ACADÉMIE DES TECHNOLOGIES
FONDATION

La Blockchain, nouvel outil pour l'industrie et les services
Mai 2023

De la société Capgemini Engineering : Mouna BEN MABROUK, Djamel KOUICEM, Christian JOUBERT, Jean-Paul GOMEZ,
De l'Académie des Technologies : Michel LAROCHE

Table des matières

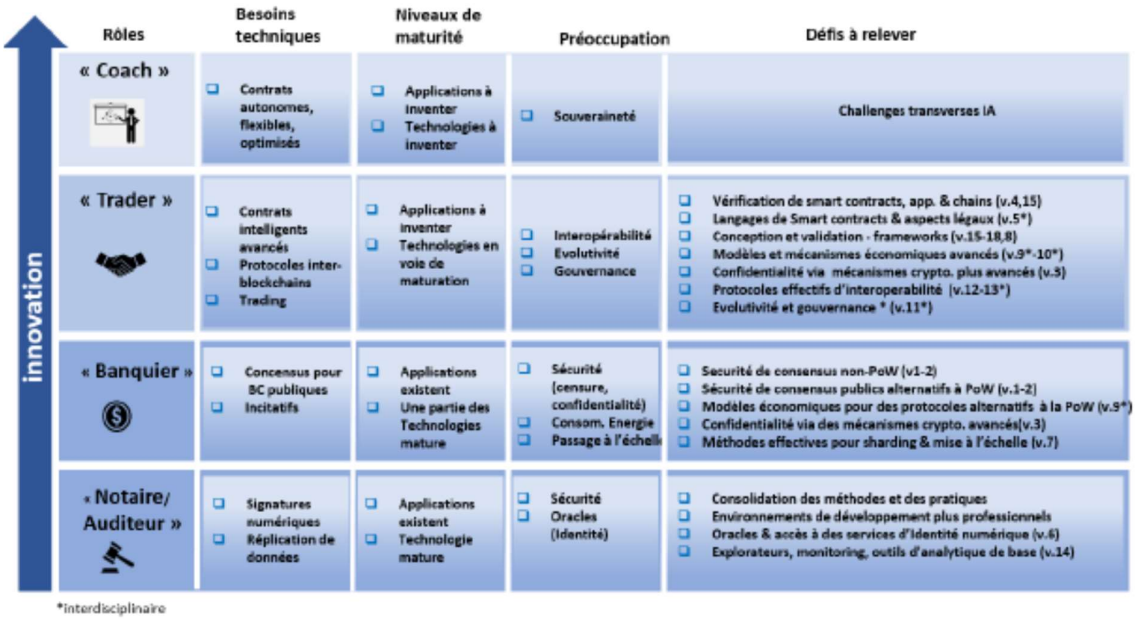
1 Introduction

C'est sous la houlette de la Direction Générale des Entreprises que, en collaboration avec l'ensemble de l'écosystème français de la Blockchain, a été préparée, et présentée en avril 2019, **la stratégie nationale blockchain** qui a pour objectif de faire de la France une « nation de la blockchain ».

Dans ce cadre, un groupe de travail, impliquant le CEA, l'IMT et l'INRIA, a eu pour mission de « **définir avec précision l'ensemble des verrous technologiques et techniques** » existant autour de ce thème.

L'important travail effectué se traduit, dans le rapport[1] publié, par de nombreuses recommandations établies sur la base d'une analyse des freins à l'utilisation de tout ou partie des technologies intégrées dans la blockchain de référence (le Bitcoin) et une identification des éléments nécessaires à leur application dans d'autres domaines prometteurs.

Le tableau de synthèse, issu du rapport évoqué, est présenté ci-dessous. Il montre l'importance du travail en perspective nécessaire pour couvrir tous les défis identifiés et ainsi développer l'usage de ces technologies dans d'autres domaines que les cryptomonnaies ou le « notariat ».



Un autre constat peut être fait. Malgré toutes les questions soulevées dans ce rapport, la Blockchain est désormais invoquée dans des propositions visant à améliorer le fonctionnement de processus commerciaux ou industriels ou utilisée par certains distributeurs dans les domaines de la consommation, en particulier alimentaire.

En fait derrière le mot « Blockchain » se cachent les différents usages que l'on peut envisager pour le système informatique entourant (et nécessaire à son bon fonctionnement) qui entoure la Blockchain simple base de données.

[1] https://www.senat.fr/notice-rapport/2017/r17-584-notice.html

Cette situation peut troubler un décideur souhaitant profiter aussi vite que d'autres des nouveaux outils disponibles. Il se pose la question des capacités et de l'intérêt réels de la Blockchain dans le domaine d'activité de son entreprise. Il souhaiterait, sans doute, ne pas avoir à s'en remettre totalement aux « spécialistes » qu'ils soient présents en interne de l'entreprise ou consultés à l'extérieur. C'est pour répondre à ce souci que nous traiterons en priorité du sujet de la **Blockchain « simple base de données »**.

L'objectif de cette **première partie** est de fournir aux « décideurs » les éléments principaux permettant une réflexion utile avant d'opter ou non pour une Blockchain.

Les **lecteurs** pourront ensuite découvrir dans **la deuxième partie** l'usage complexe qui est fait de la Blockchain dans le contexte du Bitcoin. Ce chapitre présente les aspects techniques de cette utilisation ; sa lecture est facultative mais utile si l'on souhaite s'intéresser à ses nouvelles applications

La **troisième partie**, présente les adaptations possibles de la Blockchain pour d'autres usages, notamment les contrats intelligents, smart contracts.

La **quatrième partie** détaille la variété des applications envisagées ou déjà en cours de mise en place dans l'industrie et les services.

2 La Blockchain : histoire et principes généraux

2.1 Un peu d'histoire : La Blockchain, une notoriété récente, un potentiel prometteur

En 2008, Satoshi Nakamoto a lancé le Bitcoin, première « crypto-monnaie » qui ne soit ni régie par un gouvernement, ni gérée par une banque.

Il voulait créer une monnaie hors des circuits économiques, étatiques et financiers traditionnels pour permettre la réalisation des transactions dans le monde « virtuel » du web. Pour ce faire, il a repris les fondements de la monnaie qui sont : être un intermédiaire dans les échanges, être une réserve de valeur, être une unité de compte pour le calcul économique. Ceci implique que les acteurs utilisant cette monnaie ont confiance dans la stabilité de la monnaie, dans la sureté et la transparence de l'information et des transactions ainsi que dans sa pérennité.

Or en sortant des systèmes existants (Banques et Etats), il a fallu organiser des outils et processus permettant de satisfaire toutes ces « obligations » pour répondre aux besoins d'une monnaie hors les systèmes existants.

Dans le Bitcoin, les principes de base sont les suivants : toutes les transactions effectuées sont effectuées « publiquement », tout le monde peut les effectuer, les consulter, les vérifier, dans un pseudo anonymat[2].

Satoshi Nakamoto a choisi la **technologie blockchain et ses principes architecturaux pour stocker et protéger les données enregistrées**, choix qu'il a complété par un ensemble de logiciels, règles et processus.

C'est ce choix qui a rendu **indissociables « Bitcoin »** et technologie **« Blockchain »**. Mais un point doit être souligné, il n'y a pas qu'une technologie mais une association de plusieurs spécialités, technologies élémentaires et processus dont certains ont largement précédé l'émergence du Bitcoin et de sa « Blockchain ».

Il en est ainsi de la « cryptographie », du « hachage », de « l'algorithmique » partagée ou de la notion de « bloc ».

Depuis, sont apparues d'autres crypto-monnaies : Ethereum, Ripple et Litecoin [40].

Le succès de ces applications a mis en avant le concept de la « Blockchain », et ses propriétés phares : immuabilité des transactions, transparence et décentralisation de la confiance (sans dépendance à une autorité de référence).

[2] Le bitcoin ne garantit pas l'anonymat des utilisateurs. Il s'agit plutôt de pseudo-anonymisation. Chaque utilisateur est identifié par codage généré par une autorité de certification. Cette autorité pourrait récupérer très facilement les informations nominatives et personnelles d'un utilisateur. Dans le jargon de la sécurité l'anonymat est une propriété beaucoup plus forte et est très souvent assurée moyennant des outils cryptographiques.

Des applications inspirées du Bitcoin se sont déjà développées de façon extrêmement rapide dans différentes industries et entreprises à travers le monde.

Le mot-valise « Blockchain » est ainsi par extension utilisé dans la présentation de solutions non strictement Blockchain mais simplement construite autour de la Blockchain comme base de données et profitant de l'environnement nécessaire au bon fonctionnement de celle-ci..

Les avantages effectifs ou simplement espérés de ces solutions sont les suivants :

- Potentiel de réduction des coûts d'infrastructure bancaire : - 30%.

Potentiel d'économie annuelle pour les banques utilisant la technologie blockchain : 8 à 12 milliards de dollars.Ces potentielles réductions aboutissent à évaluer le marché mondial de la blockchain (et de ses variantes) en 2024 à 19 milliards de dollars.3, en croissance de 50% par an en moyenne.[4]

Les statistiques présentées ci-dessous montrent l'importance de la croissance déjà observée et celle escomptée pour le marché de la Blockchain.

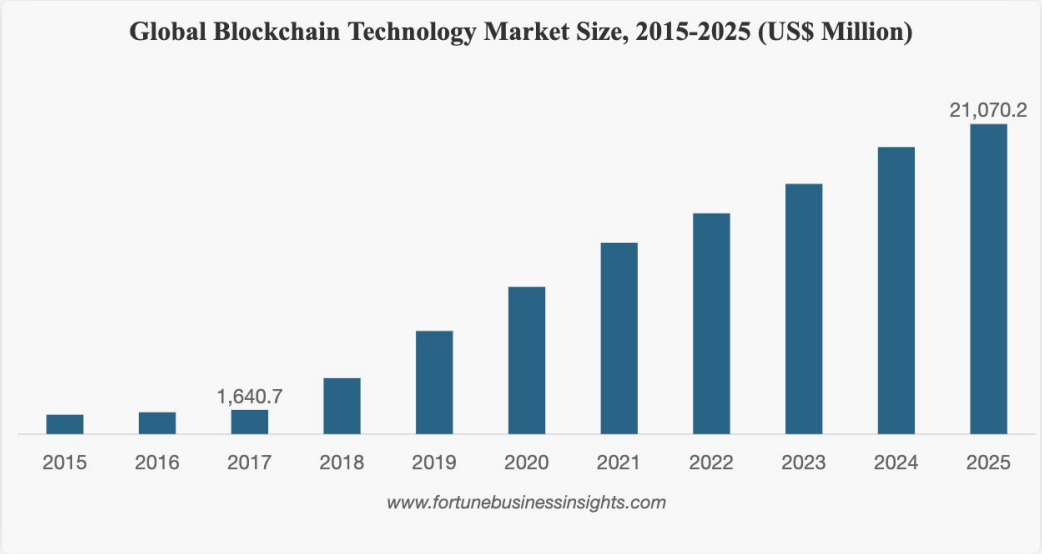


Figure 1. Evolution et prévision de croissance du marché de la technologie Blockchain dans le monde de 2018 à 2025[5]

La technologie « Blockchain » apparait donc promise à un bel avenir grâce au grand nombre d'applications déjà explorées ou envisagées.

2.2 La Blockchain « base de données »

[3] https://www.offremedia.com/le-marche-mondial-de-la-blockchain-va-progresser-de-pres-de-50-par-dici-2024-dapres-idc

[4] Pour rappel:

- Investissement moyen dans les projets blockchain en 2017 : 1 million de dollarMontant qu'IBM investit dans l'IoT alimenté par la blockchain : 200 millions de dollars en 2016

[5] https://blockblog.fr/le-marche-de-la-blockchain-dentreprise-atteindra-2107-milliards-de-dollars-dici-2025-declare-fortune-business-insights/

L'utilisation faite de la « Blockchain » dans le Bitcoin, sa première application, et la plus complexe à ce jour, sera décrite dans le 2ème partie de ce document (chap 3). Si cette utilisation est un sujet complexe les principes de base de la « Blockchain » peuvent, eux, être décrits relativement simplement.

La Blockchain c'est d'abord une **base de données[6],** donc un instrument destiné à stocker des informations, à les protéger et à les rendre disponibles aux utilisateurs qui en ont besoin.

Toutefois elle se différencie des bases de données « classiques » par **certaines caractéristiques essentielles** :

- D'abord il s'agit d'une base de données qui, comme son nom l'indique, prend la forme d'une **« chaîne de blocs de données »**. Les données y sont stockées par blocs de taille limitée, créés et scellés au fil du temps puis reliés entre eux pour former une chaîne. Une fois créé, chaque bloc est associé à une « empreinte » élaborée sur la base de l'ensemble du contenu du bloc. Cette empreinte doit être très spécifique de ce contenu et modifiée par toute évolution du bloc (pour plus de détails cf Hachage dans le §.3.3.1). Cette empreinte est ensuite intégrée dans les données du bloc suivant (et participe donc à l'élaboration de l'empreinte de ce nouveau bloc). Cette empreinte, désormais enregistrée, permet ainsi de détecter facilement toute modification du bloc précédent qui induirait, pour ce bloc, une empreinte différente de celle enregistrée. **La modification et l'effacement sont ainsi interdits par construction, dans une blockchain on ne revient pas en arrière, on ne peut que « écrire et avancer ».**

- Le système de détection de toute modification étant en place il convient de le compléter par un moyen, pour le cas où une modification serait détectée, de pouvoir rétablir la base dans sa version correcte. Ce moyen peut prendre deux formes. La première consisterait à gérer d'une façon très protégée une base de référence permettant de rétablir la base dans un état précédent. Cette référence sera complétée au fur et à mesure par l'intégration des évolutions acceptées et servira ainsi de nouvelle référence.
  Mais une telle stratégie est lourde à déployer pour une base largement utilisée, donc vulnérable. La stratégie utilisée dans le cas de la base supportant le bitcoin est très différente, elle s'appuie sur la **mise en place d'un grand nombre de copies** de la blockchain et sur **des règles très contraignantes sur la valeur de l'empreinte** (cf le minage - chap 3.4.2). Chacune de ces copies est associée à un ensemble de logiciels permettant **la comparaison fréquente des empreintes de ces différentes copies**, donc la détection de différences. La correction des copies est ensuite réalisée en choisissant comme référence la configuration majoritaire dans les copies en place. Cette stratégie a l'avantage de rendre possible une utilisation très « ouverte » de la blockchain mais nécessite d'adapter nombre de copies et fréquence de comparaisons au niveau de protection recherché. **Elle peut se révéler très lourde à mettre en œuvre** (cf chap 3 : la blockchain du bitcoin).

- Pour fonctionner de façon correcte la Blockchain doit donc s'appuyer sur une algorithmique partagée basée sur des logiciels associés à chacune de ses copies et d'un réseau permettant une communication quasi-permanente entre ces différentes copies.

Grace à ces caractéristiques les blocs, une fois scellés et ajoutés à la chaîne, ne peuvent plus être modifiés. Les données stockées y sont donc **quasi-infalsifiables[7]** qu'elles soient confidentielles ou non (ATTENTION : le traitement de la confidentialité n'est pas une propriété intrinsèque de la Blockchain et, si nécessaire doit être traité spécifiquement).

Dans une entreprise tout responsable d'une base de données doit avoir **deux soucis principaux** :

- La **protection** des données enregistrées

- La **validité** des données que l'on souhaite enregistrer

Il est clairement établi que le **premier de ces soucis est au cœur de la Blockchain.** Mais qu'en est-il du **second** ?

Bien que les pratiques habituelles puissent être utilisées (droits d'accès, confiance dans les individus en charge…) il faut noter que les concepteurs du système Bitcoin ont choisi à nouveau **une formule « différenciante »,** mais non intégrée à la base, Ils profitent du réseau informatique nécessaire à la protection de la base (voir plus haut) pour **faire accepter l'inscription sur la base d'une nouvelle donnée** (vérifier le respect des procédures et la validité de la donnée) **par les acteurs de ce réseau** (dans le cas du bitcoin il s'agit de vérifier que les comptes impliqués dans un échange de Bitcoins existent et sont suffisamment approvisionnés).

Sur la base de ces informations il est possible de comparer la blockchain aux bases de données partagées stockées dans un centre administrateur de données accessible par l'ensemble du réseau dans le but de pouvoir juger de l'adéquation de chacune des solutions avec les besoins prioritaires de l'application envisagée.

2.3 Quelle base de données choisir et pourquoi décider d'opter pour la Blockchain ?

2.3.1 Quelques rappels importants

Derrière le terme de « bases de données » se cachent aujourd'hui des objets informatiques de natures très différentes tant par leur dimension, l'importance ou le coût pour l'entreprise, que par leur conception ou leur usage.

Pour des **bases de données importantes** une entreprise a désormais le choix entre :

- une base de données « **classique** », gérée par un administrateur central (interne ou externe) garant des données, de leur qualité et de la gestion des accès à cette base,
- une « **blockchain** » à la mesure de l'usage envisagé et ses contraintes de garantie, de qualité et d'accès**.**

[6] On entend par base de données un ensemble d'informations qui est organisé de manière à être facilement accessible, géré et mis à jour. Elle est utilisée par les organisations comme méthode de stockage, de gestion et de récupération de l'information.

[7] Sous réserve d'absence d'une coalition malveillante majoritaire de parties prenantes ("Attaque 51%" dans la littérature)

Paramètres	***Blockchain***	***Base de données partagée « classique »***
Opérations externes permises	Proposition d'enregistrement d'une donnée, lecture des données enregistrées.	Création, lecture, mise à jour et suppression des données en fonction des droits attribués à chaque intervenant autorisé
Validation des données	Entente obligatoire des pairs sur l'acceptabilité des données.	Fonction des droits attribués à chaque intervenant autorisé
Accessibilité	La mise en place d'un nouveau nœud est possible. La communauté est ouverte.	Limitée aux personnes autorisées
Confidentialité	Les intervenants ne sont pas identifiables mais les données sont accessibles en clair depuis chacun des nœuds.	Fonction des droits attribués à chaque intervenant autorisé et aux précautions spécifiques prises (par ex : chiffrage).
Protection	Assurée par la multiplicité des copies et la nécessité d'obtenir un consensus de la communauté avant toute opération irréversible.	Ne fait pas partie, par construction, d'une base de données mais doit être assurée par des mesures spécifiques adaptées.
Traçabilité	La modification ou l'effacement des données n'étant pas autorisés l'historisation obtenue de fait par le chaînage assure la traçabilité. Rien ne se perd.	Ne fait pas partie, par construction, d'une base de données.
Transparence	Complète pour les données et les informations associées mais anonymat des intervenants.	Limitée car fonction des droits attribués à chaque intervenant autorisé.
Inaltérabilité	Quasi-infalsifiable	Ne fait pas partie, par construction, d'une base de données.

Figure 2 : Comparaisons entre les caractéristiques principales d'une Blockchain et celles d'une base de données classique

Leurs différences principales, et importantes, présentées ci-dessus (figure 2) rendent le choix évoqué difficile.

Ce choix nécessite d'établir une correspondance entre, d'une part, les besoins et attentes de l'entreprise et, d'autre part, les possibilités et performances des technologies disponibles. Si la Blockchain profite de l'aura du Bitcoin pour se présenter avantageusement, son usage doit être réservé à des conditions favorables. L'objet de ce chapitre est d'aider le décideur à faire un choix « éclairé ».

Selon le processus décisionnel souhaité, chacun pourra lire dans l'ordre qu'il souhaite les deux sous-chapitres :

- Si le choix reste à faire, le § 2.3.3 pourra servir à orienter la décision entre blockchain et base de données classique par l'identification des éléments favorables à chacune des solutions

- Si le choix d'une Blockchain est déjà fait les éléments présentés dans le § 2.3.4 pourront aider à sa mise en place en identifiant certains des points durs que pourrait rencontrer cette opération : prérequis, avantages, points de vigilance, contre-indications.

Mais avant de parcourir le processus décisionnel proposé il nous semble utile d'attirer l'attention sur quelques points spécifiques de la Blockchain.

2.3.2 Quelques éléments à connaître sur la Blockchain

Des points de vigilance

La nécessité de traiter les situations liées à son usage d'une algorithmie partagée, qui rend parfois difficile l'obtention automatique du consensus, deux points durs doivent être évoqués lorsque l'on veut juger de l'intérêt de la blockchain. Dans son usage de « type Bitcoin » son **fonctionnement n'est pas gratuit** car la validation des blocs de données représente un certain travail qui doit être rémunéré,

- Les logiciels qui travaillent en permanence à gérer et à enregistrer les données de transaction entraînent **une consommation d'électricité si importante** qu'elle fait douter du caractère « responsable » du système Bitcoin en général et de sa blockchain en particulier.
  A la dimension du système Bitcoin la garantie de protection obtenue grâce à la comparaison très fréquente des différentes copies nécessite que l'opération de hachage, qui est au cœur de cette fonction, soit réalisée, sur l'ensemble des nœuds du réseau, plus de 10^{32} fois par seconde ! Sur cette base, et compte tenu des performances des calculateurs spécialisés utilisés, il est possible d'estimer la consommation totale annuelle d'électricité à une valeur comprise entre 60 et 100 TWh.

  La **gestion de la sécurisation d'une blockchain coûte cher** car grande consommatrice d'énergie électrique.

- Malgré les travaux de recherche réalisés, les solutions de type Blockchain publiques ont du mal à passer à l'échelle et on reste très loin des systèmes transactionnels classiques.
- La problématique de gouvernance pour définir la responsabilité des acteurs en cas de non-respect des règlements (RGPD, etc.)

  Pour ces raisons, des utilisateurs peuvent souhaiter avoir des usages moins dispendieux, acceptant ainsi des performances réduites, et d'autres, en revanche, atteindre des performances maximales pour leur domaine d'usage.

Pour s'adapter à de nouveaux usages et tenter de contourner les réserves exposées beaucoup de travaux ont été engagés et de tentatives d'ores et dèja faites afin d'adapter la blockchain.

Pour juger de la pertinence des évolutions en cours ou de leur intérêt pour de nouvelles applications il convient de rappeler les quelques élémets clefs qui font **la réputation (le visible) et la performance (les solutions techniques)** de la blockchain façon Bitcoin.

Des points d'excellence

- Autoprotection contre la falsification de l'information enregistrée
- Accessibilté aisée à l'information stockée.
- Confiance dans la qualité de l'information stockée.
- Rapidité de réaction du « système » tant pour l'enregistrement que pour la surveillance des données.
- Base de données structurée en blocs historisés et chaînés.
- Multiplicité des copies de la base de données réparties aux nœuds d'un réseu gérées et protégées.
- Fonctionnement basé sur des relations permanentes entre « pairs », les nœuds du réseau.
- Surveillance permanente de l'intégrité des données stockées grâce à la surveillance des empreintes (souvent crées par « hachage »).
- Intrication de l'outil de surveillance et de la base de données.
- Algorithmique parallèle.
- Régénération automatique des données en cas de falsification/corruption d'une partie minoritaire des copies gérées.

2.3.3 Critères de décision entre blockchain et base de données « classique »

Dans l'hypothèse d'un **choix restant à faire,** le tableau ci-dessous peut constituer une aide à la décision par l'**auto évaluation du contexte** de mise en œuvre de la base de données.

Eléments favorables au choix d'une Blockchain		**Eléments favorables au choix d'une base de données « classique »**
Traçabilité sans faille recherchée		Droit à l'oubli
Indélébilité des données recherchée		Modification et suppression autorisées
Grand nombre d'utilisateurs appartenant à des environnements variés.		Communauté limitée en nombre ou hébergée dans un environnement limité et bien « protégé »
Utilisation très ouverte		Besoin de disposer de droits d'accès différenciés
Informations stockées à forte valeur ou grande importance		Données non « stratégiques »
Partage sans restriction facile et rapide d'informations précises		Grande confidentialité recherchée
Base de données destinée à durer		Usage limité dans le temps
Gestion basée sur le consensus de nombreux acteurs		Gestion par une autorité centrale
Accès aux informations stockées fréquent, devant être facile pour des opérateurs très dispersés		Contrôle d'accès très strict aux données enregistrées
Recherche d'une très grande confiance dans l'intégrité des données		Dispositif de protection adapté au besoin
Besoin de robustesse du stockage		

2.3.4 Eléments d'analyse afin de faciliter et réussir la mise en place d'une Blockchain

En préambule rappelons que chacune des **deux qualités marquantes** du « système Blockchain de type Bitcoin» **est indissociable** d'une des caractéristiques qui le différencie fortement des bases de données « classiques ». C'est son organisation en **chaîne de blocs** liés et verrouillés suivant la chronologie de leur création qui **rend indélébile une donnée enregistrée** et c'est la **multiplicité des copies** associée à un processus de comparaison des copies entre elles qui **protège les données de toute falsification**.

En cas de forte probabilité de **choix d'une Blockchain, cette analyse** aidera à en préciser le projet par l'identification de spécificités et points durs.

Les prérequis
Exigence d'une traçabilité sans faille
Besoin d'intégrité des données
Forte valeur ou importance des informations stockées
Non confidentialité de l'information
Besoin d'un système ouvert à un grand nombre et une grande variété d'utilisateurs
Besoin de partage et accès sans restriction, facile et rapide aux informations
Les avantages
Ineffaçabilité
Infalsifiabilité
Processus de consensus de validation des enregistrements possible
Absence de nécessité d'une autorité externe de validation des données
Exhaustivité de l'accès aux données
Strict contrôle de l'utilisation et du nombre d'utilisateurs (de 1 à l'infini)
Les points de vigilance
Coût élevé (rémunération des nœuds et énergie)
Besoin de très nombreuses copies de la blockchain
Vulnérabilité de l'algorithmie partagée
Utilisateurs appartenant tous à une structure protégée
Les contre-indications pour la Blockchain
Faible nombre d'utilisateurs potentiels
Durée de vie limitée des données
Faible valeur ou importance des informations stockées
Grande confidentialité des informations traitées
Nécessité du droit à l'oubli

Voici une **dernière recommandation au décideur** après le choix de principe « Blockchain », compte tenu de l'apparition de nombreuses offres basées sur « la Blockchain » et revendiquant une empreinte énergétique réduite. Dans l'offre qui lui sera faite, **il devra apporter une attention toute particulière**, aux principes et solutions retenus pour les deux opérations clefs que sont la **validation des données** avant leur enregistrement et le **rétablissement de l'intégrité de la chaîne** en cas d'altération.

3 La Blockchain dans l'univers du BITCOIN

Ce chapitre présente les techniques et technologies utilisées pour permettre la gestion du bitcoin et donc la création des éléments de sa blockchain ainsi que sa protection. Il présente de nombreux aspects techniques, mais pas essentiels à la bonne compréhension de notre propos. Le lecteur qui ne souhaite pas entrer dans tous les aspects techniques peut se dispenser de lire ce chapitre et passer directement au chapitre 4.

Bitcoin et Blockchain : des technologies élémentaires au service d'un objectif ambitieux

La crypto-monnaie Bitcoin permet à ses utilisateurs d'échanger des biens en dehors de tout système de référence et en tout anonymat. Elle ne circule pas dans le sens économique courant du terme et n'est utilisée que par des personnes ayant choisi de l'utiliser.

Le « système **Bitcoin** », grâce à un ensemble de logiciels remplit, de façon totalement digitale et décentralisée, les deux rôles, habituellement tenus par une banque, que sont celui de **« tiers de confiance »** gérant **des transactions monétaires** d'une part et celui de **garant des soldes des comptes** de ses utilisateurs.

Ces deux rôles s'appuient sur une base de données structurée en **Blockchain (chaîne de blocs) où sont stockées les informations** concernant uniquement la partie monétaire des transactions effectuées par les possesseurs de Bitcoin. La partie matérielle de la transaction (échange de bien ou de service, ou autre) est traitée totalement en dehors du système Bitcoin sous la seule responsabilité des acteurs de la transaction.

3.1 La transaction, objet élémentaire de la blockchain

La transaction « conventionnelle »

Dans une transaction conventionnelle, l'acheteur paye une somme à un vendeur en échange d'un bien. Une fois que le vendeur a reçu cette somme, l'acheteur n'a aucun moyen de la réutiliser pour une autre transaction, car la monnaie est dès lors en possession du vendeur.

Dans une transaction numérique, la somme n'étant pas matérielle, rien n'empêcherait l'acheteur de dupliquer un même paiement vers deux vendeurs.

Mais l'autorité centrale, le système bancaire, tient un registre comptable de tous les comptes et transactions. En enregistrant les transactions en débit chez l'acheteur et crédit chez le vendeur, cette autorité centrale garantit à la fois l'authenticité de la monnaie, sa disponibilité chez l'acheteur et l'impossibilité de double dépense.

C'est l'existence d'une autorité centrale qui interdit la double dépense.

Figure 1. Transaction numérique avec autorité centrale

Dans le « système Bitcoin », la rapidité d'acceptation et d'enregistrement d'une transaction et la confidentialité des échanges entre ses acteurs sont les qualités essentielles reconnues et appréciées par les utilisateurs du Bitcoin.

Ces qualités s'expliquent :

- D'une part par les procédures efficaces et rapides de validation et d'enregistrement qui s'appuient sur la Blockchain et la sécurité qu'elle apporte du fait de sa structure et de sa gestion très transparente (cf § 3 3 et 3.4).

- D'autre part, les acteurs d'une transaction bénéficient d'une grande protection et restent anonymes, impliqués seulement à travers l'utilisation de comptes totalement anonymisés. La cryptographie y joue un rôle essentiel.

3.2 La confidentialité des transactions dans le Bitcoin

Afin de garantir la confidentialité des échanges entre les acteurs d'une transaction, les messages échangés sont rendus illisibles grâce au chiffrement. Pour cette opération deux catégories de chiffrement basées sur le principe de clés cryptographiques sont disponibles. Il s'agit du chiffrement symétrique et du **chiffrement asymétrique**. Utilisé au **cœur de la formalisation des « transactions »**, ce dernier est un élément essentiel du fonctionnement du « système » Bitcoin.

Le chiffrement asymétrique

Le **chiffrement asymétrique** utilise une clé publique et une clé privée pour chiffrement et déchiffrement. Dans cette famille de cryptographie, maintenir un message chiffré n'est pas garanti par la complexité de l'algorithme de chiffrement mais par les clés cryptographiques. La figure ci-dessous présente le fonctionnement général de cette méthode cryptographique. Dans un système cryptographique à clé publique, chaque utilisateur dispose d'un couple de clés : une clé publique utilisée pour le chiffrement et une clé privée utilisée pour le déchiffrement. Ces deux clés sont mathématiquement liées d'une façon à ce qu'un message chiffré par une clé publique PK ne peut être déchiffré qu'avec la clé privée associée à la clé PK. Nous tenons à préciser que la connaissance de la clé publique ne peut en aucun cas induire la connaissance de la clé privée qui lui est associée.

Quand la "Source" souhaite chiffrer un message qu'elle veut transmettre à un "destinataire", elle utilisera la clé publique du destinataire. Celle-ci rendra confidentiel le message grâce à un ensemble d'opérations arithmétiques. Dès lors, seul le destinataire, disposant de la clé privée pourra déchiffrer le message. Pour déchiffrer le message, il effectuera d'autres opérations arithmétiques sur le message chiffré en utilisant sa clé privée.

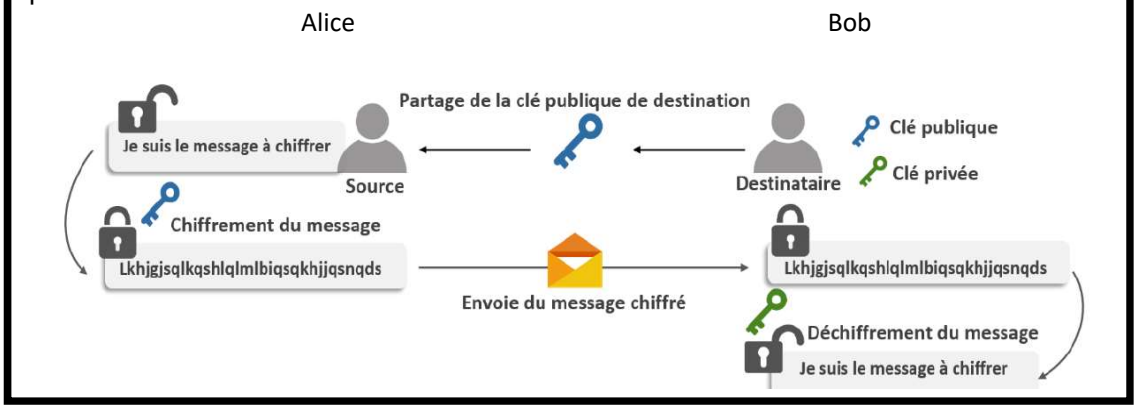


Figure 1. Chiffrement asymétrique

Le réseau Bitcoin utilise la cryptographie à clé publique basée sur les courbes elliptiques [8] afin de générer la paire de clés. La clé privée est un « grand nombre » généralement choisi aléatoirement. La clé publique en est dérivée par multiplication en courbes elliptiques.

La relation mathématique entre les deux clés permet d'utiliser la clé privée pour signer les transactions (pour émettre les Bitcoins) et la clé publique pour vérifier cette signature (pour recevoir les Bitcoins) sans que la clé privée ne soit révélée à d'autres personnes.

3.2.1 La signature numérique

L'autre concept cryptographique, la clé symétrique, est utilisé dans la blockchain dans le processus de signature numérique.

Cette dernière assure l'authentification des parties prenantes émettant et recevant les transactions.

Grâce à ce mécanisme cryptographique, il est impossible de falsifier une transaction générée et signée.

Ainsi, quand la source souhaite signer une donnée à envoyer au destinataire, elle commence par calculer le hachis (élément du cryptage expliqué au chapitre suivant) de cette donnée puis chiffre cette dernière avec sa clé privée.

Comme la source est la seule détentrice de sa clé privée, cette opération ne peut être réalisée par aucune autre entité.

Pour vérifier la validité d'une signature provenant de la source, le destinataire déchiffre, en utilisant la clé publique de la source, la donnée envoyée et vérifie qu'elle est identique au hachis de la donnée non chiffrée.

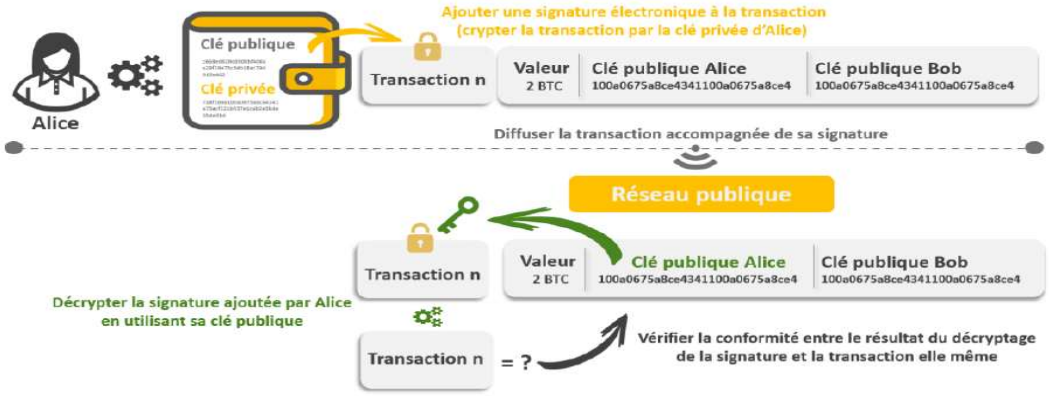


Figure 2. La signature assure l'intégrité de la transaction

3.2.2 La donnée enregistrable

A l'issue de ces échanges il est possible de caractériser la partie « monétaire » de la transaction par quelques données clefs (**origine des fonds, montant de la transaction, destination des fonds, datation de l'opération**…).

Ces données seront conservées et traitées au sein du « système » Bitcoin par des ordinateurs et des logiciels qui replacent la structure d'une banque et en jouent le rôle.

En particulier, la disponibilité des transactions depuis l'origine permet à tout instant de savoir si le « **porte-monnaie** (anonyme) » utilisé par l'acheteur contient au moins le montant de l'opération avec le complément d'une contribution destinée à nourrir la « réserve » Bitcoin.

C'est le rôle et le défi de la Blockchain (et des logiciels qui lui sont associés) d'être la base de données qui recueille toutes ces données, en assure une très grande protection contre toute tentative de modification tout en permettant une grande liberté d'accès.

3.3 Le "cœur de la blockchain", enregistrement et protection des données : hachage - construction du bloc - chaînage

Dans une base de données de type Blockchain les **« données »** ne sont pas regroupées dans un ensemble unique mais dans des **groupements de taille volontairement limitée (des blocs), créés au fil du temps et de la génération des « données élémentaires » que l'on veut ne plus être modifiées**, volontairement, accidentellement ou à la suite d'une action malveillante.

Lorsqu'un groupement de **« données élémentaires** », préalablement **revues, validées et acceptées** aura été constitué, il devra passer par certains traitements obligatoires afin d'être transformé en un **bloc infalsifiable**.

- Chaque donnée sera hachée (cf encadré) afin d'être caractérisée par une première **« empreinte ».**
- Ces informations (**données élémentaires et empreintes**) seront complétées par des informations de contexte (ex : horodatage, référence de validation, paramètres de cryptage …)
- L'ensemble ainsi constitué (**un bloc**) sera lui-même haché afin de générer « **l'empreinte du bloc »,** également appelée **« hash »** du bloc.

[8] Outil mathématique de construction d'algorithmes pour la génération de clés cryptographiques

3.3.1 **Le hachage**

Le principe du hachage des données est d'attribuer à toute donnée, petit fichier ou important dossier, une **empreinte numérique** calculée à partir de la donnée et nommée aussi **hachis (hash en anglais**). Cette empreinte permet de l'identifier parmi d'autres avec un bon taux de confiance (cf ci-dessous) et d'en vérifier l'intégrité.

Une « fonction de hachage » peut rendre différents services : elle peut rendre plus rapide l'identification d'un fichier (le calcul de l'empreinte d'un fichier nécessitant un temps négligeable au regard d'une comparaison complète de deux fichiers).

Elle permet aussi, après réception d'un fichier, de comparer l'empreinte reçue avec celle calculée par l'expéditeur avant son envoi, suivant des règles identiques.

Si les empreintes (hachages) ne correspondent pas, il est certain que le fichier a été altéré, accidentellement corrompu ou volontairement modifié, avant de parvenir au destinataire.

Le processus assure donc la fiabilité de la donnée transmise.

Afin d'en faciliter la lecture les empreintes, calculées en binaire, sont présentées en hexadécimal. L'empreinte MD5 est construite en 128 bits (32 caractères hexadécimaux) pour 256 bits pour SHA256

Exemples de hachage :

- « Académie » en **MD5** :
  86FDCB8DC8A81CF3DEEFD1FA9345E7E2

- « Academie » en **MD5** :
  A54C0CC336CA41B87EC7F929228FB87F

- « Académie » en **SHA256** :
  AE5247D4610C43DE2C795557E5243575C695E2F16EC54BC0FCE9F6D22ACC8A60

L'ancêtre de cette pratique consistait simplement à comparer la longueur des messages mais cette « empreinte » avait peu de capacité discriminante. Désormais de nombreux logiciels de « hachage » sont disponibles. Ils permettent de fournir des empreintes de bien meilleure efficacité discriminante. L'offre est large et le choix devra se faire en fonction des qualités nécessaires à l'atteinte des objectifs poursuivis (par ex : facilité d'usage ou grande sécurité …).

Les qualités importantes attendues d'un logiciel de « hachage » sont les suivantes :

- **Rapidité** : La production d'une empreinte, processus fréquent, doit être rapide,
- **Reproductibilité** : Un même fichier doit toujours produire une même empreinte,
- **Sécurité** : La connaissance de l'empreinte ne doit pas permettre de remonter au fichier haché,
- **Efficacité** : Le hachage, garantie l'authenticité des données, doit produire des empreintes différentes pour des entrées différentes,
- **Visibilité** : La **moindre modification** d'une entrée doit se traduire par une **importante modification** de l'empreinte.

Bien que l'une de ces qualités, **l'efficacité**, soit limitée par le simple fait qu'en hachant on cherche à réduire notablement la place occupée par l'empreinte par rapport à celle occupée par le fichier. Plus l'empreinte est petite, plus le risque augmente d'avoir deux empreintes identiques pour deux fichiers différents (situation de **collision)**. Afin de réduire ce risque on utilise des empreintes occupant de nombreux bits (128, 256 ou plus) aboutissant à des nombres très importants d'empreintes possibles ($2^{128} > 3x10^{38}$).

Il est ainsi possible de « figer » des fichiers d'informations. Il suffit, après les avoir « hachés » de **vérifier périodiquement, pour chaque fichier**, la non-modification de son empreinte par rapport à celle d'origine stockée « sous bonne protection ». Cette empreinte est aussi un moyen de retrouver rapidement un fichier particulier. C'est pourquoi la **technique du hachage est souvent utilisée dans la « Technologie Blockchain »** lors de l'intégration des données dans la base**.**

3.3.2 **Construction du bloc**

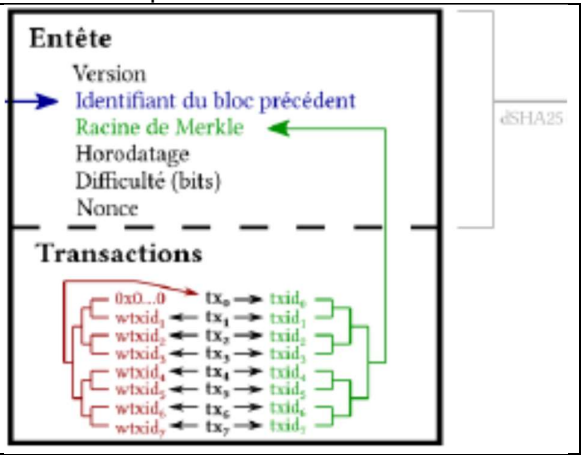
Lors de la constitution d'un bloc, chaque transaction fait l'objet d'un premier hachage qui lui attribue une empreinte. Les empreintes des différentes transactions sont ensuite combinées entre elles puis avec les données de contexte du bloc pour aboutir à une empreinte représentative du bloc. Cette dernière étant altérée pour toute modification même minime du bloc, constitue une alerte extrêmement sensible à la corruption des données stockées.

Exemple :

Structure d'un bloc Bitcoin

Les données sont ici des transactions.

Elles font l'objet de processus successifs de hachages et regroupements avant d'être finalement intégrées à l'ensemble des données de contexte et servir de source à l'élaboration de l'empreinte du bloc, son **« Hash »** :



Cette empreinte est construite en utilisant le principe de « l'arbre de Merkle »

Hachage - L'Arbre de Merkle

L'arbre de Merkle utilise un arbre binaire complet pour produire un ensemble de signatures à usage unique associées à une seule clé publique. On définit donc un arbre de Merkle comme étant un arbre binaire complet avec une valeur associée à chaque nœud de façon que la valeur de chaque nœud interne à l'arbre soit le résultat d'une fonction à sens unique appliquée aux valeurs de ses nœuds descendants.

Pour visualiser cela, nous pouvons voir sur la figure suivante qui décrit un arbre de Merkle simplifié lié à un bloc donné où T désigne une transaction et H désigne un haché. Le hachis de toutes les transactions du bloc entier est obtenu en hachant séparément chacune des transactions puis en les regroupant deux-à-deux et hachant la concaténation et ainsi de suite jusqu'à n'avoir qu'un seul hachis qu'on appelle « racine de Merkle » qui représente le hachis final du bloc. S'il y a un nombre impair de transactions, une d'entre elles est doublée en gardant une trace et son hachis est concaténé à lui-même.

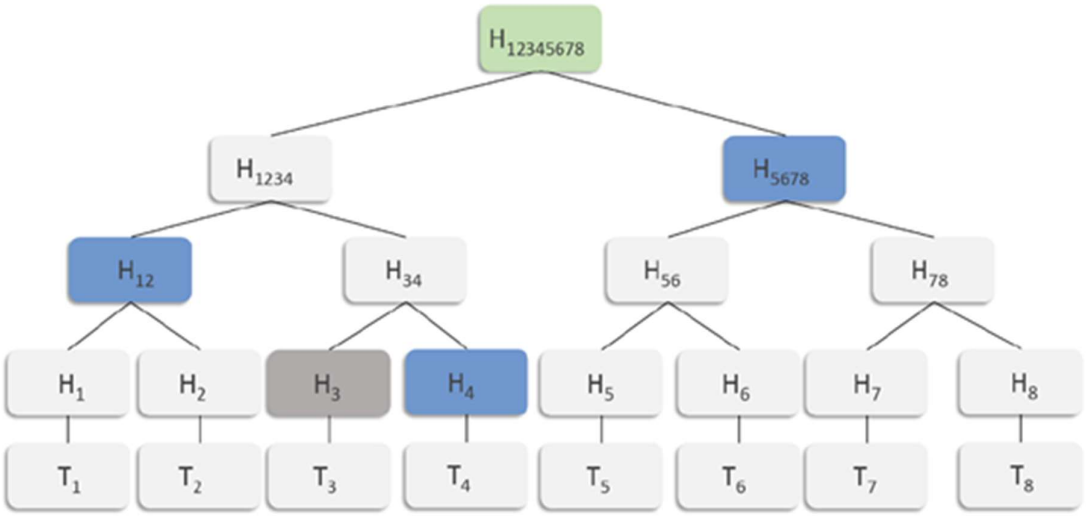


Figure 1 Exemple de vérification d'une transaction dans un arbre de Merkle

Afin d'illustrer l'utilité de cette structure imaginons qu'un bloc donné dont le hachis de Merkle est H12345678 veuille vérifier l'existence de la transaction T3. Au lieu de télécharger toutes les transactions (qui peuvent être très volumineuses dans la réalité d'une Blockchain), on va cibler les hachis qui nous permettent de remonter de H3 vers la racine de l'arbre. On récupère donc seulement H4, H12, et H5678. Laissant ainsi le dernier hachis manquant pour pouvoir remonter à la racine dans la donnée à vérifier T3.

L'exemple ci-dessus décrit le processus de hachage, particulièrement sophistiqué, utilisé pour l'application Bitcoin. L'objectif peut même être atteint en utilisant un protocole de hachage plus « rustique ».

Après un tel traitement, toute modification d'un élément du bloc se traduira par une modification de son empreinte.

3.3.3 **Le chaînage**

Une dernière opération pour faire de ce bloc de données un élément de la Blockchain est de le rattacher aux autres blocs pour constituer une « chaîne ». Cette opération de « **chaînage** » est faite au fil du temps. Après la création d'un premier bloc au démarrage du système (genesis, genèse en français), les blocs suivants sont ajoutés chronologiquement. De structure commune, chaque bloc ajouté est relié au précédent par **l'inclusion, dans ses données de contexte, du « hachis » du bloc précédent.** Cette simple mesure, en liant un bloc nouvellement créé aux blocs anciens, rend de plus en plus[9] difficile une modification malveillante ou accidentelle des blocs anciens, donc de l'information qui y est stockée. Cette information **est ainsi rendue de plus en plus infalsifiable**. La « Blockchain » c'est une chaîne de blocs dans laquelle chaque bloc tire profit de l'existence de la chaîne.

Le chaînage

Figure 2 Exemple de vérification d'une transaction dans un arbre de Merkle

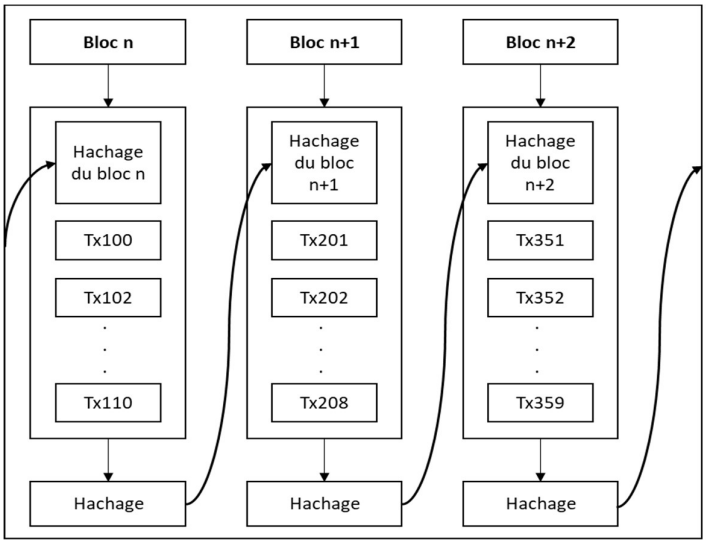


Figure 2. Structure générale de la Blockchain Bitcoin

La règle édictée lors de la création de la Blockchain impose que le hachis du bloc précédent soit ajouté au bloc courant. Lors de la création d'un nouveau bloc, le **hachis du dernier bloc de la chaîne** est combiné avec les transactions prises en charge et les données de contexte pour constituer un nouveau bloc qui devient la nouvelle extrémité de

[9] Ainsi, plus la chaîne est longue, plus le processus d'ajout de blocs est dynamique et plus elle est répliquée, moins elle est attaquable

3.4 Vie de la Blockchain : réplication, nœuds, réseau, minage, algorithmique partagée

La garantie évoquée précédemment est obtenue dans le cadre de la blockchain par la conjugaison de deux dispositifs : **la mise en place en parallèle sur de nombreux calculateurs de copies de la blockchain** d'une part et **d'un processus de surveillance de la non évolution des empreintes** (les Hachis) précédemment calculées. En cas d'évidence de modification d'une copie celle-ci peut être rétablie dans son état d'origine grâce à l'existence de copies majoritairement non altérées (consensus des nœuds par vote majoritaire).
La capacité de protection de ce dispositif dépendra donc des deux paramètres essentiels que sont la fréquence d'exécution du processus de surveillance et le nombre de nœuds (donc de copies) du réseau. **Plus fréquente est l'exécution, plus nombreuses sont les copies, meilleure sera la protection.** Ce principe nécessite que les copies existent en nombre suffisant pour qu'une action malveillante ne soit pas en possibilité de modifier une majorité des copies avant que le processus de surveillance ne détecte l'anomalie et ne la corrige.
IMPORTANT : Cette opération de surveillance est facilitée par l'usage du **hachage** mais aussi par une particularité importante d'une base de données structurée en « Blockchain ». Les enregistrements se font au fil du temps sans possibilité de revenir sur ce qui est enregistré. Aucune modification n'étant autorisée l'apparition d'un écart sur un Hash ne peut être que la preuve de la présence d'une altération à corriger.

3.4.1 Réplication, nœuds, réseau

Pour « **être infalsifiable** », la Blockchain a besoin d'un « **substrat** » constitué de **nœuds informatiques.** Reliés entre eux par un **réseau pair à pair,** ils échangent en permanence. Chaque nœud (moyen de calcul) dispose, outre d'une copie de la blockchain et d'un ensemble de logiciels permettant, **à côté de la simple surveillance** de l'intégrité de la base de données, **d'assurer de manière autonome et collaborative toutes les actions nécessaires à la « vie » de la Blockchain et du service qui l'utilise** : gestion et validation des données (en particulier des « transactions »), des blocs et des échanges nécessaires entre nœuds, respect des règles édictées pour la Blockchain (nature et structure, i.e. fond et forme, des informations), formalisation des transactions et vérification de « l'approvisionnement des comptes » … .

La recherche de garantie « d'infalsifiabilité » peut être complétée par l'utilisation de la cryptographie lors de l'inscription des données dans un bloc, afin d'augmenter la protection contre les écritures illicites. Ces différentes mesures (hachage, cryptographie, multiples copies…) font que l'attaque simultanée et réussie d'une majorité des copies (nécessaire pour corrompre l'enregistrement) devient extrêmement difficile à mener (car nécessitant une puissance de calcul gigantesque sans rapport avec le gain escompté de l'attaque), donc peu probable.

Grâce à l'existence de nombreux exemplaires identiques de la chaîne de blocs et aux différents rôles tenus par les nœuds, la monnaie « Bitcoin » peut se passer d'organe central (tiers de confiance, tel que le banquier) pour gérer et garantir la conformité des opérations réalisées.

3.4.2 **Validation d'un bloc (le minage)**

Un nœud quelconque peut, avec l'accord de ses « pairs », **proposer la constitution d'un nouveau bloc** de données contenant le hachis du bloc précédent et respectant les règles édictées pour la Blockchain (taille du bloc, contenu accepté …). Ce n'est qu'après leur accord (**« consensus des nœuds »** sur la validité de ce bloc) que ce nouveau bloc pourra être ajouté à la « chaîne ».

Les messages (les transactions) sont largement distribués sur l'ensemble du réseau. **Sur une période donnée,** chaque nœud du réseau reçoit de nombreux messages de nombreux **fournisseurs.** Après réception d'une quantité suffisante de messages, **chaque nœud peut** les combiner en un seul bloc. La taille maximale d'un bloc sur le réseau Bitcoin a été fixée à 1 Mo, ce qui correspond à quelques milliers de transactions "standard".

De fait si tous les nœuds disposent des mêmes informations ils pourront tous lancer la constitution d'un nouveau bloc au même instant et sur les mêmes bases. [10]

Mais il ne suffit pas de rassembler des transactions « valides » il faut aussi ajouter une information pour compléter le bloc (**le nonce** - cf structure d'un bloc en bitcoin) de sorte que le **hachis obtenu commence par un certain nombre de 0**. Trouver un tel nombre est une opération lourde, nécessitant une grosse puissance de calcul. Les nœuds acceptant de faire ce travail s'appellent des « mineurs », **ils sont récompensés lorsqu'ils réussissent (POW - proof of work)**. Mais cette contrainte a l'intérêt de rendre plus difficile la falsification de la chaîne.

Après cette opération si un tiers modifiait le contenu de ce bloc son hachage serait modifié et le bloc serait considéré comme invalide.

De plus chaque message étant horodaté sa date ne peut pas être modifiée sans que soit affectée la valeur de hachage du bloc. La protection des messages du bloc est ainsi renforcée contre les altérations.

Le minage dans le Bitcoin : une opération lourde

Au-delà du travail de vérification des transactions intégrées dans le bloc, le protocole du Bitcoin demande que le hachis d'un bloc commence par un certain nombre de 0. Ce nombre dépend de la difficulté du problème, plus on augmente le nombre de 0 plus la validation devient difficile, ainsi un 0 de plus fait doubler la difficulté. Cette dernière est ajustée périodiquement chaque 4 semaines (qui correspond aussi à la validation de 2016 blocks) de telle sorte qu'on reste sur un débit de validation de l'ordre d'un bloc par 10 min. Pour avoir un bloc dont le hachis commence par un certain nombre de 0, il faut ajouter aux informations incluses dans le bloc (transactions et données de contexte) une donnée complémentaire (256 bits), appelée le **nonce**, afin d'obtenir pour le bloc une valeur du Hash respectant la contrainte décrite. Etant donnée l'irréversibilité d'une fonction de hachage, **trouver une telle valeur demande beaucoup de calcul** nécessitant de nombreux essais de hachage. La seule manière d'obtenir cette valeur c'est de la générer aléatoirement et calculer le hash du bloc pour tester si celui-ci commence par un certain nombre de 0 (un processus répétitif). Le premier mineur qui aura obtenu une telle valeur pourra proposer sa version du bloc à l'accord des autres nœuds. Les autres mineurs peuvent très facilement vérifier la validité de cette valeur de nonce par un simple calcul de hash. **Le mineur ayant trouvé cette valeur** sera rémunéré et son bloc sera ajouté à la chaîne de tous les nœuds et les mineurs travailleront à la préparation du bloc suivant.

[10] NB : dans le cas du Bitcoin, le passage de ce stade à celui d'un bloc acceptable est une opération lourde qui, du fait de la rémunération qui lui est attachée, entraîne une forte compétition entre les nœuds (chasseurs de prime).

3.4.3 Consensus et algorithmique distribuée - au cœur de la blockchain

A l'origine, le principe est de construire un réseau ne comportant aucun nœud prépondérant : la règle est identique pour tous. Ils effectuent toutes les opérations élémentaires assignées aux nœuds, grâce aux mêmes logiciels et aux mêmes règles. Ils échangent en permanence les informations de travail. Ils doivent en particulier donner leur accord pour tout enrichissement de la chaîne. C'est un parfait exemple **d'algorithmique distribuée.**

Il n'y a pas de chef d'orchestre, c'est l'ensemble des nœuds qui « décide » dans un mode de gouvernance « démocratique » dans le cadre des règles définies. Ce processus de « **consensus** » intervient aux 2 étapes clefs de l'enregistrement : **la validation des données** élémentaires à prendre en compte et **l'acceptation pour intégration d'un bloc** de données. Pour cela, chaque nœud peut proposer un nouveau bloc intégrant les données élémentaires déjà validées et à sa disposition.

L'accord de l'ensemble des nœuds et la mise à jour de la chaîne s'établissent ensuite sur la base d'une « vérité » constituée par calcul à partir de « l'avis » majoritaire des nœuds : c'est le **consensus**.

Enfin ce fonctionnement étant par nature asynchrone il s'expose à la loi édictée en 1985 sous la forme du théorème FLP (Fisher, Lynche et Paterson) : « Il est impossible de résoudre de manière déterministe le consensus dans un système asynchrone, en cas de défaillance de processus ».

Remarque : Dans ce fonctionnement « distribué », tous les nœuds disposent des mêmes informations au même instant et tout devrait être cohérent. Mais cette condition n'est jamais totalement respectée du fait de l'asynchronisme induit par le décalage des actions, les temps de calcul et les temps de transit des informations. C'est ainsi que la construction d'un nouveau bloc peut commencer par des nœuds éloignés disposant d'informations potentiellement différentes (blocs différents ou bien propositions différentes de validation de mêmes blocs, avec des empreintes différentes).

Le processus de consensus se déroule dans des intervalles de temps discrets prédéfinis qui ont un lien avec le délai entre transaction et ajout à la blockchain. Le délai de confirmation dépend de la taille du bloc, des volumes de transaction et des algorithmes de consensus utilisés. Dans le cas du Bitcoin, la recherche du consensus suit le principe du « Proof of Work », décrit dans le chapitre précédent. Pour information, les quatre algorithmes de consensus les plus reconnus sont [11] [24] :

- **Proof of Work (PoW)** : cet algorithme de consensus est l'algorithme le plus connu et le plus utilisé dans les différentes applications blockchain. Avec PoW, les mineurs décident de l'ajout des nouveaux blocs. Bitcoin et Ethereum sont les deux utilisateurs principaux de l'algorithme de consensus PoW [12][25].

- **Proof of Stake (PoS)** : dans cet algorithme de consensus, aucun mineur n'est présent. La validation du bloc est faite par les validateurs ayant participé à sa création. Ainsi, toute personne possédant un bien dans la transaction peut-elle être validateur de transaction. Contrairement à PoW, cet algorithme joue un rôle important dans la réduction de l'énergie et du temps consommés dans le processus de consensus.

11 Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, ''A blockchain based truthful incentive mechanism for distributed P2P applications,'' IEEE Access, vol. 6, pp. 27324–27335, 2018.
12 N. Andersen. (2016). Blockchain Technology A Game-Changer in Accounting. Accessed: Feb. 2, 2019. [Online]. Available:

Contrairement à PoW, cet algorithme joue un rôle important dans la réduction de l'énergie et du temps consommés dans le processus de consensus.

Néanmoins, le PoS n'est pas encore suffisamment mûr pour être pratiqué dans l'industrie comme le PoW [**Erreur ! Signet non défini.**] [25].

La nouvelle version d'Ethereum 2.0 apparue en 2020 est progressivement en train de migrer vers un algorithme de consensus du type Poof of Stack (PoS).

- **Proof of Authority (PoA)** : avec cet algorithme, seuls les comptes et les utilisateurs approuvés peuvent placer de nouvelles transactions dans les blocs.

  Ainsi, cette approche pourrait être considérée comme un modèle plus centralisé, qui permet un processus de consensus plus rapide[**Erreur ! Signet non défini.**].tolérance aux pannes byzantines [13]pratiques : dans cette approche, une première réplique et une seconde réplique sont utilisées dans le processus de consensus.
  La seconde évalue en permanence les décisions correspondantes à la première dans les blockchains et prend toutes les mesures nécessaires pour la corriger[**Erreur ! Signet non défini.**].
  Cet algorithme est adapté dans le contexte de blockchain privées où les acteurs du système sont connus.
  L'algorithme peut tolérer jusqu'à un tiers de pannes byzantines (comportements malhonnêtes, crashes de systèmes et erreurs de calcul) provenant des nœuds formant la blockchain. Il faut prévoir au moins 2/3 de nœuds honnêtes dans le réseau pour assurer le bon fonctionnement de cet algorithme.

3.5 Complément - Les différents nœuds dans le bitcoin

https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

[13] Définition Wikipédia : En informatique, on appelle panne byzantine ou comportement byzantin tout comportement d'un système ne respectant pas ses spécifications, en donnant des résultats non conformes1,2. On distingue couramment les **pannes byzantines naturelles** des **pannes byzantines volontaires**.

- Les pannes byzantines naturelles proviennent généralement d'erreurs physiques non détectées (mémoire, transmissions réseaux, etc.).
- Les pannes byzantines volontaires proviennent principalement d'attaques visant à faire échouer le système (sabotage, virus, etc.).

L'authentification et la signature par des moyens de cryptographie permettent de limiter les erreurs byzantines.

A l'origine du Bitcoin, le principe était de construire un réseau ne comportant aucun nœud prépondérant. En pratique, 4 types de nœuds coexistent.

3.5.1 Nœuds complets

Ces nœuds **stockent une copie exacte, complète de la blockchain Bitcoin**. En outre ils participent à la validation d'un nouveau bloc en confirmant préalablement à sa prise en compte qu'il est conforme à toutes les règles établies.

3.5.2 Nœuds miniers

Les nœuds miniers sont des nœuds complets qui, en plus de stocker une copie complète de la chaîne de blocs, **font également fonctionner un logiciel d'exploitation minière**, dans le but de préparer de nouveaux blocs. Ce sont les nœuds d'origine.

3.5.3 Super-nœuds

Les super-nœuds, sont des nœuds complets **qui fonctionnent de manière ouverte et publique.** Actuellement, on estime qu'il y a environ 10 000 super-nœuds Bitcoin publics. Ces nœuds fonctionnent comme points de communication et d'interconnexion avec les autres nœuds du réseau.
.

3.5.4 Nœuds légers

Les nœuds légers ou nœuds de diffusion **ne participent pas à la validation des transactions.** Ils fonctionnent en relation et au travers des super-nœuds. Ils n'ont pas besoin de stocker une copie complète de la chaîne de blocs et peuvent être implantés sur les appareils mobiles tels que les téléphones et les tablettes.

4 Les évolutions de la « BLOCKCHAIN »

4.1 La Blockchain « post Bitcoin »

Désormais le terme ne couvre plus la seule base de données mais inclut les outils algorithmiques qui l'entourent et qui peuvent gérer beaucoup plus que la seule fonction d'enregistrement et de protection des données. La description de ce nouvel ensemble peut être enrichi.

La blockchain « post bitcoin » en bref

- **Il s'agit d'une base de données communautaire organisée sous la forme d'une succession de blocs de données.**

- **Chaque membre de la communauté peut disposer d'une copie de la base de données abritée sur son ordinateur.**

- **Tous les logiciels nécessaires à la gestion et à l'évolution de la base de données sont aussi installés sur chacun de ces ordinateurs et fonctionnent en automatique.**

- **L'ensemble est constitué en réseau de « pair-à-pair » où tous les « nœuds » sont équivalents, dialoguant et se coordonnant en permanence afin :**
  - **d'autoriser l'enregistrement d'une nouvelle donnée,**
  - **de constituer et d'accepter un nouveau bloc,**
  - **de mettre à jour l'ensemble des copies,**
  - **de détecter toute falsification des données stockées,**
  - **de rejeter les copies qui auraient été falsifiées.**

- **Ces décisions sont prises par vote majoritaire des nœuds, sans intervention humaine.**

- **La chaîne de blocs s'allonge au fil du temps, ce qui renforce son infalsifiabilité. Une donnée enregistrée ne peut donc être modifiée ou supprimée.**

- **L'accès aux données enregistrées est libre du fait de l'impossibilité de falsifier une donnée enregistrée.**

- **L'intégrité de la base est obtenue grâce à la comparaison fréquente des copies (permises grâce aux mécanismes de hachage et chiffrement asymétrique). Leur nombre et la fréquence de comparaison seront ajustés en fonction de l'importance et de la protection attendue des données stockées.**

Pour s'adapter à de nouveaux usages et tenter de contourner les réserves exposées beaucoup de travaux ont été engagés et de tentatives d'ores et déjà faites afin d'adapter la blockchain.

Pour juger de la pertinence des évolutions en cours ou de leur intérêt pour de nouvelles applications il convient de rappeler les quelques éléments clefs qui font **la réputation (le visible) et la performance (les solutions techniques)** de la blockchain façon Bitcoin.

- Autoprotection contre la falsification de l'information enregistrée
- Accessibilté aisée à l'information stockée.
- Confiance dans la qualité de l'information stockée.
- Rapidité de réaction du « système » tant pour l'enregistrement que pour la surveillance des données.
- Base de données structurée en blocs historisés et chaînés.
- Multiplicité des copies de la base de données gérées et protégées.
- Surveillance permanente de l'intégrité des données stockées grâce à la surveillance des empreintes crées par « hachage ».
- Intrication de l'outil de surveillance et de la base de données.
- Algorithmique parallèle.
- Régénération automatique des données en cas de falsification/corruption d'une partie minoritaire des copies gérées.
- Fonctionnement basé sur des relations entre « pairs ».

C'est ainsi que l'auto-protection repose sur l'existence de nombreuses copies et de comparaisons très fréquentes entre ces copies. L'attaque d'une blockchain implique donc l'attaque simultanée d'une majorité (plus de 50%) des copies, ce qui représente un coût et un effort disproportionné (puissance de calcul et consommation électrique) par rapport au gain escompté.

4.2 Premières évolutions de la blockchain

Outre l'existence d'un algorithme de consensus, sur le modèle éventuel du Bitcoin, les chaînes de blocs peuvent différer par leurs « modèles d'autorisation » accordée aux utilisateurs du réseau. C'est sur ce thème qu'ont ainsi émergé trois types principaux de blockchains :

- **Public :** ouvert à tous les utilisateurs : tout le monde peut rejoindre et ajouter à la blockchain à sa guise en suivant la règle du consensus définie. Chacun peut créer de nouveaux blocs dans le respect des règles.

- **Privée** : La blockchain privée répond à quelques critères : Communauté fermée et valideur centralisée, stockage décentralisée au niveau des nœuds. Les participants de la blockchain font tous partie de la même organisation. Ils sont préalablement définis. Le système de consensus employé est de nature centralisée et régi par les acteurs de la même organisation. L'accessibilité aux données peut être libre en lecture au public. Une seule organisation définit les règles du jeu et seuls les acteurs habilités par cette organisation peuvent y intervenir. Aujourd'hui, ce type de blockchain est principalement utilisé pour permettre à des utilisateurs non aguerris de s'approprier le fonctionnement d'une blockchain.

- **Consortium** : La blockchain consortium concerne plusieurs organisations et répond à quelques critères : Communauté fermée d'organisations ne se faisant pas mutuellement confiance, stockage décentralisée au niveau des nœuds. Les organisations sont ainsi préalablement définies. Un ensemble d'organisations définit les règles de participation et d'intervention. Des nœuds de validation existent dans chaque organisation. La validation entre organisations s'effectue par consensus entre elles. Il s'agit d'une blockchain hybride entre blockchain privée et publique.

Les qualités et spécificités des différents types de blockchain sont indiquées ci-dessous :

	Publique	**Privée**	**Consortium**
Décentralisation	Complète	Aucune	Partielle
Sécurité	Très forte	Faible	Moyenne à forte (selon le nombre de nœuds)
Capacité de passage à l'échelle	Non (débit de transactions très faible)	Forte (validation rapide de transactions)	Moyenne
Privauté (privacy) des données	Moyenne (pseudo anonymisation)	Forte	Variable (selon le cas d'usage)
Confidentialité des données	Aucune (nécessité de crypter)	Assurée (par l'organisme gestionnaire)	Assurée (selon le cas d'usage)
Transparence	Totale	Inexistante (équivalente à une base de données)	Partielle
Mécanismes possibles pour le consensus	*PoW, PoS, DPoS*	*Raft, PBFT, BFT, PoA, Paxos*	*Raft, PBFT, BFT, PoA, Paxos*

En résumé :

- Une **blockchain publique** possède généralement un nombre important de nœuds rendant ainsi la phase de validation des transactions plus longue contrairement à une blockchain privée.
- Une **blockchain privée** permet de garantir la confidentialité des données alors que dans une blockchain publique, toutes les informations sont accessibles à tous les membres du réseau.
- Dans une **blockchain publique**, toute transaction peut être vérifiée par le public alors que dans une **blockchain privée** seuls les utilisateurs de confiance peuvent vérifier et valider une transaction.
- Les **blockchains privées** sont caractérisées par le fait d'avoir un nombre plus restreint de nœuds, ce qui les rend plus vulnérables aux attaques. En effet, plus une blockchain a de nœuds plus la falsification est difficile.

Si ces évolutions permettent de simplifier la mise en œuvre d'une Blockchain donc d'en répandre l'usage, elles n'affectent en rien la nature de cette technologie qui reste dédiée au **stockage indélébile de simples informations.**

4.3 Le « Smart Contract » : de la gestion de données à la gestion d'exécutables informatiques

Dans le cadre du Bitcoin, la Blockchain abrite le résultat de transactions impliquant deux individus (ou entités) sans rentrer dans les détails de l'objet de la relation (qui n'est qu'un simple échange entre les deux entités).

Dans la vie courante, de nombreuses situations impliquent relations et échanges entre plusieurs individus (ou entités) et nécessitent une contractualisation lourde des engagements et devoirs de chacune des parties. Chaque acteur impliqué dans un contrat doit faire confiance aux autres et doit remplir sa part d'obligation du contrat. Dans ce système classique, les parties prenantes doivent avoir recours à une entité digne de confiance, un notaire par exemple. Cette dernière maintient une copie originale du contrat et assure que tous les acteurs respectent toutes les conditions. **L'idée a germé de formaliser sous forme de programmes mathématiques les termes de tels contrats, et d'abriter ces programmes dans une blockchain pour profiter de son infalsifiabilité.** Les **contrats intelligents (smart-contracts**) sont un mécanisme fonctionnant sur une architecture Blockchain et qui permet d'aller au-delà de l'usage classique de crypto-monnaie ou de finance. Ils permettent la décentralisation des marchés de biens et services, en posant des règles de jeu et des conditions sur les transactions entre les acteurs de ces marchés.

Vitalik Buterin et les « contrats intelligents »

Passionné par le système de Bitcoin, dès l'âge de 17 ans, un jeune canadien, Vitalik Buterin, né en Russie et habitant à Toronto abandonne ses études en informatique pour se consacrer entièrement au Bitcoin (Eudes, 2014). Pourtant il arrive rapidement à la conclusion que le système est imparfait. Le jeune décide alors, à l'âge 19 ans, d'utiliser la technologie Blockchain pour un mécanisme bien plus généralisé que celui du bitcoin qui se limite à la validation des transactions de crypto-monnaies. Ce système nommé Ethereum intègre un langage Turing complet qui permet la validation de n'importe quel contenu numérique pour n'importe quel service, et offre aux développeurs d'applications une manière de les décentraliser, d'où la naissance des smart-contrats.

Un « **contrat intelligent** » maintient la notion d'accord pour agir ou ne pas agir, cependant il enlève le besoin d'une confiance centralisée. Cette confiance devient complètement décentralisée grâce à la blockchain. Dans un smart-contract, les règles que les acteurs doivent respecter sont définies sous forme d'un code informatique. Celles-ci seront exécutées et validées par la blockchain. Un smart-contract est à la fois défini par son code et exécuté automatiquement grâce à son code.

Un smart-contract est caractérisé par trois propriétés fondamentales :
L'autonomie : une fois le smart-contract validé et publié dans le registre distribué, il se suffit à lui-même et aucun acteur ne peut plus en modifier les termes.

L'autosuffisance : pour son bon fonctionnement, un contrat intelligent doit s'appuyer seulement sur les données stockées en blockchain. Par exemple, il doit avoir la capacité de mobiliser les ressources utiles (puissance de calcul ou volume de stockage), de lever des fonds à travers la fourniture de services ou l'émission d'actions, et les dépenser via les ressources disponibles.

La décentralisation : les smart-contracts sont décentralisés dans le sens où ils ne subsistent pas dans un seul serveur central ; ils sont distribués et auto-exécutés à travers les nœuds du réseau de la blockchain.

Les smart-contracts sont donc des contrats décentralisés, autonomes et "pseudo-anonymement" exécutables sur la chaîne de blocs. Ils sont écrits en langage informatique, constituent une couche interagissant avec la Blockchain et sont exécutés dans son environnement. Les acteurs, nœuds de la blockchain, mettent en place diverses stratégies d'exécution de ces contrats.

Ce concept, initialement introduit et développé par la plateforme Ethereum, permet de résoudre diverses problématiques émergentes via des applications industrielles.

5 Les applications industrielles existantes ou potentielles de la BLOCKCHAIN

La blockchain a dépassé le domaine de la crypto-monnaie et révolutionne maintenant plusieurs industries. Elles ont commencé à adopter la solution basée sur la blockchain pour améliorer les processus métiers.

On constate que les blockchains publiques ne répondent pas forcément à tous les besoins et aux autres cas d'usages de la Blockchain. Nous vous présentons dans ce paragraphe les évolutions effectives, envisagées ou envisageables de la blockchain avec quelques exemples.

5.1 Blockchain pour chaîne d'approvisionnement (supply chain)

5.1.1 Le besoin

Une chaîne d'approvisionnement est un ensemble d'acteurs qui jouent des rôles successifs et ramifiés de fournisseurs à clients et inversement. Chacun a sa responsabilité dans cette chaîne, et a des obligations et une autonomie d'action.

Dans une chaîne classique, l'intégrateur final garantit (de façon souvent peu transparente) la qualité du produit. Le client final peut même douter que son produit acheté est bien celui de l'intégrateur final. La confiance dans l'intégrateur final peut ainsi être compromise.

Le besoin identifié dans une chaîne d'approvisionnement est que l'intégrateur final reçoive bien le produit promis par le fournisseur initial et de fournir une garantie quant à la qualité du produit reçu.

Par exemple, plusieurs domaines d'application :

- Production de produits de luxe
- Traçabilité des œuvres d'art
- Production alimentaire,
- Production de médicaments
- Suivi des pièces automobiles et/ou de la fabrication des véhicules
- Suivi des pièces aéronautiques

5.1.2 Les outils et solutions pour répondre à ce besoin

Une solution Blockchain offre les avantages suivants :

- Absence d'autorité centrale de confiance remplacée par un ensemble de règles définies en commun par les acteurs de la chaîne,

- Quasi-impossibilité d'occultation, mauvaise foi, contrefaçon ou falsification d'informations ;

- Certification de la nature et de la provenance du produit vendu (origine, normes alimentaires, environnementales, de fabrication, de qualité, etc.),
- Traçabilité et transparence pour le client final ainsi que pour les acteurs intermédiaires en ce qui concerne les informations importantes pour la chaîne de production,

- Extension possible de la blockchain au produit lui-même pour connaitre ses propriétaires successifs.

NB : La traçabilité peut concerner les matières premières. Par exemple, le café produit par une coopérative en Amérique latine passe par différents intermédiaires (exportateurs, importateurs…). Le client final souhaite les identifier dans sa commande de café. Chaque marchandise est tracée grâce à un identifiant unique stocké et suivi dans une blockchain de type consortium. La blockchain est ici capable d'historiser toutes les informations liées à la traçabilité de la marchandise mais aussi tous les échanges de documents, contrats et certificats entre les différents acteurs. Elle historise aussi tous les flux d'information de transactions financières entre ces acteurs.

Cas particulier de la chaîne logistique dans les entrepôts ou les ateliers de fabrication : Des robots dotés de capteurs permettent d'assurer la traçabilité des colis dans une chaîne logistique. Quand les capteurs détectent le passage d'un colis à proximité, une blockchain peut récupérer cette information, la décentraliser et la rendre disponible aux différents acteurs de la chaîne logistique.

5.1.3 La maturité de ces solutions

Microsoft, le géant de la technologie, en collaboration avec Mojix, une start-up spécialisée dans les systèmes de radiofréquence (RFID), ont développé un système pour identifier les produits et les suivre dans les différentes étapes depuis la fabrication des pièces jusqu'à la livraison au client. Ce système, appelé Manifest, utilise la plateforme Ethereum et a été développé par une équipe de professeurs et étudiants au laboratoire RFID de l'université d'Auburn.

5.2 Blockchain pour applications de santé

L'industrie de la santé a également été identifiée comme une industrie majeure susceptible de bénéficier de la technologie Blockchain.

5.2.1 Le besoin

Le secteur de la santé est un écosystème vaste et complexe qui implique de nombreux acteurs : patients, médecins, chercheurs, infirmiers et autres acteurs périphériques. A l'échelle organisationnelle, voire individuelle, le système d'information, lui -même est complexe : partenariats intersectoriels, contrats gouvernementaux, besoins de santé publique. En matière de sécurité, le plus grand défi est certainement le manque de confiance des patients vis-à-vis de l'exploitation de leurs données de santé. Les patients doivent être assurés que leur dossier

médical est protégé des tentatives de vol de données personnelles et que seules les personnes autorisées y ont accès. Ce droit légitime est clairement stipulé dans les nouvelles règlementations européennes de protection de données personnelles et à caractère sensible.

Pour résumer, dans le domaine de la santé,

- Les caractéristiques recherchées sont : sécurité, confiance, respect du secret médical, traçabilité des médicaments.
- Des problèmes majeurs tels que les atteintes à la vie privée, les vols ou consultations indues de données, les coûts élevés et la fraude peuvent résulter d'un manque d'interopérabilité, de simplicité, de transparence, d'auditabilité et de contrôlabilité.
- La contrefaçon des médicaments est une préoccupation à la fois commerciale et citoyenne qui implique un besoin de traçabilité.

Ci-après sont listés quelques exemples d'application qui nécessitent une attention particulière en termes de sécurité et confidentialité :

- Applications de surveillance des patients à distance et notamment le suivi des vaccinations des patients atteints de la CoViD'19,
- Plateformes d'appel de la sécurité sociale pour les patients atteints de diabète
- Contrôle d'accès au dossier médical patient (DMP),
- Outillage d'analyse des cohortes dans le cadre d'études épidémiologiques ou de mise sur le marché de médicaments,
- Gestion de chaîne d'approvisionnement médical et traçabilité-sécurité des médicaments.

5.2.2 Les outils et solutions pour répondre à ce besoin

La Blockchain apporte un certain nombre d'avantages décrits ci-dessous

- **Transparence et vérifiabilité :** La Blockchain peut fournir un système immuable, transparent et vérifiable que les réseaux pair-à-pair classiques ne peuvent proposer. Elle peut aussi fournir une infrastructure plus simple et plus rentable par rapport aux infrastructures à clé publique (PKI) traditionnelles qui sont très souvent complexes.

- **Économie de coûts, confiance accrue, rapidité de traitement, haute disponibilité, absence d'erreur opérationnelle, fiabilité de la production :** l'utilisation de Blockchains privées ou en consortium peut répondre à l'ensemble de ces besoins.

- **Protection de la vie privée :** Dans les applications de santé, la blockchain utilisée doit être privée, cachant l'identité de tout individu avec des codes complexes et sécurisés pouvant protéger la sensibilité des données médicales. En plus des mécanismes de pseudo-anonymisation implémentés dans les blockchains privées, d'autres mécanismes cryptographiques tel que les outils Zero Knowledge Proof sont ajoutés pour renforcer la protection des données médicales sensibles. La nature décentralisée de la technologie permet également aux patients, médecins et prestataires de soins de partager les mêmes informations rapidement et en toute sécurité.

- **Maintien et suivi des DMP :** Les dossiers médicaux peuvent être maintenus et suivis dans la blockchain d'une façon immuable ce qui permet de mieux les protéger des tentations de falsification et prévenir les erreurs coûteuses. La nature décentralisée de la technologie crée un écosystème facilitant l'accès aux données sur les patients qui peuvent être référencées rapidement et efficacement par les médecins, les hôpitaux, les pharmaciens et toute autre personne impliquée dans le traitement. Ceci est rendu possible grâce aux mécanismes de hachage implémentés ainsi que les systèmes cryptographiques à clé publique permettant d'identifier d'une façon unique et vérifier l'authenticité de toute donnée ou transaction stockée dans la blockchain. De cette façon, la blockchain peut conduire à des diagnostics plus rapides et à des plans de soins personnalisés. Les smart contacts sont des outils essentiels qui permettent le suivi des DMP grâce à l'implémentation de fonctions nécessaires de suivi, modification, partage et attribution des droits d'accès, etc.

- **Approvisionnement des médicaments :** La blockchain a de sérieuses implications dans la gestion de la chaîne d'approvisionnement pharmaceutique, et sa décentralisation garantit pratiquement une transparence totale dans le processus d'expédition. Une fois qu'un registre pour un médicament est créé, on stocke le point d'origine de fabrication du médicament (c'est-à-dire un laboratoire médical). La blockchain continue ensuite à enregistrer les données à chaque étape, y compris qui les a traitées et où elles se sont trouvées, jusqu'à ce qu'elles parviennent au consommateur. Ce suivi est implémenté grâce aux contrats intelligents d'une façon autonome et sécurisé et qui implique tous les acteurs dans le processus de fabrication et expédition des médicaments.

Remarque complémentaire : Sous un autre angle, la Blockchain fournissant une monnaie virtuelle comme récompense aux preuves de travail, la puissance de traitement qu'elle mobilise permettrait de résoudre des problèmes scientifiques lourds en calcul. Cela pourrait aider à trouver des remèdes pour certaines maladies ou à réaliser les lourds calculs en recherche clinique. Nous pouvons citer à titre d'exemple la plateforme FoldingCoin qui récompense ses mineurs avec des jetons contre le partage de la puissance de calcul. . Un autre projet aussi ambitieux et similaire s'appelle CureCoin qui est disponible sur https://www.curecoin.net/. Il reste à savoir dans quelle mesure ces projets réussiront leurs objectifs, mais l'idée est très prometteuse.

5.2.3 La maturité de ces solutions

Plusieurs solutions ont émergé pour la protection des données médicales sensibles à l'image de Akiri, Factom, Medicalchain, Guardtime. Mais ces solutions restent dans un stade de prématurité à cause des nombreux freins technologiques et juridiques.

- Le cadre réglementaire qui régit la gestion des données personnelles - le Règlement Général sur la Protection des Données (RGPD) - s'applique à la technologie blockchain. Nombre de start-up négligent ce point dans le processus de développement des applicatifs, par méconnaissance.
- La définition de la gouvernance du réseau distribué qu'est la blockchain présente d'autres problématiques de taille : Qui pourra faire quoi sur la base de données ? Qui pourra les lire ? Qui pourra les modifier ? Répondre à ces questions de fonctionnement est essentiel pour s'assurer de l'efficacité de la blockchain dans le domaine médical. Cela doit être pensé en amont.

La technologie blockchain constitue une avancée considérable car elle apporte transparence et intégrité. Cependant, la réponse à tous les besoins mentionnés nécessitera des adaptations intelligentes et divers développements avant l'obtention de solutions totalement opérationnelles.

5.3 **Blockchain pour la sécurisation des réseaux télécoms**

L'évolution des réseaux Télécom, assemblage multi échelle de sous-réseaux, crée des vulnérabilités telles que d'importants problèmes de sécurité apparaissent. La Blockchain attire l'industrie des télécommunications [14], [15]. Permettra-t-elle de faire face à la croissance continue : des appareils sans fil, du trafic de données et des services ?

5.3.1 Le besoin

Malgré plusieurs avancées technologiques, les réseaux 5G (5ème Génération) ne sont pas encore complètement autonomes, autogérés, coopératifs et décentralisés. Les besoins sont : l'IoT(Internet of Things), [16], le D2D (Device To Device, en français, appareil à appareil), le V2V (Vehicle To Vehicle) [17], [18], l'Edge Computing [19][20], le Cloud/Fog Computing [21] et les RAN (Radio Access Network, en français, Réseau d'Accès Radio) [22].Les réseaux distribués et décentralisés sont essentiels au succès de divers cas d'utilisation de l'IoT, sur les plans informatique et stockage. Ils sont la base de tout cas d'utilisation nécessitant collaboration et coopération.

Les réseaux 5G gèrent une quantité massive de données générées par les appareils IoT et fournissent une connectivité à des milliards d'appareils avec un degré variable de QoS (Quality Of Service, qualité de service). La fourniture des services via une combinaison de plusieurs technologies implique une coordination et une collaboration complexes qui nécessitent un système ouvert, transparent et sécurisé. Par exemple, les réseaux de petites cellules ultra-denses dans l'infrastructure 5G utilisés pour fournir des hauts débits de données et de faibles latences introduisent des problèmes de sécurité et de fiabilité dans le réseau. Les

[14] Blockchains in Mobile Networks. Accessed : Mar. 20, 2020. [Online]. Available : https://e.huawei.com/us/publications/global/ict_insights/ 201703141505/core-competency/201703150928

[15] Blockchain Telco. Accessed : Mar. 20, 2020. [Online]. Available : https:// www2.deloitte.com/content/dam/Deloitte/za/Documents/technologymedia-telecommunications/za_TMT_Blockchain_TelCo.pdf

[16] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, ‘‘Survey on blockchain for Internet of Things,’’ Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.

[17] X. Zhang and X. Chen, ‘‘Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network,’’ IEEE Access, vol. 7, pp. 58241–58254, 2019.

[18] T. Jiang, H. Fang, and H. Wang, ‘‘Blockchain-based Internet of Vehicles : Distributed network architecture and performance analysis,’’ IEEE Internet Things J., vol. 6, no. 3, pp. 4640–4649, Jun. 2019.

[19] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, ‘‘When mobile blockchain meets edge computing,’’ IEEE Commun. Mag., vol. 56, no. 8, pp. 33–39, Aug. 2018.

[20] Edge Computing : traitement (calcul et stockage) de données délocalisé, sur le "bord" du réseau

[21] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, ‘‘Cloud/fog computing resource management and pricing for blockchain networks,’’ IEEE Internet Things J., vol. 6, no. 3, pp. 4585–4600, Jun. 2019.

[22] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, ‘‘Blockchain radio access network (B-RAN) : Towards decentralized secure radio access paradigm,’’ IEEE Access, vol. 7, pp. 9714–9723, 2019.

problèmes de sécurité peuvent survenir en raison de l'installation de Evil-Twin ("jumeau maléfique", procédé de piratage par hameçonnage par duplication de l'identifiant de l'appareil victime) alors que les problèmes de fiabilité peuvent résulter d'un transfert fréquent en raison de la taille des cellules. Par conséquent, fournir une connexion fiable et sécurisée est important mais en même temps difficile pour les réseaux 5G.

5.3.2 **Les outils et solutions pour répondre à ce besoin**

Physiquement, une solution 5G Blockchain s'appuie sur une architecture de réseau P2P (Peer-To-Peer, en français, pair à pair).

La blockchain fournit un référentiel fiable distribué, immuable et unique, sans intermédiaire. Elle constitue ainsi, pour le MWC (Mobile World Congress), une perspective intéressante pour les futurs réseaux 6G. La réalisation du plein potentiel des réseaux 5G nécessite l'utilisation de la Blockchain ce qui inclura à terme : la gestion autonome des ressources, la sécurité et la prévention de la fraude, le foisonnement informatique, la distribution de contenu fiable et la gestion de grandes quantités de données.

Le plus grand défi pour les plates-formes 5G est de garantir un système ouvert, transparent et équitable compte tenu du nombre de ressources et du risque d'utilisation malveillante[23]. La solution blockchain, avec ses caractéristiques uniques de décentralisation, son haut niveau de confidentialité des données, sa sécurité, sa transparence et son immuabilité, s'impose et doit être intégrée dans l'architecture 5G. Elle permet au réseau de devenir : auto-entretenu, auto-géré, capable d'effectuer des transactions, de gérer des mises à jour automatiques et sécurisées sans nécessité d'un courtier central. La Blockchain soutiendra une nouvelle génération de réseaux sans fil distribués, en permettant un approvisionnement transparent entre des nœuds d'accès et des appareils hétérogènes. Avec la Blockchain, les dispositions et les accords entre les nœuds d'accès, les réseaux et les abonnés sont, par définition, négociés à la volée, ce qui pourra se concrétiser en contrats intelligents numériques.

En outre, l'intégration de diverses technologies a conduit à une nouvelle architecture de base qui éliminera progressivement l'actuel protocole[24]

La blockchain permettra aux appareils du réseau de négocier le meilleur service avec l'opérateur de réseau, qui sera ensuite exécuté à l'aide du contrat intelligent. Ce modèle autorisera la fourniture de services personnalisés à des nœuds individuels sur le réseau, ce qui entraînera de nouveaux modèles de facturation et commerciaux dans le réseau 5G [25].

Les réseaux 5G fourniront une large gamme de services dans plusieurs secteurs verticaux, ce qui nécessitera une allocation rapide des ressources et une orchestration sécurisée et fiable du réseau. Pour répondre à la volée à des exigences aussi diverses, un degré élevé de coordination et de configurabilité dans le réseau est requis. De plus, les

[23] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, ‘‘Blockchain for 5G : Opportunities and challenges,’’ in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2019, pp. 1–6.

[24] EPC Evolved Packet Core (EPC) réseau central qui est une partie d'un réseau informatique qui interconnecte les réseaux, fournissant un chemin pour l'échange d'informations entre différents sous-réseaux dans le même bâtiment, dans différents bâtiments, d'un environnement de campus ou sur de vastes zones.

[25] M. A. R. Chaudhry and Z. A. Soptimizer, ‘‘Blockchain : A key enabler for 5G,’’ IEEE Standards Univ., vol. 10, no. 1, 2019. [Online]. Available : https://www.standardsuniversity.org/e-magazine/may-2019-volume-9- issue-1-blockchain-standards/blockchain-a-key-enabler-for-5g/

réseaux 5G, une fois généralisés, vont nécessiter l'ajout de plusieurs nouvelles technologies telles que l'Edge Computing, les petites cellules (Small Cells), le SDN (Software Defined Network), le NFV (Network Function Virtualisation), le cloud et le D2D (Device to Device).

La complexité du réseau 5G (et au-delà) pourrait dépasser la capacité technique et financière d'un seul opérateur. Les ressources pourraient être partagées entre plusieurs parties prenantes pour fournir des services aux utilisateurs finaux. Par exemple, l'infrastructure radio, le stockage et le calcul pourrait être partagés entre les opérateurs et le spectre loué. Par conséquent, dans le futur réseau 5G, un degré élevé de coordination serait requis entre plusieurs parties prenantes.

Certains des secteurs verticaux devraient être activés par la 5G :

- L'IoT pour plusieurs applications telles que la ville intelligente, les transports, le réseau intelligent, la surveillance des infrastructures critiques et la santé intelligente
- La communication de véhicule à véhicule
- Le jeu collaboratif,
- La diffusion vidéo
- La réalité augmentée (AR)
- La réalité virtuelle (VR)
- L'ultra haute définition (UHD).

Ces secteurs verticaux sont assez divers dans leurs exigences en termes de vitesse, de latence et de capacité.

5.3.3 La maturité de ces solutions

Toutes ces exigences n'ont pas encore obtenu toutes les réponses en matière de gestion, sécurité, confidentialité, accord de niveau de service (SLA) et interopérabilité.

La Blockchain, en particulier le consortium Blockchain, est la candidate la plus pertinente pour résoudre ces défis dans les réseaux 5G. Mais elle n'est actuellement utilisée que de façon timide.

Le réseau décentralisé de la blockchain peut parfaitement s'intégrer dans un réseau distribué comme la 5G avec plusieurs parties prenantes impliquées. Pour instaurer la confiance entre elles, tout en garantissant la sécurité, la confidentialité et le règlement sans tracas des cotisations, la Blockchain leur donnera accès transparent aux données sans monopole de contrôle. Chaque partie prenante doit alors conclure un accord de type SLA via un contrat intelligent. Ce dernier automatisera le processus d'allocation des ressources et d'orchestration du réseau pour fournir un service transparent aux utilisateurs finaux.

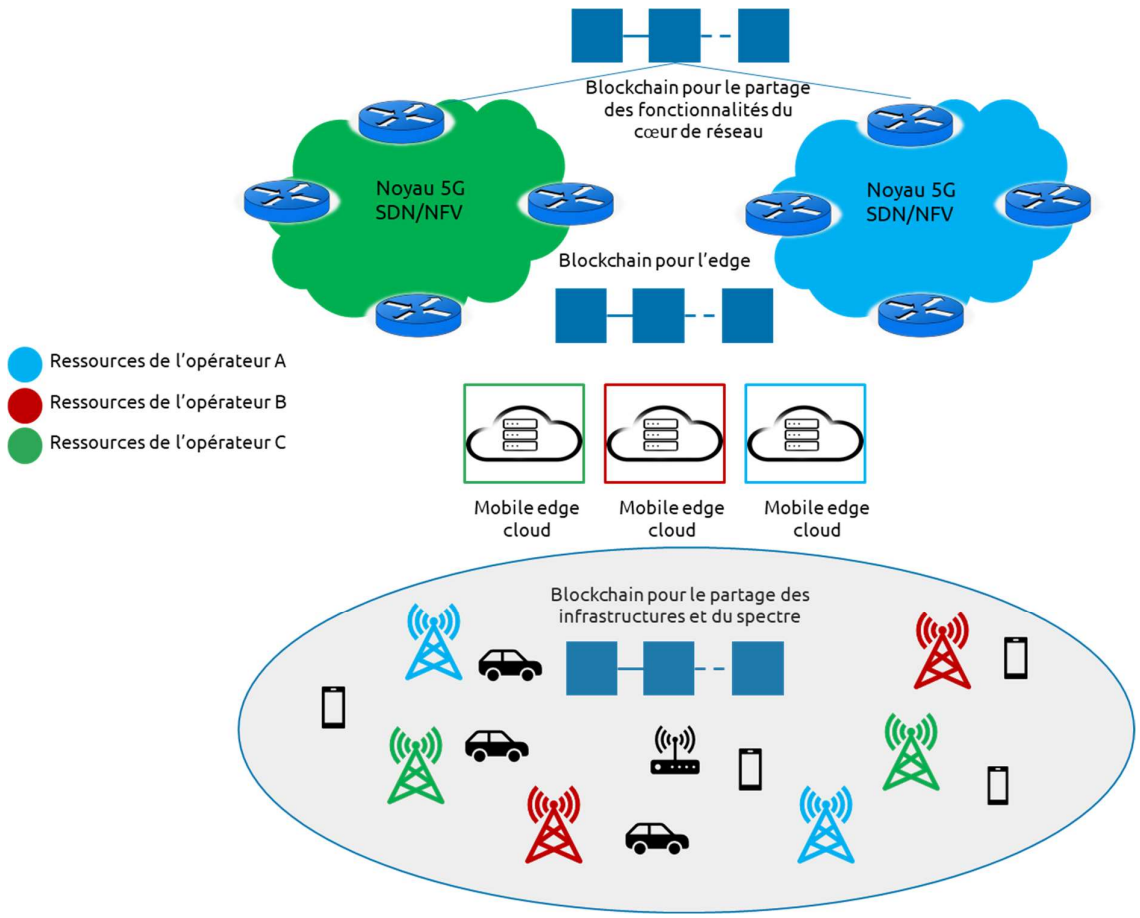


Illustration du fonctionnement de la 5G avec plusieurs opérateurs impliqués.

Le réseau 5G (et au-delà) peut ainsi, comme l'ont montré plusieurs études bénéficier des avantages de la Blockchain. Comme les futurs réseaux 5G devraient être de nature hautement distribuée et décentralisée, les problèmes de gestion et de sécurité du réseau deviennent plus nombreux et difficiles par rapport aux générations précédentes qui sont très centralisées. La Blockchain devrait résoudre les problèmes de sécurité fondamentaux tels que l'intégrité, l'authentification, la confiance et la disponibilité sur l'ensemble du réseau. Les contrats intelligents devraient permettre l'allocation/le partage de ressources de bout en bout, la gestion et l'orchestration du réseau fournissant les services 5G. La Blockchain autorisera ainsi plusieurs nouveaux modèles économiques, réduira les tracas associés à la coopération entre les opérateurs de réseau et gérera de manière transparente plusieurs processus.

5.4 Blockchain pour le financement participatif (Crowdfunding)

Le crowdfunding ou le financement participatif est une mode innovant de récolte de fonds permettant à des entreprises ou particuliers de financer leurs projets. Aujourd'hui, plusieurs plateformes (comme Kickstarter) jouent le rôle d'intermédiaire de confiance entre les porteurs de projets et les contributeurs.

5.4.1 **Le besoin**

Un porteur de projet souhaite présenter ses idées et son projet et définit un montant à atteindre pour le financer. Il faut récolter les fonds de contributeurs. Un processus à définir doit garantir que tous ces fonds sont transmis aux porteurs de projet en échange de la rémunération de ce service. Il est important que tous les acteurs, contributeurs et porteurs de projets, fassent confiance à la plateforme de Crowdfunding. D'un côté, les contributeurs doivent être sûrs que leur argent ira aux projets qu'ils souhaitent soutenir. Et de l'autre, les porteurs de projets doivent être sûrs qu'ils toucheront bien l'intégralité des donations et contributions. Dans le système actuel, ce besoin de confiance est délégué à un seul organisme central. Il y a donc un manque de transparence de décentralisation.

Dans un processus décentralisé de collecte de fonds, il est important que les porteurs des projets et les contributeurs aient confiance en les plateformes intermédiaires.

5.4.2 **Les outils et solutions pour répondre à ce besoin**

La blockchain et les contrats intelligents formalisent l'engagement entre tous les acteurs du financement participatif. Le contrat intelligent récolte de façon sûre le fruit des transactions des contributeurs vers les porteurs de projet. Ainsi est régi le processus fiable, décentralisé et autonome d'envoi et réception de fonds. Le contrat intelligent peut stipuler que l'atteinte du montant fixé pour la récolte de fonds déclenchera la validation des transactions et l'envoi des fonds au porteur du projet ; en revanche, si l'objectif n'est pas atteint dans un délai prédéterminé, les contributeurs ne seront pas débités.

Grâce à la blockchain, le processus de financement participatif est rendu complètement transparent, automatisé, protégé des fraudes et ce, sans entité jouant le rôle d'intermédiaire de confiance.

5.4.3 **La maturité de ces solutions**

Le financement participatif basé sur la blockchain est désormais très développé et prend plusieurs formes comme le ICO (Initial Coin Offering) et le STO (Security Token Offerings). De nombreux projets innovants ont vu le jour grâce aux mécanismes décentralisés de levée de fonds, basés sur la blockchain et les cryptomonnaies.

La première plateforme qui a collecté le plus de fonds grâce au mécanisme de levée de fonds ICO (Initial Coin Offering) est la plateforme Ethereum porté par Vitalik Buterin en 2015. La fondation Ethereum a levé l'équivalent de 18 millions de dollars et est devenue la cryptomonnaie la plus valorisée après le bitcoin.

Projet emblématique, la blockchain Tezos a aussi battu le record en 2017 avec une levée de fonds de 232 millions de dollars.

Le financement participatif est très développé aux Etats-Unis, mais moins développé en France, et ne représente que 4% des levées de fonds.

Une des premières levées de fonds en France a été sollicitée par la start-up B2Expand pour développer le jeu vidéo "Beyond The Void" et a récolté, via Ethereum, une somme de 110 000 euros.

D'autres levées de fonds ont été portées par l'INRIA (Institut National de Recherche en Informatique Appliquée) pour financer des projets de recherche autour du cloud distribué.

Ce projet a pu collecter l'équivalent de 12,5 millions de dollars (environ 2761 Bitcoin) en moins de trois heures via Novaxia NEO. Ce montant n'aurait jamais pu obtenir si rapidement avec les moyens de levées de fonds traditionnels comme le IPO (Initial Public Offering).

5.5 Blockchain pour les NFT « Non-Fungible Token » ou jetons virtuels non fongibles

Dans un contexte où le numérique prédomine de plus en plus dans notre mode de vie, les NFT (Non-Fungible Token ou jeton non fongible) sont considérés comme la dernière tendance pour valoriser l'authenticité d'un objet.

Il s'agit d'un concept séduisant à fort enjeu financier.

5.5.1 Le besoin

Les NFT explosent dans le domaine des œuvres : art, jeux vidéo, objets de collection (y compris numériques).

Cette technologie permet de donner une identité infalsifiable à des objets, pour en gérer la propriété et la rareté.

Ceci n'était pas possible jusqu'ici dans le domaine du numérique où tout était reproductible à l'infini.

La plupart des monnaies peuvent être qualifiées de fongibles, y compris des cryptomonnaies comme le bitcoin : si on échange un bitcoin contre un autre, sa valeur et son usage restent identiques.

A l'inverse, le NFT identifie une chose unique qui ne peut pas être remplacée par une autre, même reproduite à l'identique.

Pour être NFT-ables, les œuvres doivent être « certifiées » et rendues uniques et non fongibles (i.e. non divisibles et non interchangeables).

Le besoin est donc de construire une méthode de certification suffisamment robuste et fiable pour garantir et authentifier l'unicité d'un bien (œuvre d'art…) ou d'un concept (brevet…) et son traçage.

5.5.2 Les outils et solutions pour répondre à ce besoin

Cette certification peut être opérée virtuellement par le biais de la blockchain.
Dans le monde des NFT, la blockchain apporte une garantie que ces œuvres ne pourront jamais plus être reproduites.

Remarque : C'est la raison pour laquelle les NFT voient leur popularité grimper en flèche, en particulier, dans le monde de l'art.

Le rôle de la blockchain dans les NFT :

La plateforme où l'on trouve le plus de NFT est la blockchain Ethereum[26].

Grâce à la Blockchain, les acheteurs et les vendeurs peuvent retracer le parcours du NFT depuis sa création et identifier son propriétaire.

[26] Cette blockchain a sa propre cryptomonnaie : l'Ether.

Un jeton NFT est non fongible grâce à un certificat d'authenticité attribué par la blockchain. Il s'agit d'une propriété numérique inviolable.

Les données échangées sont transparentes et sécurisées par un système mondial et décentralisé, ce qui évite toute manipulation ou hacking.

Cette technologie de stockage fonctionne sans la présence d'un organe de contrôle.

Le créateur d'un NFT peut alors l'encoder sur la blockchain afin de rendre ses caractéristiques uniques.

La blockchain stocke toutes les informations sur les contrats, les transactions ou encore les titres de propriété.

Les procédés cryptographiques utilisés par cette technologie rendent chaque NFT infalsifiable et unique.

C'est la première fois dans l'histoire qu'une technologie permet de rendre unique cet objet essentiellement réplicable qu'est l'objet numérique.

Quel est l'intérêt ?

Pour l'artiste ou le vendeur (musique ou film, par exemple), c'est un moyen de s'imposer, avec l'œuvre unique et estampillée, au sein du marché sursaturé des œuvres reproduites légalement ou illégalement. En outre, les NFT peuvent inclure une clause d'intéressement à la revente (« sell-on clause ») qui fait bénéficier l'auteur d'un pourcentage sur chaque revente ultérieure.

L'intérêt d'acheter une œuvre avec NFT est de pouvoir s'afficher comme son propriétaire et de l'utiliser, ce qui peut contribuer au soutien de son auteur.

Certains utiliseront les NFT comme un actif spéculatif. Comme dans le monde de la cryptomonnaie, sa valeur peut connaitre des fluctuations inattendues.

Les NFT peuvent jouer un rôle important lorsqu'ils sont rattachés à des jeux vidéo. Un NFT peut donner accès à un classement spécial ou à un objet virtuel auquel les autres joueurs n'ont pas accès.

NB:

- *Les NFT reposent sur des contrats intelligents qui sont des programmes irrévocables exécutant automatiquement des instructions prédéfinies que le créateur lui-même ne peut amender après implantation.*
- *Le processus par lequel un artiste crée un NFT, c'est-à-dire par lequel il associe l'une de ses œuvres à un smart-contract, appose sa signature numérique, puis l'enregistre dans la blockchain, est appelé « minting » (monnayage)[27]. Il existe différents formats de NFT, les plus courants étant le format ERC 721 pour les œuvres tirées à un seul exemplaire et le format ERC 1155 pour les NFT en tirage numéroté.*

L'auteur peut ainsi décider librement des droits de propriété intellectuelle qu'il consent à transférer par l'intermédiaire du NFT. Par défaut, la vente d'un NFT n'entraîne pas de transfert automatique des droits de propriété intellectuelle afférents.

En effet, lorsqu'un acheteur se porte acquéreur d'un NFT, il n'achète pas l'œuvre : il se porte acquéreur du NFT, c'est-à-dire d'une reproduction de l'œuvre située au sein de la blockchain. Il n'est pas, par défaut, détenteur de l'œuvre elle-même ni des droits patrimoniaux qui s'y rattachent. Par conséquent, il ne saurait exploiter celle-ci à des fins commerciales, ni empêcher l'utilisation de celle-ci à d'autres fins.

Par défaut, l'acheteur obtient un simple droit, non exclusif, de jouir de la reproduction de l'œuvre associée au NFT, à condition que l'usage qu'il en fait soit personnel. Il peut ainsi par exemple exposer l'œuvre dans son crypto-portefeuille ou sur un service d'exposition de NFT en 3D. Il dispose également des droits de propriété afférant au NFT lui-même.

5.5.3 La maturité de ces solutions

Malgré l'apparition récente (2017) du concept NFT avec le jeu de société monétisé Cryptokitties, son marché est en pleine expansion et s'est développé très rapidement depuis 4 ans. Le marché des NFTs a atteint 9.2 milliards de dollars en 2021.

Au premier trimestre 2021, les NFT ont battus des records. Selon certaines études, les NFT auraient même dépassé les cryptomonnaies dans certains pays. Google Trend (octobre 2021) montre un intérêt croissant des recherches d'information sur les NFT.

Cette tendance est prédominante aux Etats Unis car les NFT couvrent divers secteurs artistiques et permettent de certifier les objets vendus sur ce marché (les droits d'auteur n'étant pas protégés pas aux Etats-Unis).

Il existe aujourd'hui plusieurs plateformes de vente des NFTs comme OpenSea, MakersPlace, Zora protocol, dont les opérations de vente et achat sont régies par l'offre et la demande.

La raison pour laquelle les gens paient des montants importants pour les NFT est que l'auteur, la propriété et l'unicité sont vérifiables.

L'œuvre conserve ainsi sa rareté donc sa valeur alors que, une fois copiée, elle perdrait toute originalité.

La communauté Ethereum travaille actuellement au développement d'une version améliorée de la norme ERC 721 qui permettrait la mise en place d'un standard commun.

Chaque auteur de NFT pourrait ainsi déterminer les modalités et le montant des royalties qu'il souhaite percevoir sur chaque transaction du marché secondaire intéressant son œuvre (vente, location).

Une telle évolution constituerait une avancée majeure dans le domaine de l'art. L'auteur n'aurait plus à suivre avec attention le parcours de ses NFT : le smart contract étant irréversible, il procéderait automatiquement au paiement de la somme due à l'auteur.

Il serait possible d'aménager contractuellement, avec beaucoup de souplesse, les droits attachés au NFT.

L'auteur pourrait ainsi décider de vendre concomitamment au NFT la totalité ou une partie des droits patrimoniaux s'exerçant sur son œuvre, ce qui permet de les louer.

5.6 Blockchain pour smartGrid

5.6.1 Le besoin

Le réseau intelligent ("smart grid") qualifie un concept de réseau, de son organisation et de sa gestion s'appuyant sur le "réseau conventionnel" et sur des technologies de calcul et de communication numériques.

Le réseau traditionnel et sa gestion centralisée sont transformés en un réseau de répartition et redistribution plus modulable, adaptable, précis, efficace, pour tout dire "intelligent".

Les "smart grid" ont vocation à intégrer des réseaux locaux appelés "micro-grid". Ce concept peut s'appliquer à des flux matériels ou immatériels : eau, gaz, électricité, information, etc..

Le changement climatique et la préoccupation de soutenabilité (économie, écologie et acceptabilité sociétale) de la gestion énergétique sont l'élément contextuel de ce concept.

La démocratisation des technologies de production locale d'énergie est un des autres éléments contextuels.

De nombreux acteurs ont été parallèlement incités à produire localement de l'énergie. S'est posé alors la problématique de l'intégration des flux d'énergie de ces petites unités de production dans un modèle de réseau dépassant largement le modèle centralisé descendant initial.

Ces transformations et modernisations participent à la transformation du paysage énergétique en intégrant davantage de sources renouvelables, réduisant ainsi l'utilisation de combustible fossile.

Alors que le "réseau conventionnel" dessert seulement les consommateurs via des lignes de "transport" et de "distribution", le réseau de type "smart grid" rapproche producteurs et consommateurs en incorporant des producteurs d'énergie indépendants voire des producteurs-consommateurs.

Plus récemment, le concept d'"Internet de l'énergie" (IE) a été introduit comme une version améliorée du "smart grid".

L'IE utilise les technologies Internet pour intégrer l'information, l'énergie et son économie. Il vise à :

- faciliter l'intégration transparente d'une production propre et renouvelable à partir de diverses sources d'énergies
- favoriser les interactions entre les nœuds du réseau qui devient ainsi décentralisé et intelligent.

L'idée clé est qu'avec l'énergie, soient véhiculées les informations et données de sa gestion. Ici, les nœuds du réseau incluent : les unités de production "traditionnelle", les "micro-grids", les ressources énergétiques distribuées, les unités de stockage d'énergie, les véhicules électriques, les systèmes cyber-physiques, les "pro-sommateurs" ("producteurs-consommateurs" cités plus haut), les fournisseurs de services et les marchés de l'énergie, etc.

Le "smart grid" et l'"IE" a pour vocation d'intégrer à la fois la génération centralisée (à longue distance) et la génération décentralisée (à courte distance).

L'émergence des énergies renouvelables et l'accroissement du nombre de nœuds du réseau impliquent pour le smart grid un certain nombre de défis techniques : la capacité de contrôle de l'ensemble, son évolutivité, son extensibilité, la charge de calcul et de communication et la cyber-sécurité.

5.6.2 Les outils et solutions pour répondre à ce besoin

Dans cette évolution vers des systèmes décentralisés, l'application de la blockchain paraît comme la technologie la plus appropriée pour faciliter cette transformation en raison des caractéristiques suivantes :

1. Décentralisation : Le réseau blockchain est basé sur un principe de nœuds décentralisés utilisant des protocoles de consensus. Ce réseau fonctionne de manière "pair à pair" sans que la confiance s'appuie sur une autorité et une maintenance centralisées.
2. Évolutivité : L'ajout non limitatif de nœuds au réseau blockchain découle structurellement de sa maintenance gérée par les pairs.
3. Robustesse et résilience : Dans le réseau Blockchain, toute panne, toute erreur ou toute activité malveillante est identifiée et sa correction facilement réalisée à partir des stockages locaux valides.
4. Sécurité : Les nœuds du réseau blockchain ne dépendent d'aucun intermédiaire de confiance pour communiquer les uns avec les autres. Tous les enregistrements et transactions sont sécurisés par cryptographie asymétrique, système reconnu comme sûr. La sécurité repose, de plus, sur la possibilité d'exécution automatique (i.e. sans intervention humaine, courtier et aucune autorisation centrale) de scripts en lien avec les "contrats intelligents"[28].
5. Immuabilité : Étant donné que la technologie blockchain utilise des techniques cryptographiques et maintient un registre global synchronisé entre les nœuds, le contenu des blocs ne peut pas être modifié[29].
6. Transparence et vérifiabilité : Par construction, le réseau Blockchain est transparent car tous les nœuds du réseau sont capables de vérifier l'authenticité et la non-altération de tous les enregistrements.

Avec les caractéristiques mentionnées ci-dessus et les avantages d'une sécurité cryptographique à jour, la blockchain constitue une intéressante alternative aux systèmes centralisés conventionnels améliorant robustesse, sécurité, confidentialité et confiance tout en éliminant la difficulté de gestion d'un système décentralisé.

Les avantages de la blockchain dans le domaine du smart grid sont :

- Adaptation au commerce et au marché décentralisés de l'énergie,
- Infrastructure décentralisée d'enregistrement en phase avec l'infrastructure de production-consommation,
- Adaptation à une gestion cyber-physique de l'énergie,
- Possibilité d'intégration des véhicules électriques et unités de rechargement,
- Intégration de la totalité des réseaux-sous-réseaux et des éléments du smartGrid.

5.6.3 La maturité de ces solutions

Afin de favoriser la progression de l'intégration de la blockchain et du réseau intelligent, plusieurs initiatives pratiques ont vu le jour plus récemment sous forme d'essais, de projets et de produits. Dans cette section, nous présentons les principaux projets de blockchain, les essais industriels et les produits axés sur différents scénarios de smartgrid en cours de déploiement et de publication.

[28] à moins que la majorité des nœuds ne devienne malveillante
[29] à moins que la majorité des nœuds ne devienne malveillante

- SolarCoin : SolarCoin [1] est une initiative visant à créer et à offrir des récompenses aux producteurs d'énergie solaire, qui vise à fournir des incitations pour une planète alimentée par l'énergie solaire. SolarCoin peut être défini comme des jetons numériques qui reposent sur la blockchain. Ces jetons numériques se maintiennent au taux de 1 SolarCoin pour 1 MWh d'énergie solaire produite. Le but est de renforcer le développement de l'énergie solaire à travers le monde. SolarCoin compense le coût de l'électricité, ce qui permet de rembourser rapidement les installations solaires. Les producteurs d'énergie solaire reçoivent gratuitement ce SolarCoin.
- NRGcoin : NRGcoin [2], [3] est en fait un projet industrie-université qui a été initialement développé à la Vrije Universiteit Brussel.
- Désormais, l'Enervalis (www.enervalis.com) a mis à jour ce projet en un contenu industriel. NRGCoin aide à intégrer les ressources d'énergie verte dans le réseau local en le rendant plus avantageux pour les producteurs et les services publics et plus économique pour les consommateurs et le gouvernement. Avec NRGcoin, l'énergie n'est pas forcément échangée, mais plutôt achetée et vendue au moyen d'un contrat intelligent. Ainsi, ce NRGCoin n'est pas considéré directement comme une approche de trading d'énergie P2P. En outre, NRGCoin ne se concentre pas uniquement sur l'énergie solaire et n'est pas simplement une crypto-monnaie. Au contraire, il soutient toutes sortes de ressources renouvelables et propres.
- Electronic Energy Coin : Le projet Electronic Energy Coin (E2C) [4] est présenté comme une plate-forme d'achat et de vente d'énergie verte développée à l'aide de la blockchain et d'un contrat intelligent. Ce projet vise une révolution énergétique en assurant une distribution d'énergie plus sûre, anonyme, juste et appropriée.
- KWHCoin : KWHCoin [5] est une crypto-monnaie basée sur la blockchain ainsi qu'une communauté qui est soutenue par des unités d'énergie propre. KWHCoin a pour vision de diriger l'expansion de l'énergie propre en réduisant le coût des transactions d'énergie blockchain. WHCoin agit comme un jeton pour une application décentralisée (DApp) où les producteurs et les consommateurs peuvent se connecter et configurer leurs ressources de production d'énergie.

[1] “Solarcoin a blockchain-based solar energy incentive whitepaper,” Accessed: November 2019, available: https://solarcoin.org/wp-content/ uploads/SolarCoin Policy Paper EN-1.pdf.

[2] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Nowe, “NRGcoin: Virtual currency for trading of renewable en- ´ ergy in smart grids,” in 11th International conference on the European energy market (EEM14). IEEE, 2014, pp. 1–6.

[3] M. Mihaylov, I. Razo-Zapata, and A. Nowe, “NRGcoin a blockchain- ´ based reward mechanism for both production and consumption of renewable energy,” in Transforming Climate Finance and Green Investment with Blockchains. Elsevier, 2018, pp. 111–131.

[4] “Electronic Energy Coin (E2C) whitepaper,” Accessed: November 2019, Available: https://electronicenergycoin.com/e2c whitepaper v2. pdf.

[5] “KWHCoin whitepaper,” Accessed: November 2019, available: https:// kwhcoin.com/whitepapers/KWHCoin-White-Paper-Revised-(English) .pdf.

5.7 Les autres plateformes blockchains publiques

Il existe d'autres types de blockchains publiques dont nous vous présentons ici deux exemples iconiques.

5.7.1 Ethereum

Nous avons vu précédemment au chapitre 4.4 les actions de Vitalik Buterin qui, par souci d'améliorer le système Bitcoin a créé le système Ethereum.

Grâce à l'arrivée du système Ethereum, la blockchain est désormais devenue une technologie qui sort complètement du cadre du monde de la finance et cryptomonnaies. Grâce aux systèmes de contrats intelligentes, la blockchain est utilisée pour développer des logiques métiers dans des applications diverses et variées.

5.7.2 Tezos

Tezos est une plateforme blockchain pour le déploiement de contrats intelligents. Sa cryptomonnaie est la Tez (ꜩ, XTZ). Les caractéristiques principales de Tezos sont :

- Être basé sur une preuve d'intérêt pour la cuisson de nouveaux blocs,
- Avoir un code open source et évolutif,
- Viser un processus démocratique concernant les décisions d'évolution,
- Élaborer des contrats intelligents dans sa propre langue appelée Michelson

Les fondateurs de Tezos sont Arthur Breitman (homme d'affaire franco-américain) et sa femme, à travers la Fondation Tezos, une organisation à but non lucratif basée en Suisse. Les premiers papiers menant à la création de Tezos ont été publiés en 2014 à travers une levée de fonds ICO (Initial Coin Offering) créé en 2017 et qui a battu le record avec 232 millions de dollars. Le langage cadre pour la blockchain est OCamlPro, et a été principalement développé par la société française Nomadic Labs. La chaîne est adaptée pour construire un nouveau bloc chaque minute, et bientôt va changer à 30 secondes.

L'algorithme de consensus de Tezos est basé sur le Proof of Stake qui signifie qu'afin d'être sélectionné pour valider un nouveau bloc dans la chaîne, un "boulanger" doit posséder un "rouleau" (ou s'être vu déléguer les droits de "cuisson") de 8000 ꜩ. La sélection se fait par tirage au sort.

Le "boulanger" voit une partie de ses jetons être immobilisée dans un dépôt de garantie jusqu'à ce que le blocage soit vérifié. Le "boulanger" sélectionné et les endosseurs sont récompensés une fois le bloc validé.

Ce procédé est considéré comme sécurisé, notamment en raison de sa faible récompense en cas de comportement égoïste.

Le principal avantage de ce processus est le faible coût de calcul de la création d'un nouveau bloc. Contrairement au Proof of Work, qui renforce la sécurité par le seul coût de forgeage d'un bloc, deux millions de fois celui du Tezos en coût énergétique.

Tezos, organisé comme un open source, permet à tout développeur de soumettre une proposition, afin de modifier, ajouter, supprimer une fonction dans le protocole. Les changements peuvent aller de la modification de la méthode d'approbation à la modification de la taille d'un "rouleau", en passant par l'amélioration du langage de codage des contrats intelligents et la modification de la taille des blocs.

L'idée principale derrière cela est d'éviter les hard fork[30]: si une partie du réseau d'une blockchain n'est pas d'accord avec les règles du jeu établies, une nouvelle version peut apparaitre et aura pour effet de diviser la communauté. Tezos propose un système de vote implémenté dans la chaîne pour valider chaque proposition. Pour voter sur les propositions, l'électeur doit posséder (ou avoir été délégué) certains droits (par exemple le rôle de "boulanger"). Les droits donnent droit à des votes qui se déroulent périodiquement (en principe tous les quatre mois).

[30] A l'origine, un hard fork est un changement de protocole qui rend les anciennes versions invalides. Si les anciennes versions continuent à fonctionner, elles se retrouveront avec un protocole différent et avec des données différentes de celles de la nouvelle version. Cela peut entraîner une confusion importante et des erreurs possibles.

Références et bibliographie :

[1] Z. Dong, F. Luo, and G. Liang, ‘‘Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems,’’ J. Modern Power Syst. Clean Energy, vol. 6, no. 5, pp. 958–967, Sep. 2018.

[2] T. Yang, Q. Guo, X. Tai, H. Sun, B. Zhang, W. Zhao, and C. Lin, ‘‘Applying blockchain technology to decentralized operation in future energy Internet,’’ in Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI2), Nov. 2017, pp. 1–5.

[3] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, ‘‘Blockchain technology in the energy sector: A systematic review of challenges and opportunities,’’ Renew. Sustain Energy Rev., vol. 100, pp. 143–174, Feb. 2019.

[4] L. Thomas, Y. Zhou, C. Long, J. Wu, and N. Jenkins, ‘‘A general form of smart contract for decentralized energy systems management,’’ Nature Energy, vol. 4, pp. 140–149, Jan. 2019.

[5] B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, ‘‘A critical review of blockchain and its current applications,’’ in Proc. Int. Conf. Elect. Eng. Comput. Sci. (ICECOS), Aug. 2017, pp. 109–113.
[6] (2018). Introduction to Smart Contracts—Solidity. Accessed: Nov. 26, 2018. [Online]. Available: https://solidity.readthedocs.io/ en/v0.5.3/index.html#
[7] R. Beck, ‘‘Beyond bitcoin: The rise of blockchain world,’’ Computer, vol. 51, no. 2, pp. 54–58, Feb. 2018.
[8] G. Karame and S. Capkun, ‘‘Blockchain security and privacy,’’ IEEE Security Privacy, vol. 16, no. 4, pp. 11–12, Jul. 2018.
[9] J. Moubarak, E. Filiol, and M. Chamoun, ‘‘On blockchain security and relevant attacks,’’ in Proc. IEEE Middle East North Africa Commun. Conf. (MENACOMM), Apr. 2018, pp. 1–6.
[10] M. N. Luke, S. J. Lee, Z. Pekarek, and A. Dimitrova. (2018). Blockchain in Electricity: A Critical Review of Progress to Date. Accessed: Nov. 10, 2018. [Online]. Available: http://www.energienachrichten.info/file/01%20Energie-Nachrichten%20News/2018-05/80503_Eurelectric_1_blockchain_eurelectric-h-DE808259.pdf
[11] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, ‘‘A review on consensus algorithm of blockchain,’’ in Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC), Oct. 2017, pp. 2567–2572.
[12] P. Brody. (Sep. 6, 2017). How Blockchain is Revolutionizing the Supply Chain Management. Accessed: Jan. 5, 2019. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-blockchain-and-the-supplychain-three/$FILE/ey-blockchain-and-the-supply-chain-three.pdf
[13] N. Neidhardt, C. Köhler, and M. Nüttgens, ‘‘Cloud service billing and service level agreement monitoring based on blockchain,’’ in Proc. 9th Int. Workshop Enterprise Modeling Inf. Syst. Archit., 2018, pp. 1–5.
[14] Carrefour. (2019). Carrefour is Now Using Blockchain Technology, Unlock-BC. Accessed: Feb. 3, 2019. [Online]. Available: https://www. unlock-bc.com/news/2019-01-13/carrefour-is-now-using-blockchaintechnology
[15] P. Bryzek. (2018). How Blockchain is Used by Governments as a Form of National Identity. Accessed: Jan. 10, 2019. [Online]. Available: https://medium.com/@bryzek/how-blockchain-is-used-by-governmentsas-a-form-of-national-identity-e24a4eefb7d8

[16] A. Mizrahi. A Blockchainbased Property Ownership Recording System. Accessed: Jan. 10, 2019. [Online]. Available: https://chromaway.com/papers/A-blockchain-based-property-registry.pdf
[17] B. Algaze. (2018). A blockchain-based approach to smart cities. ExtremeTech. Accessed: Feb. 1, 2019. [Online]. Available: https://www.extremetech.com/extreme/265796-blockchain-approach-smart-cities
[18] C. Parashar. (2018). Blockchain: The future of smart home automation & security. Crypto Canucks. Accessed: Feb. 1, 2019. [Online]. Available: https://cryptocanucks.com/blockchain-the-future-of-smart-homeautomation-security/
[19] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, ''Blockchain for IoT security and privacy: The case study of a smart home,'' in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), Mar. 2017, pp. 618–623.
[20] Nick. (2018). Blockchain cases for healthcare. Industry review. Intellectsoft. Accessed: Feb. 2, 2019. [Online]. Available: https://blockchain. intellectsoft.net/blog/blockchain-cases-for-healthcare-industry-review/
[21] Y. Wehbe, M. A. Zaabi, and D. Svetinovic, ''Blockchain AI framework for healthcare records management: Constrained goal model,'' in Proc. 26th Telecommun. Forum (TELFOR), Nov. 2018, pp. 420–425.
[22] M. Patel, ''Blockchain approach for smart health wallet,'' Int. J. Adv. Res. Comput. Commun. Eng., vol. 6, no. 10, pp. 1–5, Oct. 2017.
[23] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ''A blockchain based privacy-preserving incentive mechanism in crowdsensing applications,'' IEEE Access, vol. 6, pp. 17545–17556, 2018.
[24] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, ''A blockchain based truthful incentive mechanism for distributed P2P applications,'' IEEE Access, vol. 6, pp. 27324–27335, 2018.
[25] N. Andersen. (2016). Blockchain Technology A Game-Changer in Accounting. Accessed: Feb. 2, 2019. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf
[26] D. Vujičić, D. Jagodić, and S. Ranić, ''Blockchain technology, bitcoin, and Ethereum: A brief overview,'' in Proc. 17th Int. Symp. INFOTEHJAHORINA (INFOTEH), Mar. 2018, pp. 1–6.
[27] (2016). Dubai Blockchain Tehcnology. Accessed: Feb. 1, 2019. [Online]. Available: https://www.smartdubai.ae/initiatives/blockchain
[28] T. Wetzel. (2018). Humanitarian Aid: How Blockchain Technology Can Help Refugees and Those in Developing Countries, Medium. Accessed: Jan. 5, 2019. [Online]. Available: https://medium.com/@twwetzel76/ humanitarian-aid-how-blockchain-technology-can-help-refugees-andthose-in-developing-countries-2ebc9477b536
[29] A. Ipakchi and F. Albuyeh, ''Grid of the future,'' IEEE Power Energy Mag., vol. 7, no. 2, pp. 52–62, Mar./Apr. 2009.
[30] H. Farhangi, ''The path of the smart grid,'' IEEE Power Energy Mag., vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.
[31] W. Su and A. Q. Huang, The Energy Internet. Sawston, U.K.: Woodhead Publishing, 2018.
[32] Blockchains in Mobile Networks. Accessed: Mar. 20, 2020. [Online]. Available: https://e.huawei.com/us/publications/global/ict_insights/ 201703141505/core-competency/201703150928

[33] Blockchain Telco. Accessed: Mar. 20, 2020. [Online]. Available: https:// www2.deloitte.com/content/dam/Deloitte/za/Documents/technologymedia-telecommunications/za_TMT_Blockchain_TelCo.pdf
[34] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, ''Survey on blockchain for Internet of Things,'' Comput. Commun., vol. 136, pp. 10–29, Feb. 2019.
[35] X. Zhang and X. Chen, ''Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network,'' IEEE Access, vol. 7, pp. 58241–58254, 2019.
[36] T. Jiang, H. Fang, and H. Wang, ''Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis,'' IEEE Internet Things J., vol. 6, no. 3, pp. 4640–4649, Jun. 2019.
[37] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, ''When mobile blockchain meets edge computing,'' IEEE Commun. Mag., vol. 56, no. 8, pp. 33–39, Aug. 2018.
[38] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, ''Cloud/fog computing resource management and pricing for blockchain networks,'' IEEE Internet Things J., vol. 6, no. 3, pp. 4585–4600, Jun. 2019.
[39] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, ''Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm,'' IEEE Access, vol. 7, pp. 9714–9723, 2019.
[40] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, ''Blockchain for 5G: Opportunities and challenges,'' in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2019, pp. 1–6.
[41] M. A. R. Chaudhry and Z. A. Soptimizer, ''Blockchain: A key enabler for 5G,'' IEEE Standards Univ., vol. 10, no. 1, 2019. [Online]. Available: https://www.standardsuniversity.org/e-magazine/may-2019-volume-9- issue-1-blockchain-standards/blockchain-a-key-enabler-for-5g/