nous ont amenés à considérer les questions suivantes :

« Les bénéfices ne sont pas clairs »

> La blockchain est annoncée comme une révolution, mais **est-elle la panacée** ? On le sait, pour être acceptée, une technologie doit faire la preuve de sa pertinence par rapport aux besoins. Dans quels cas, est-elle donc adaptée ?

« Préoccupations par rapport à la sécurité des données »

> La blockchain repose sur le principal argument de la création de confiance notamment par rapport à la sécurité. Cette confiance est-elle justifiée. **Existe-t-il des risques de sécurité ?**

« Manque de maturité de la technologie »

> La technologie blockchain est-elle utilisable dès à présent ? **Est-elle suffisamment mature ?** Si ce n'est pas le cas, pourquoi ?

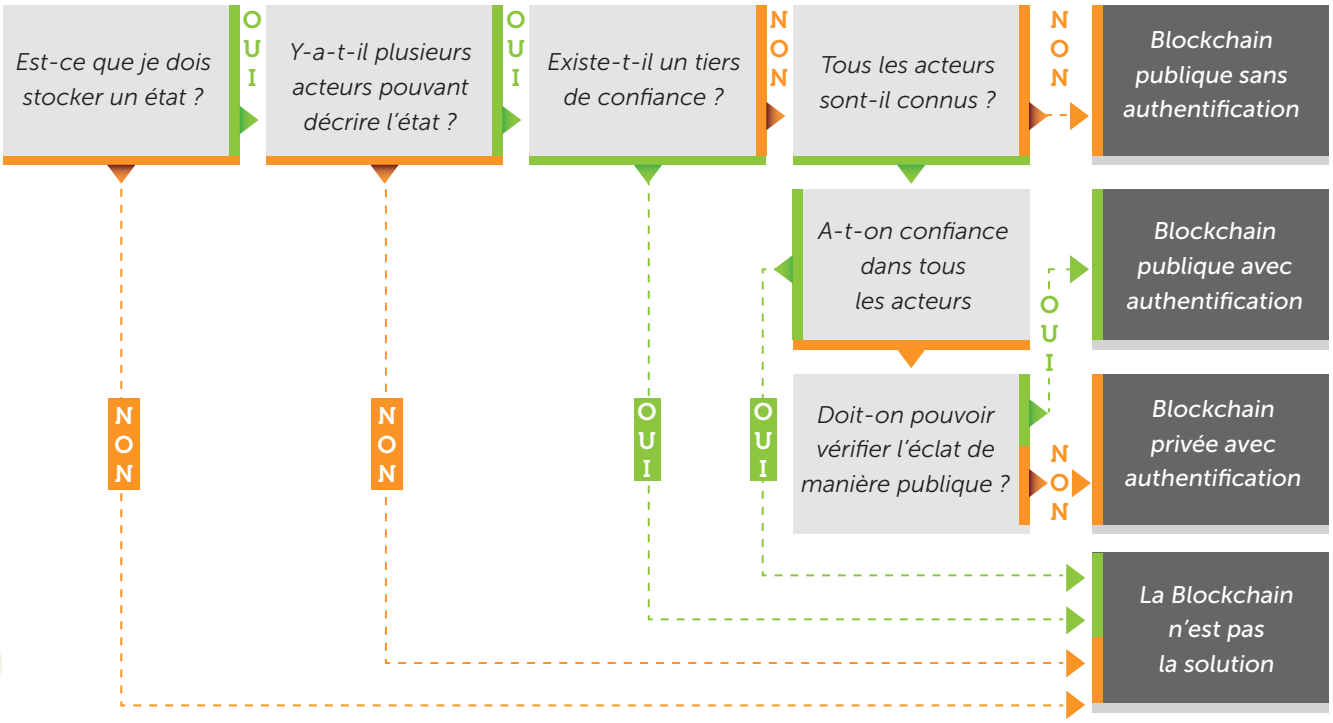
« Incertitude réglementaire »

> La blockchain, notamment publique, repose sur un changement complet de paradigme en matière de gouvernance et de modalités d'exécution de transactions. Pour autant pour que les entreprises puissent convaincre de la pérennité de leur projet, elles doivent montrer un certain respect du cadre légal. **Où en est la blockchain vis-à-vis des aspects juridiques ?**

1 La technologie blockchain est-elle la panacée ?

NON, bien sûr que non, comme toute technologie, il y a des avantages et des inconvénients qui doivent être compris pour ne pas aller au-devant de désillusions. Il y a surtout des cas où la technologie blockchain n'apparaît même pas pertinente.

Gidéon Greensplan traitait déjà ce sujet en 2015 dans un billet du site Multichain **(49)**. Il rappelait ainsi que pour implanter une blockchain, il fallait d'abord se poser la question de savoir si une base de donnée partagée était utile, s'il y avait bien différents contributeurs dont certains présentaient un problème de confiance, si on avait réellement besoin de se passer de tiers de confiance et si on avait bien une idée claire par rapport aux valideurs à qui l'on distribuait la confiance. Ceci a été repris dans un article de Wüst et Gervais en 2017, qui ont proposé une méthode pour aider à déterminer les cas où le recours à la blockhain a du sens (voir figure ci-après).



Il est donc important de considérer la blockchain au regard de ses besoins et de ne pas en attendre plus que ce qu'elle peut apporter.

« Toute seule, elle ne peut pas tout faire », explique Alexandre Stachtchenko, l'un des cofondateurs de Blockchain France cité dans un article de l'Usine Nouvelle **(28)**. *« Si elle sait gérer formidablement bien les actifs numériques, dès que des produits physiques rentrent en compte, il faut ajouter des QR codes, des objets connectés, des capteurs… La blockchain n'est qu'une architecture qui catalyse toutes ces technologies ».*

Ainsi, comprenons donc bien ce que permet la blockchain et ce qu'elle ne permet pas. Une information stockée est a priori infalsifiable à partir du moment où elle y est inscrite. Mais si ce qui a été inscrit n'était pas juste au départ, cela restera faux ad vitam aeternam (il faudra éventuellement une autre transaction pour corriger).

Dès lors, ceci repose la question de la disparition du tiers de confiance, soulignée comme étant l'un des intérêts de la technologie. Comme cela a été évoqué notamment dans le cas d'usage sur la traçabilité, il reste nécessaire de vérifier que les informations inscrites dans la blockchain sont conformes à la réalité et que celles qui en sortent ne vont pas être corrompues. **La nécessité du « tiers de confiance » se déplace donc en périphérie du système.(3)**

Les smart contracts posent un problème particulier par rapport à cette confiance périphérique. En effet, ils nécessitent des données d'entrée pour déclencher automatiquement des actions en fonction de conditions établies à l'avance. Ces données proviennent de sources externes à la blockchain, du monde virtuel ou réel (bases de données, objets connectés, ...)...

Or, de par sa construction, la blockchain est « aveugle » au monde extérieur **(50)**. Elle ne peut faire appel à des services extérieurs pour récupérer des données sinon l'appel serait intégré à une transaction et donc relancé à chaque réplication de la blockchain. La donnée doit être injectée dans la blockchain et avant cela, son intégrité doit être assurée.

Pour résoudre cette problématique, la blockchain fait donc appel à un nouveau rôle, proche du tiers de confiance : l'Oracle (terme du jargon Ethereum).

Les oracles sont des « agents » qui vont être chargés de faire le lien avec le monde réel afin de permettre l'inscription dans la blockchain de données sécurisées et fiables. Ces agents peuvent tout à fait être des tiers de confiance physiques, comme avant, mais si c'est le cas, il faut se poser la question de l'intérêt de la technologie... Ce peut être également des applications qui vont vérifier que la donnée entrée est conforme à ce qui figure au niveau de la source (la société **Oraclize** propose une telle solution). Ce peut être un collectif qui, par consensus, va valider la donnée (des plateformes comme **Augur** proposent ce type de services). Ce peut enfin être des objets connectés ; dans ce cas, ces objets doivent eux-mêmes être associés à des solutions permettant une remontée ou une réception de données sécurisées.

On retient :

- Implémenter une blockchain doit répondre à des problématiques précises. Il ne s'agit pas d'une solution miracle.
- La blockchain ne garantit l'intégrité et la sécurité des données qu'à partir du moment où elles y sont inscrites. Des données fausses peuvent être inscrites ou des données peuvent être corrompues à la sortie. La notion de tiers de confiance pourrait se reporter en périphérie de la chaîne.
- Une nouvelle forme d'agent de confiance est nécessaire pour lier le monde réel à la blockchain : l'oracle.

2 | La technologie blockchain permet-elle une confiance totale ?

NON. Elle permet d'avoir plus de confiance que dans d'autres systèmes mais le « risque 0 » n'existe pas.

Un article de Igor Kabashkin publié à l'occasion d'une conférence « Network and System security » à Helsinky en Aout 2017 **(51)**, répertorie les différents risques qui peuvent se présenter dont :

> **Perte de la clé privée :** la clé privée est personnelle et permet à son propriétaire d'initier les transactions et de bénéficier des transactions dont il était destinataire. S'il la perd ou que quelqu'un s'en empare, il n'a plus aucune possibilité d'accès à la transaction concernée.

> **Perte d'anonymat** (ou pseudonymat) : le système lui-même n'est pas si anonyme qu'annoncé. Un même utilisateur peut réaliser des transactions groupées avec des clés publiques liées entre elles. Si l'identité réelle est découverte, toute l'activité peut être retracée.

> **Bugs dans le programme :** par définition, une blockchain inscrit de façon inaltérable les données. Mais tout est géré par algorithmes. S'il y a un bug dans un programme (dans un smart contract notamment), le bug et son résultat sont figés et une faille de sécurité peut être exploitée. L'affaire TheDAO a fait grand bruit : un bug dans le code a permis à un membre du réseau de détourner 50 millions de dollars. S'il s'agit d'un bug dans la blockchain, il faut prévoir une mise à jour du protocole, ce qui peut poser un souci de cohérence avec l'historique (risque de créer une deuxième branche, « une fork », à la chaîne). Si c'est dans un smart contract, il faut un deuxième programme pour corriger le premier, qui lui, ne peut être modifié. A ce titre, une blockchain est jugée peu évolutive.

> **Durabilité des algorithmes cryptographiques**. La blockchain est sécurisée par ces algorithmes. Si de nouveaux procédés permettent de les attaquer, c'est tout le système qui s'écroule. A ce jour, cependant, aucun dysfonctionnement de ce type n'a été relevé.

> **Prise de contrôle de la blockchain :** les blockchains sont basés sur des protocoles très résistants aux attaques, notamment les protocoles de consensus. Mais si des nœuds parviennent à détenir plus de 50% de la puissance de calcul (dans le cas d'une preuve de travail) ou s'entendent entre eux pour la validation des blocs, ils peuvent prendre le contrôle de la chaine en faisant en sorte de créer la chaîne la plus longue (nous avons vu que dans bitcoin, l'une des règles est qu'en cas de création de deux branches concurrentes, la chaine la plus longue devient légitime). Des mesures de contrôles doivent donc être mises en place pour se prémunir de telles attaques.

> **Abandon de la blockchain :** l' « entretien » de la blockchain tient sur la bonne volonté des participants (les nœuds). S'ils décident de ne plus travailler pour la blockchain, celle-ci meure.

D'après Primavera de Philippi, chercheuse au CERSA, (citée par **Blockchain France** après l'affaire « TheDAO ») : *« il n'existe aucun système qui soit réellement « trustless », qui évacue entièrement la question de la confiance. Si l'idée peut bien fonctionner en tant qu'outil rhétorique, l'idéal d'une technologie parfaitement trustless n'est rien d'autre qu'un idéal »* (20 juillet 2016)

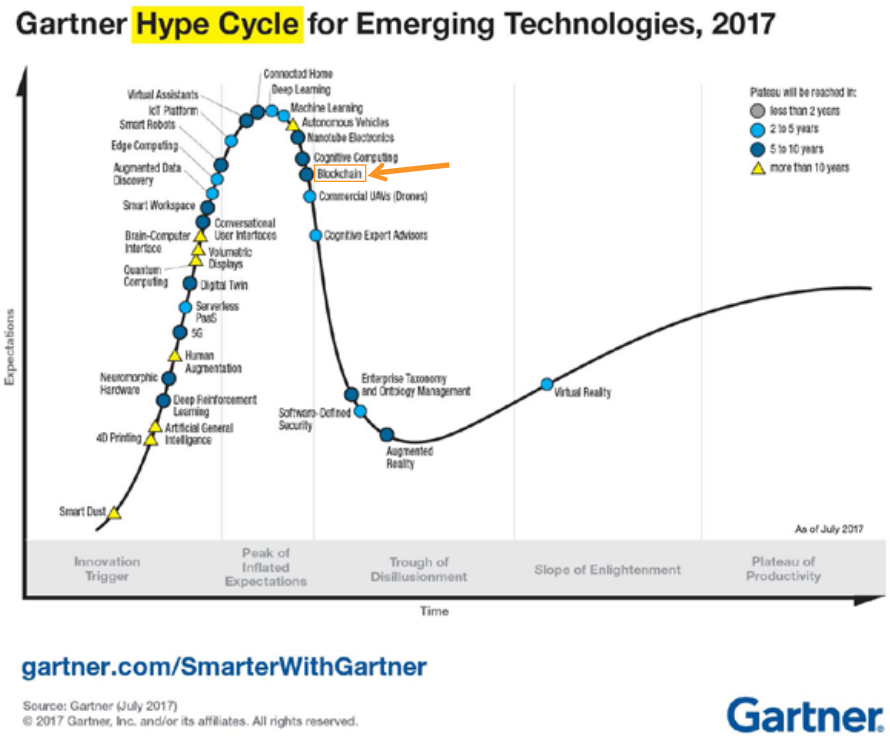
On retient :

- La blockchain est sécurisée à différents niveaux : par l'usage des principes de cryptographie, par la duplication sur les différents nœuds du réseau, par la mise en œuvre de protocoles de validation... En cela, il s'agit d'une technologie qui apporte plus de confiance dans la sécurité que d'autres.
- Mais comme pour tout système, des failles de sécurité peuvent toujours être identifiées. Certaines ont déjà donné lieu à des dysfonctionnements. D'autres restent hypothétiques.
- Les premières mises en œuvre montrent que la confiance ne peut être totalement abandonnée à la technologie : cela reste un idéal.

3 | La technologie blockchain est-elle mature ?

NON si l'on en croit le groupe Gartner...

Il publie chaque année le « cycle du hype » qui permet de positionner les différentes technologies émergentes sur une courbe décrivant 5 phases du processus d'adoption des technologies : lancement de la technologie, espérances démesurées (emballement médiatique, multiplication des start-up), désillusion (critiques médiatiques, échecs des premiers essais), clarification (identification des véritables intérêts) et le plateau de productivité (maturité de la technologie). Ces 5 phases peuvent se dérouler sur plusieurs années avec un délai d'arrivée à maturité différent selon les technologies...



La courbe 2017 place la technologie blockchain encore dans la phase « attentes démesurées », juste à l'orée de la phase « désillusion ». Elle indique également une arrivée à maturité dans 5 ans au moins...

Ceci est également le sentiment de Christine Hennebert, chercheuse au CEA LETI de Grenoble sur la sécurisation des protocoles de l'Internet des objets et l'implémentation des fonctions de sécurité dans les objets connectés, interrogée dans le cadre de cette étude :

« Concernant la blockchain, on lit énormément de choses dans la presse, mais dans la grande majorité des cas, il n'y a rien derrière ces effets d'annonce. Cette technologie est à ses prémisses et en cours d'expérimentation. Je crois qu'elle porte un gros potentiel, mais il est à démontrer au travers de premiers projets et retours d'expérience. Il y a beaucoup à faire. Je crois que certaines solutions (robustes) émergeront pour le public d'ici 4 ans, mais probablement pas avant. »

C. Hennebert, Septembre 2017.

Quels sont les principaux problèmes qui font qu'aujourd'hui cette technologie n'atteint pas encore un niveau de maturité suffisant ?

Il s'agit essentiellement de problèmes liés au « passage à l'échelle » (c'est-à-dire le passage en vraie grandeur après l'expérimentation). Les limites sont d'abord techniques. Elles sont surtout décrites par rapport aux blockchains publiques (telles les cryptomonnaies) et portent sur :

> **La taille de la blockchain** et sa capacité à supporter un accroissement du nombre d'utilisateurs : d'après les statistiques consultables sur le site **https://blockchain.info/fr/**, la taille de la chaine bitcoin a augmenté de 58% en un an, atteignant environ 137 000 MB en octobre 2017. Considérant que le nombre d'utilisateurs est actuellement encore très limité et que la puissance de calcul requise pour le minage augmente considérablement avec la taille de la chaine, le système est jugé difficilement « scalable », c'est-à-dire apte à supporter une montée en charge. Le coût énergétique est également décrié (début 2017 le coût énergétique de la preuve-de travail était estimé à 3,8 milliards de kWh par an, bitcoin.fr).

> **Le volume de transactions** : actuellement Ethereum et Bitcoin permettent de traiter respectivement 25 et 7 transactions par secondes quand VISA autorise des pics à 20 000 transactions par seconde. Ceci s'explique par le temps nécessaire au minage : pour rappel, il faut environ 10 mn entre 2 ajouts de blocs pour bitcoin.

> **La capacité de stockage** : une blockchain n'est pas une base de données au sens habituel du terme. Ses capacités de stockage de données sont limitées : une blockchain est plus prévue pour stocker l'empreinte de la donnée, la preuve de son existence, que la donnée elle-même. Comme nous l'avions également vu pour le système d'oracle, cela implique donc de prévoir et d'entretenir une infrastructure complémentaire.

> **L'interopérabilité** entre la blockchain et d'autres systèmes est également un point de vigilance. D'après Nicolas Pauvre, chef de projet, chez GS1 France, interrogé dans le cadre de cette étude, la blockchain ne permet pas de s'affranchir des problématiques de définition de standards, de structuration et de codification des échanges. « A court terme, l'enjeu est d'assurer l'interopérabilité avec les systèmes existants pour lesquels la blockchain arrive en surcouche. Différentes blockchains doivent également pouvoir fonctionner ensemble ».

Des solutions à ces différentes problématiques sont en voie d'être apportées mais demandent à être encore sérieusement éprouvées. Par exemple :

> Concernant le passage à l'échelle et la fluidité des transactions, des voies d'amélioration sont explorées dans les principales blockchains en service (par améliorations progressives des protocoles, par augmentation de la taille des blocs...).

Notons qu'en matière d'internet des objets, la blockchain, par la décentralisation qu'elle apporte et donc la disponibilité du système, semble apporter un plus par rapport aux systèmes classiques. Un chef de projet Atos, interrogé dans le cadre de cette étude, explique « que la blockchain est plutôt intéressante coté IoT car cela évite de passer par des unités de certification uniques qui introduisent des points de contention au vue du grand nombre des échanges sur les objets connectés ».

> Concernant le coût énergétique, notons qu'il ne se pose pas nécessairement dans les mêmes termes pour une blockchain publique ou une blockchain privée compte tenu des systèmes de validation des blocs bien différents mais le CEA-LETI à Grenoble, par exemple, travaille actuellement sur la quantification de la consommation requise selon le niveau de sécurité souhaité.

> Concernant les problématiques d'harmonisation et d'interopérabilité : GS1 a annoncé une collaboration avec IBM et Microsoft pour progresser dans l'établissement de standards d'interopérabilité. L'AFNOR a également créé une commission de normalisation sur le sujet de la blockchain. Mais le travail commence à peine...

Ces problématiques de « passage à l'échelle » soulèvent également des questions liées à la gouvernance. Plus les chaines se développent, plus il y a de parties prenantes et plus il est difficile de s'entendre. Par exemple, le travail d'amélioration des performances de bitcoin a déjà divisé la communauté – et donc la blockchain - en deux : certains prônant des améliorations progressives (une « soft fork » où il est question de proposer une mise à jour du protocole : c'est le camp « Segwit ») et d'autres une mise à jour radicale (une « hard fork » introduisant une nette augmentation de la taille des blocs: c'est le camp « Bitcoin cash »).

On retient :

- La blockchain n'est pas une technologie mature.
- Techniquement, elle souffre encore d'incertitudes quant à sa capacité à intégrer un plus grand nombre d'utilisateurs et des réponses d'interopérabilité avec d'autres composantes des systèmes d'information doivent être apportées.
- En termes de gouvernance, un équilibre est à trouver : une chaîne qui se développe implique un plus grand nombre de parties prenantes à mettre d'accord...

4 | Doit-on craindre le flou juridique autour de la blockchain ?

OUI et NON... Certes, le cadre légal de la blockchain est encore loin d'être défini. D'un côté, cela peut être un bien car légiférer trop tôt peut nuire à la créativité et à l'innovation. Mais d'un autre côté, cela peut également constituer un frein important à l'adoption. En effet, un flou juridique implique de fait une prise de risque. Une simple méconnaissance ou un problème d'interprétation peut conduire à enfreindre une réglementation en vigueur (et donc s'exposer à des pénalités) ou à perdre en crédibilité en faisant des promesses qui ne pourront être tenues.

Jusqu'ici, la technologie blockchain n'affranchit pas de la règlementation s'appliquant dans des secteurs spécifiques (finance, assurance, santé, jeux, etc.), relative à l'identité (règles Know Your Customer par exemple) ou à la collecte de données sur les individus...

D'aucuns prônent la « blockchain law » qui rebattrait totalement les règles de fonctionnement dans le domaine juridique comme elle promet de les changer dans d'autres domaines, arguant qu' « une bonne partie des engagements qui sont noués sur la blockchain sont difficilement compatibles avec les exigences du droit classique » (Voir l'article de Blockchain France sur le sujet : « Blockchain et Droit : Code is deeply Law ») **(53)**. Il est vrai par exemple que la blockchain n'a pas de frontière. Bitcoin est une blockchain mondiale. Dans ce cas, en cas de problème, quelle loi territoriale doit être appliquée ?

Repartons des principales catégories de cas d'usage pour identifier quelques questions d'ordre juridique qui se posent à l'heure actuelle :

» TENUES DE REGISTRE

A ce jour, on ne reconnait pas la blockchain comme étant support d'une preuve juridique de détention ou de l'existence d'une transaction. Pour le moment, il faut donc encore démontrer au juge, comme pour n'importe quel autre support numérique, que l'enregistrement est recevable (ce qui revient à expliquer que la blockchain permet de garantir l'authenticité, l'intégrité des informations, etc.).

Le cadre légal évolue rapidement cependant, même s'il se concentre pour le moment sur les aspects financiers. En France, les évolutions suivantes ont ainsi eu lieu :

> **Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse :** l'article L223-12 stipule que « l'émission et la cession de mini bons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations [...] ».

> La loi n°**2016-1691 du 9 décembre 2016 (loi « Sapin II »)**, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, habilite le gouvernement à modifier le cadre législatif pour faciliter la transmission de certains titres financiers au moyen de la technologie « blockchain ».

> La Direction Générale du Trésor a mené une consultation préalable à la rédaction d'un projet de texte **(54)** puis, de septembre à octobre 2017, une consultation sur un **projet d'ordonnance** blockchain/ titres financiers.

Mais d'autres questions restent posées :

> Celle de **la responsabilité** de la certification : si les blockchains permettent de se passer de certains tiers de confiance, tels les notaires ou les banques, qui assumera la responsabilité qui leur incombait

A LIRE AUSSI :

Panorama des enjeux juridiques de la blockchain, Blockchain Partner **(52)**

jusqu'ici en cas de dysfonctionnement. Dans le cas d'une blockchain privée, le problème est peut-être plus simple mais dans le cas d'une blockchain publique, qui par définition n'appartient à personne, qui sera responsable en cas de préjudice envers un utilisateur ? Le système est-il à ce point fiable qu'il exclut toute question de ce type ?

> Celle du **droit à l'oubli.** La problématique est intimement liée au caractère immuable des données inscrites. En effet, par principe, une fois inscrite, une donnée ne peut être ni supprimée, ni modifiée et pourtant des acteurs autres que l'individu concerné, y ont accès...

» TRANSACTIONS NUMÉRIQUES

A ce sujet, les questions tournent essentiellement autour du statut du « token », l'unité d'échange gérée dans une blockchain. Un token peut correspondre à des entités très variées : un produit dont on suit la traçabilité, un jeton de réputation, un coupon fidélité, un droit de vote, une unité de cryptomonnaie... Mais, en fait, un token n'a pas de valeur intrinsèque. Sa valeur provient de l'usage ou du bénéfice qu'on lui attribue et qui entretient une spéculation. Dès lors cela pose des questions juridiques, car si la règlementation tranche pour une définition unique, elle peut de facto faire peser une règlementation spécifique (code monétaire et financier, code du commerce...) ou faire appliquer certaines dispositions du droit fiscal (TVA...). Pour le moment par exemple, en France, le token est associé à un simple bien meuble, plutôt par élimination par rapport aux autres statuts. La reconnaissance des cryptomonnaies, elle, est très différente selon les pays. Si la plupart les acceptent au moins en tant que « moyen de paiement », peu sont ceux qui leur reconnaissent une valeur légale.

» SMART-CONTRACTS

Ce qu'il faut comprendre avec les smart contracts c'est que, contrairement à ce que suggère le terme, ce ne sont justement pas des contrats. Ce sont des codes informatiques qui exécutent des dispositions contractuelles. Le contrat entre les parties, en lui-même, relève donc des mêmes dispositions qu'auparavant, c'est-à-dire de la connaissance des règlementations en vigueur, et doit donc concerner des parties averties. En revanche, la question de la sécurité juridique se pose. Comme tout code informatique, le smart contract peut être soumis aux bugs. Mais par principe, les smart contracts sont immuables... En cas de problème d'exécution, à qui revient la responsabilité ? Aux développeurs qui l'ont construit ? Encore faudrait-il pouvoir les identifier. Aux co-contractants qui n'ont pas vérifié si toutes les clauses du contrat étaient bien traduites dans le langage informatique ? Mais un code informatique n'est pas lisible par tous... Ces questions restent ouvertes.

On retient :

- Le cadre juridique de la blockchain reste flou.
- Ne pas légiférer trop vite laisse place à l'expérimentation. Une règlementation trop coercitive irait à l'encontre de la philosophie des blockchains publiques, par définition indépendantes des organes de contrôle centraux.
- Mais le flou juridique fait peser un risque sur ceux qui initient des solutions et ceux qui les utilisent (non identification du responsable, non reconnaissance du préjudice, non reconnaissance de la « preuve » conférée par la blockchain...)
- Le cadre légal et réglementaire évolue au fil des développements des usages. Les usages financiers sont actuellement les plus observés.

CONCLUSION

Derrière le terme blockchain se cachent donc en fait bien des choses :

> une combinaison innovante de technologies pré-existantes permettant la gestion d'un registre de transactions distribué et sécurisé,
> un mode de gouvernance collaboratif qui réinvente la confiance sans tiers de confiance,
> un écosystème d'acteurs en structuration,
> un changement de paradigmes dans de nombreux domaines...

La blockchain bouleverse les cadres établis, notamment les cadres juridiques, et invite à construire de nouveaux cas d'usage pertinents afin d'atteindre le potentiel que beaucoup reconnaissent, dans tous les domaines.

Le secteur agricole est évidemment directement concerné. La blockchain ouvre d'intéressantes perspectives que ce soit en matière de traçabilité, de meilleure valorisation du travail des exploitants, de conditions de travail plus favorables aux petits producteurs ou de pilotage de l'exploitation connectée. La création d'une chaine de confiance où l'exploitant peut maîtriser ses données est un enjeu d'avenir. Le fort développement des objets connectés en agriculture profitera nécessairement des apports de la technologie blockchain associée aux smart contracts, ces programmes autonomes qui permettent d'établir un lien avec le monde réel.

De nombreux défis restent à relever, notamment en matière de sécurisation des données en périphérie de la blockchain. Mais aujourd'hui, la technologie, ou plutôt « les » technologies de registres distribués, n'en sont qu'à leurs balbutiements et il ne serait pas raisonnable, en agriculture comme ailleurs, d'y placer des espoirs démesurés. De nombreuses questions, tant techniques, que juridiques ou sociétales restent posées. Il faudra probablement attendre encore 5 ans au moins avant que des cas d'usage robustes n'apparaissent réellement.

Cette synthèse a pour but d'apporter des éléments de compréhension à partir d'une littérature très fournie. Mais elle doit être prolongée par l'expérimentation et les retours d'expérience. Le champ des possibles est large entre blockchain privée ou publique, recours ou non aux outils et services des « grands » acteurs du numérique, interfaçage avec les systèmes d'information existants ou à venir,... Le retour sur investissement doit également être évalué mais, même sans vrais objectif de résultats, l'expérimentation est le seul moyen de développer l'infrastructure et les compétences au sein des entreprises. C'est la clé pour s'approprier une technologie qui, même expliquée, reste complexe à mettre en œuvre.

La Chaire AgroTIC continuera bien évidemment à suivre les évolutions jusqu'à ce que la blockchain atteigne le stade de la maturité technologique.

CHAIRE AgroTIC

ÉTUDES D'OPPORTUNITÉ
Contact : nathalie.toulon@agro-bordeaux.fr

RÉFÉRENCES

(1) BLOCKCHAIN FRANCE. La blockchain décryptée. Les clés d'une révolution. Observatoire Netexplo, 2016. ISBN 978-2-9546672-1-8.

(2) UCHANGE. Comprendre la blockchain (livre blanc par U) [en ligne]. [Consulté le 23 août 2017]. Disponible à l'adresse : http://www.finyear.com/Comprendre-la-blockchain-livre-blanc-par-U_a35431.html

(3) MEDEF. Livre Blanc - La blockchain pour les entreprises [en ligne]. Avril 2016. MEDEF, BCG. Disponible à l'adresse : http://www.cigref.fr/wp/wp-content/uploads/2017/06/Livre-blanc-Blockchain-pour-entreprises.pdf

(4) DARDAYROL, Jean-Pierre (coordinateur). Août 2017 - Blockchains et smart contracts : des technologies de la confiance ? Les annales des Mines [en ligne]. Les Annales des Mines, 2017. Réalités industrielles. Disponible à l'adresse : http://www.annales.org/ri/2017/ri_aout_2017.html

(5) PILKINGTON, Marc. Blockchain Technology: Principles and Applications [en ligne]. 18 septembre 2015. Social Science Research Network. [Consulté le 7 juillet 2017]. Disponible à l'adresse : https://papers.ssrn.com/abstract=2662660

(6) BLOCKCHAIN FRANCE. Qu'est-ce que la blockchain ? Blockchain France [en ligne]. 22 septembre 2015. [Consulté le 11 juillet 2017]. Disponible à l'adresse : https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

(7) BITCOIN.FR, (Jean-Luc). Bitcoin c'est quoi ? Bitcoin.fr [en ligne]. 8 juin 2011. [Consulté le 22 août 2017]. Disponible à l'adresse : https://bitcoin.fr/qu-est-ce-que-bitcoin/

(8) BOURGUIGNON, Sébastien. Quelle utilité au consensus dans la blockchain ? Siècle Digital [en ligne]. 7 novembre 2016. [Consulté le 23 août 2017]. Disponible à l'adresse : https://siecledigital.fr/2016/11/07/utilite-consensus-blockchain/

(9) THERON, Loup. Quel consensus dans une blockchain privée ? | OCTO talks ! [en ligne]. [Consulté le 4 octobre 2017]. Disponible à l'adresse : https://blog.octo.com/quel-consensus-dans-une-blockchain-privee/

(10) COCHELIN, Pascal (Terre-net Média). La blockchain va-t-elle arriver en agriculture ? Terre-net [en ligne]. [Consulté le 10 septembre 2017]. Disponible à l'adresse : https://www.terre-net.fr/innovation-et-technologie/article/blockchain-en-agriculture-monnaie-paiements-transactions-contrats-2894-125241.html

(11) VITALIK BUTERIN. Vitalik Buterin: On Public and Private Blockchains. CoinDesk [en ligne]. 7 août 2015. [Consulté le 22 août 2017]. Disponible à l'adresse : https://www.coindesk.com/vitalik-buterin-on-public-and-private-blockchains/

(12) MOUGAYAR, William. Implementing Blockchain: Who Are You Going to Call? CoinDesk [en ligne]. 4 mai 2016. [Consulté le 11 octobre 2017]. Disponible à l'adresse : https://www.coindesk.com/which-blockchain-implementations/

(13) TEDX TALKS. La Blockchain: réinventer les rapports de confiance | Claire BALVA | TEDxLyon [en ligne]. Février 2017. [Consulté le 11 octobre 2017]. Disponible à l'adresse : https://www.youtube.com/watch?v=JID9c-MABis

(14) POLROT, Simon. Qu'est-ce qu'une cryptomonnaie, un token, un actif numérique ? Ethereum France [en ligne]. 24 mai 2017. [Consulté le 11 octobre 2017]. Disponible à l'adresse : https://www.ethereum-france.com/qu-est-ce-qu-une-cryptomonnaie-token-bitcoin-ether-gnt-gno-dgd-plu-rep-rlc/

(15) SAUCÈDE, Florent et FENNETEAU, Hervé. Les blockchains et l'idéal de la traçabilité totale dans la chaîne logistique au prisme des théories du canal de distribution. In : Paché, G. (dir.), Images de la logistique : Eclairages managériaux et sociétaux. Presses Universitaires d'Aix-Marseille, 2017. pp. 49-55.

(16) BLOCKCHAIN FRANCE. La fin de l'idéal trustless. Blockchain France [en ligne]. 20 juillet 2016. [Consulté le 20 octobre 2017]. Disponible à l'adresse : https://blockchainfrance.net/2016/07/20/la-fin-de-lideal-trustless/

(17) GARIN, Matthieu et ROCHE, Maxime. La blockchain : un nouveau modèle pour la confiance ? RiskInsight [en ligne]. 27 septembre 2016. [Consulté le 4 octobre 2017]. Disponible à l'adresse : https://www.riskinsight-wavestone.com/2016/09/blockchain-nouveau-modele-confiance/

(18) MAYEGA, Emmanuel. Crédit Agricole Store : le bitcoin et la blockchain en rayons (rediffusion). Assurance & Banque 2.0 [en ligne]. 12 août 2016. [Consulté le 13 octobre 2017]. Disponible à l'adresse : http://www.assurbanque20.fr/credit-agricole-store-le-bitcoin-et-la-blockchain-en-rayons/

(19) POLROT, Simon. Slock.it : la promesse des objets connectés sur la blockchain. Ethereum France [en ligne]. 4 avril 2016. [Consulté le 11 octobre 2017]. Disponible à l'adresse : https://www.ethereum-france.com/slock-it-la-promesse-des-objets-connectes-sur-la-blockchain/

(20) BLOCKCHAIN PARTNER. Agriculture, agroalimentaire et blockchain [en ligne]. 2017. [Consulté le 21 août 2017]. Disponible à l'adresse : http://blockchainpartner.fr/wp-content/uploads/2017/05/Etude-Agriculture-Agroalimentaire-Blockchain-Partner.pdf

(21) IPSOS POUR LA FONDATION DANIEL ET NINA CARASSO. Alimentation durable : les Français de plus en plus attentifs à ce qu'ils mangent. IPSOS FRANCE [en ligne]. 8 novembre 2016. [Consulté le 20 septembre 2017]. Disponible à l'adresse : http://m.ipsos.fr/decrypter-societe/2016-11-08-alimentation-durable-francais-plus-en-plus-attentifs-ce-qu-ils-mangent

(22) LATRIBUNE.FR. Œufs contaminés au fipronil : France et Royaume-Uni touchés, Europe désorganisée. La Tribune [en ligne]. 8 août 2017. [Consulté le 27 septembre 2017]. Disponible à l'adresse : http://www.latribune.fr/entreprises-finance/industrie/agroalimentaire-biens-de-consommation-luxe/oeufs-contamines-au-fipronil-france-et-royaume-uni-touches-europe-desorganisee-746545.html

(23) HACKETT, Robert. Walmart and IBM Partner to Put Chinese Pork on a Blockchain | Fortune.com. [en ligne]. 19 octobre 2016. [Consulté le 21 août 2017]. Disponible à l'adresse : http://fortune.com/2016/10/19/walmart-ibm-blockchain-china-pork/

(24) SHAFFER, Erica. Walmart, IBM provide blockchain update | MEAT+POULTRY [en ligne]. juin 2017. [Consulté le 30 septembre 2017]. Disponible à l'adresse : http://www.meatpoultry.com/articles/news_home/Business/2017/06/Walmart_IBM_provide_blockchain.aspx?ID={24B47705-09C1-4A89-A98C-28403AF874C1}&cck=1

(25) IBM COMMUNICATIONS. Blockchain for Food Safety. [en ligne]. 22 août 2017. [Consulté le 27 septembre 2017]. Disponible à l'adresse : http://www-03.ibm.com/press/us/en/pressrelease/53013.wss

(26) GROUPE CARREFOUR. 4 nouveaux engagements sur la qualité alimentaire. Groupe Carrefour [en ligne]. Février 2017. [Consulté le 10 septembre 2017]. Disponible à l'adresse : http://www.carrefour.com/fr/nos-actualites/4-nouveaux-engagements-sur-la-qualite-alimentaire4 nouveaux engagements sur la qualité alimentaire

(27) PROVENANCE.ORG. Provenance | From shore to plate: Tracking tuna on the blockchain. Provenance [en ligne]. Juillet 2016. [Consulté le 30 septembre 2017]. Disponible à l'adresse : https://www.provenance.org/tracking-tuna-on-the-blockchain

(28) PROTAIS, Marine. La blockchain sur les traces de la supply chain. https://usinenouvelle.com/ [en ligne]. 9 mars 2017. [Consulté le 30 septembre 2017]. Disponible à l'adresse : https://www.usinenouvelle.com/article/la-blockchain-sur-les-traces-de-la-supply-chain.N510414

(29) VIDALENS, Publié par KÉVIN. Vins italiens seront enregistrés sur Blockchain, « Authenticité garantie ». Création site internet mérignac [en ligne]. 18 avril 2017. [Consulté le 30 septembre 2017]. Disponible à l'adresse : http://kevidoweb.com/vins-italiens-seront-enregistres-blockchain-authenticite-garantie/

(30) MATZEU DE VIALAR, Laurène. Stefano Volpi, co-fondateur de Connecting Food. Voxlog [en ligne]. 16 mars 2017. [Consulté le 27 septembre 2017]. Disponible à l'adresse : http://www.voxlog.fr/rencontre/37/stefano-volpi-co-fondateur-de-connecting-food

(31) HUSTACHE, Marie-Laure. Stefano Volpi, co-fondateur de la start-up Connecting Food. saf agr'iDées [en ligne]. 1 septembre 2017. [Consulté le 27 septembre 2017]. Disponible à l'adresse : https://www.safagridees.com/interview/stefano-volpi/

(32) RENAUD, Ninon. Blockchain : Stratumn lève 7 millions d'euros. lesechos.fr [en ligne]. 8 juin 2017. [Consulté le 30 septembre 2017]. Disponible à l'adresse : https://www.lesechos.fr/08/06/2017/lesechos.fr/030374334987_blockchain---stratumn-leve-7-millions-d-euros.htm

(33) WHITWORTH, Joe. Blockchain can transform traceability - Bureau Veritas. FoodQualityNews.com [en ligne]. Avril 2017. [Consulté le 27 septembre 2017]. Disponible à l'adresse : http://www.foodqualitynews.com/Industry-news/Bureau-Veritas-on-disruptive-Blockchain-technology

(34) BLOCKCHAIN FRANCE. Blockchain et assurances. Blockchain France [en ligne]. 17 février 2016. [Consulté le 1 octobre 2017]. Disponible à l'adresse : https://blockchainfrance.net/2016/02/17/assurances-et-blockchain/

(35) DENIS, Bénédicte. La Blockchain Dans Le Secteur De L'assurance | Actualités Du Droit | Wolters Kluwer France. [en ligne]. 21 septembre 2017. [Consulté le 1 octobre 2017]. Disponible à l'adresse : https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/8937/la-blockchain-dans-le-secteur-de-l-assurance

(36) ABADIE, Aurélie. L'Argus de l'Assurance - Risque agricole : l'assurance contre les aléas climatiques peine à décoller - Les Services de l'assurance. L'Argus de l'assurance [en ligne]. juin 2017. [Consulté le 2 octobre 2017]. Disponible à l'adresse : http://www.argusdelassurance.com/gestion-des-risques/risque-agricole-l-assurance-contre-les-aleas-climatiques-peine-a-decoller.119395

(37) ATLAS MAGAZINE. Assurance agricole : produits, spécificités et importance du soutien de l'Etat. [en ligne]. Juin 2017. [Consulté le 12 octobre 2017]. Disponible à l'adresse : http://www.atlas-mag.net/article/lassurance-agricole-0

(38) CUNY, Delphine. Retard d'avion : Axa lance une assurance automatique sur la Blockchain. La Tribune [en ligne]. 14 septembre 2017. [Consulté le 1 octobre 2017]. Disponible à l'adresse : http://www.latribune.fr/entreprises-finance/banques-finance/retard-d-avion-axa-lance-une-assurance-automatique-sur-la-blockchain-750202.html

(39) SWISS RE. Hackaton challenge : blockchain-based agricultural microinsurance (document225386321776382 6328.indd - SR_hackathon_factsheet.PDF) [en ligne]. 2017. [Consulté le 1 octobre 2017]. Disponible à l'adresse : https://www.ears.nl/static/consensus-2017/SR_hackathon_factsheet.PDF

(40) PIGEOT, Adrien. Quand les usages et la technologie permettent de réinventer le mutualisme | OCTO talks ! [en ligne]. mai 2016. [Consulté le 1 octobre 2017]. Disponible à l'adresse : https://blog.octo.com/quand-les-usages-et-la-technologie-permettent-de-reinventer-le-mutualisme/

(41) MÉTAIRIE, Jérémy et GARNIER, Charles. Note d'innovation Hubchain - septembre 2017. septembre 2017. Région Nouvelle Aquitaine - CATIE.

(42) ARVALIS INSTITUT DU VÉGÉTAL (CHEF DE FILE). Appel à projet « recherche technologique » 2017 - Dossier finalisé - Projet Multipass. 2017.

(43) ORANGE HUMAN SIDE. Mieux gérer ses consentements grâce à la blockchain - Human Inside Orange. Human Inside [en ligne]. 13 janvier 2017. [Consulté le 4 octobre 2017]. Disponible à l'adresse : https://humaninside.orange.com/fr/mieux-gerer-ses-consentements-grace-la-blockchain/

(44) DICKSON, Ben. How blockchain will finally convert you: Control over your own data. VentureBeat [en ligne]. 9 septembre 2017. [Consulté le 12 octobre 2017]. Disponible à l'adresse : https://venturebeat.com/2017/09/09/how-blockchain-will-finally-convert-you-control-over-your-own-data/

(45) GODAN.INFO. Agriledger | GODAN. [en ligne]. [Consulté le 12 octobre 2017]. Disponible à l'adresse : http://www.godan.info/organizations/agriledger

(46) ONU POUR L'ALIMENTATION ET L'AGRICULTURE. Pertes et gaspillages dans le monde - Etude menée pour le Congrès international Save Food - Interpack 2011, Dûsseldorf, Allemagne [en ligne]. 2012. ONU pour l'alimentation et l'agriculture. Disponible à l'adresse : http://www.fao.org/docrep/016/i2697f/i2697f.pdf

(47) CHARMEIL, Lara. Quand la blockchain permet de certifier le bilan carbone des grandes entreprises. We Demain, une revue pour changer d'époque [en ligne]. [Consulté le 13 octobre 2017]. Disponible à l'adresse : https://www.wedemain.fr/Quand-la-blockchain-permet-de-certifier-le-bilan-carbone-des-grandes-entreprises_a2257.html

(48) HACKIUS, Niels et PETERSEN, Moritz. Blockchain in Logistics and Supply Chain: Trick or Treat? (PDF Download Available). In : Prepint of accepted article [en ligne]. octobre 2017. [Consulté le 22 août 2017]. Disponible à l'adresse : https://www.researchgate.net/publication/318724655_Blockchain_in_Logistics_and_Supply_Chain_Trick_or_Treat

(49) GREENSPAN, Gidéon. Avoiding the pointless blockchain project | MultiChain. [en ligne]. 22 novembre 2015. [Consulté le 15 octobre 2017]. Disponible à l'adresse : https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

(50) POLROT, Simon. Les Oracles, lien entre la blockchain et le monde. Ethereum France [en ligne]. 13 septembre 2016. [Consulté le 17 octobre 2017]. Disponible à l'adresse : https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/

(51) KABASHKIN, Igor. Risk Modelling of Blockchain Ecosystem. Network and System Security 11th International Conference, NSS 2017 Helsinki, Finland, August 21–23, 2017 Proceedings. 2017. pp. 31p.

(52) BLOCKCHAIN PARTNER. Panorama des enjeux juridiques de la blockchain [en ligne]. Juin 2017. Blockchain Partner. Disponible à l'adresse : https://blockchainpartner.fr/wp-content/uploads/2017/06/Enjeux-juridiques-de-la-blockchain-Etude-Blockchain-Partner.pdf

(53) BLOCKCHAIN FRANCE. Blockchain et Droit: Code is deeply Law. Blockchain France [en ligne]. 19 septembre 2017. [Consulté le 19 octobre 2017]. Disponible à l'adresse : https://blockchainfrance.net/2017/09/19/blockchain-et-droit/

(54) DIRECTION GÉNÉRALE DU TRÉSOR PUBLIC. Synthèse de la consultation publique sur la transmission de certains titres financiers au moyen de la technologie « blockchain » - Trésor-Info. [en ligne]. août 2017. [Consulté le 19 octobre 2017]. Disponible à l'adresse : https://www.tresor.economie.gouv.fr/Articles/2017/08/31/synthese-de-la-consultation-publique-sur-la-transmission-de-certains-titres-financiers-au-moyen-de-la-technologie-blockchain

CHAIRE AgroTIC

ÉTUDES D'OPPORTUNITÉ

Contact : Nathalie Toulon,
nathalie.toulon@agro-bordeaux.fr

Retrouvez toute l'actualité de la chaire sur :
www.agrotic.org/chaire