ARTCI

AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

BULLETTIN

Juillet 2017

de *Veille Technologique*

Spécial blockchain

Editorial

En 1996, John Perry Barlow - *membre fondateur de EFF (Electronic Frontier Foundation), une ONGI de protection des libertés sur Internet* – affirmait dans sa célèbre Déclaration d'Indépendance du Cyberespace : « *Nous sommes en train de créer un monde où tous peuvent entrer sans privilège et sans être victimes de préjugés découlant de la race, du pouvoir économique, de la force militaire ou de la naissance* ». Ce qui laisse présager l'espoir d'un Internet ouvert, démocratique et juste.

Et pourtant, on assiste environ deux décennies plus tard à une concentration du pouvoir et de la richesse avec l'hégémonie des géants du web dont les plateformes centralisent l'essentiel des activités sur Internet, et à l'ingérence des gouvernements dans le principe de fonctionnement de cet outil qui se voulait indépendant et libre.

Alors, faut-il ou pas gouverner Internet ? A tort ou à raison, chacun y va de son argumentaire sur ce que devrait être le modèle de gouvernance de l'Internet.

Mais selon toute vraisemblance, Internet n'a pas tenu ses promesses de résoudre ses propres problèmes qui appelleraient à une intervention extérieure. Dans le sillage de son développement ont émergé de nombreux défis, notamment sécuritaire, de souveraineté, de protection des droits et de la vie privée ou tout simplement de confiance. Comment faire confiance à l'autre dans cet univers de totales inconnues ? Parler de confiance dans un tel contexte semble a priori utopique, sauf que du caractère distribué et cosmopolite de l'Internet émerge des innovations à même d'apporter de grands bouleversements.

En 2008, sous le pseudonyme Satoshi Nakamoto est publié un *Livre Blanc* pour décrire le principe de fonctionnement d'une monnaie électronique complètement décentralisée : le Bitcoin. C'est une monnaie qui se caractérise par son opposition radicale aux systèmes de paiement conventionnels qui reposent sur un tiers de confiance. Elle s'appuie pour cela sur la technologie Blockchain qui est un registre distribué et sécurisé des transactions entre utilisateurs qui se font mutuellement confiance grâce à la robustesse ou à l'immuabilité du système.

En s'affranchissant des systèmes traditionnels dont la notion de confiance reposait sur une entité centralisée, la Blockchain ouvre la voie à de multiples applications dans le domaine bancaire, de l'assurance, de l'immobilier, des transports, de la santé, de l'éducation, des services publics, etc. De par le monde, les attentes sont manifestes vis-à-vis de cette technologie qui, j'ose le croire, permettra d'enrayer les inégalités, en favorisant l'accès des populations les plus démunies aux services financiers.

La révolution technologique induite entre autres par la Blockchain nécessite de s'appuyer sur des architectures à caractère ubiquitaire et robustes, à même de supporter l'identification et le traitement des informations sur une longue période de temps. C'est le cas de l'architecture d'objet numérique (DOA), une architecture générale pour un système distribué de stockage, de localisation et de récupération de l'information via Internet.

Je vous invite donc à découvrir ces différentes révolutions technologiques et à contribuer à enrichir les échanges autour de ces technologies afin que leur potentiel puisse pleinement se développer au profit de l'économie numérique.

BILE Diéméléou

Directeur Général de l'ARTCI

Bulletin
de veille technologique -
Juillet 2017
ARTCI, Côte d'Ivoire

Directeur de Publication:

M. BILE Diéméléou

Rédacteur en Chef:

M. KOUAKOU Guy-Michel

Equipe de rédaction:

M. ZEBOUA Patrick

M. YAO N'Guessan Kevin

Mlle LASME Mel Paule Renée

Contacts

Marcory Anoumanbo, 18 BP 2203 Abidjan 18.

Tél : + 225 20 34 58 80

Fax : + 225 20 34 43 75

...Au lecteur

Parce que votre avis compte, nous serions heureux de recevoir vos suggestions et remarques, afin d'améliorer nos prochaines publications, à :

veilletechno@artci.ci

Sommaire

Blockchain

INTRODUCTION

La première blockchain est apparue en 2008 avec la monnaie électronique Bitcoin, devenue aujourd'hui l'une de ses nombreuses applications. Bitcoin est une monnaie électronique utilisée pour les transactions financières sur Internet à l'instar de PayPal mais diffère radicalement des systèmes de paiement conventionnels, car elle ne repose pas sur un Tiers de confiance TTP (*en anglais Trusted Third Party ou TTP*) pour la validation de ses transactions. Elle repose plutôt sur la technologie blockchain (ou chaîne de blocks en français) qui permet la gestion et la maintenance d'un registre de transactions distribué et sécurisé.

En effet, la Blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe de contrôle[1]. Par extension, elle représente un système de base de données qui permet d'établir un historique horodaté de tous les échanges entre les utilisateurs de cette blockchain depuis sa création. Elle peut être soit publique, donc ouverte à tous à l'instar de Bitcoin, soit privée avec un accès et un usage limités à un certain nombre d'acteurs.

Quand elle est publique, une blockchain peut être assimilée à un grand livre de compte public accessible à tout le monde mais infalsifiable grâce à des mécanismes cryptographiques.

C'est donc une technologie sécurisée complètement distribuée qui facilite la création de la confiance entre les différentes parties grâce à des mécanismes cryptographiques et à un système basé sur le consensus. Elle constitue de ce fait une révolution vis-à-vis des systèmes traditionnels dont la notion de confiance reposait sur une entité centralisée.

La blockchain rompt ainsi avec les logiques pyramidales à l'œuvre dans nos sociétés et est vue comme la technologie qui permettrait de bouleverser ce paradigme, en favorisant notamment des logiques de coopération au sein d'organisations collaboratives décentralisées.[2]

Bitcoin demeure à ce jour l'exemple le plus connu d'application blockchain. Mais en dehors des services financiers, la blockchain est une technologie qui ouvre de nouvelles perspectives capables de bouleverser plusieurs domaines tels que la santé, l'assurance, l'immobilier, les transports, l'éducation ou les services publics, etc.

BLOCKCHAIN : COMMENT ÇA MARCHE ?

Considérons une transaction entre deux parties. Dans les systèmes conventionnels, un tiers de confiance est requis pour valider la transaction. Une banque par exemple maintient un registre de toutes les transactions tels que les dépôts, les retraits, les virements, etc. Elle est donc en mesure de certifier la validité de la transaction.

Le but de la blockchain est de s'affranchir de ce registre central. Ainsi, plutôt que d'être maintenu par une seule partie, le registre des transactions est entièrement distribué, ouvert et accessible à toutes les parties. Par conséquent, le processus de validation et de sécurisation des transactions est assuré par les nœuds du réseau blockchain appelés « mineurs », qui s'appuient sur la copie identique du registre qu'ils possèdent et la transaction en cours.

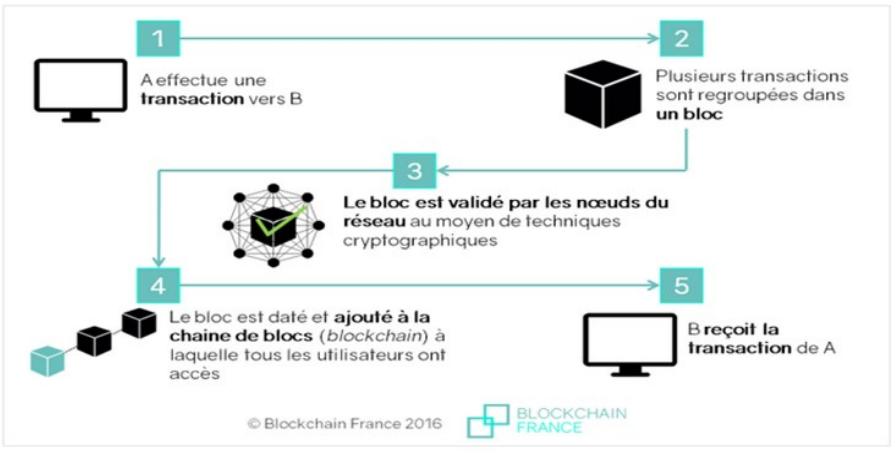

Figure 1 - Schéma de validation d'une transaction

Ainsi, comme le montre la figure 1, plusieurs transactions sont regroupées dans un bloc. Puis, une fois validé, le nouveau bloc est horodaté et ajouté à la chaîne de blocs et les transactions qu'il contient sont visibles sur l'ensemble du réseau.

Figure 2 - Une blockchain

La blockchain peut donc être vue comme une infrastructure de réseau peer-to-peer sécurisée qui permet une gestion distribuée des transactions entre les nœuds du réseau.

C'est un processus automatique, vérifiable et basé sur un consensus. Ce qui lui confère une grande robustesse donc digne de confiance. En effet, « *un adversaire ne pourra jamais injecter de transactions malveillantes sur le système distribué, étant donné que les autres parties détecteront la fraude et ne donneront pas de consensus* ».[3]

LE CONSENSUS AU CŒUR DU PRINCIPE DE FONCTIONNEMENT DE LA BLOCKCHAIN

Par définition, un consensus est un accord entre plusieurs parties.

Dans un système distribué, la notion de consensus devient complexe et difficile à déterminer dans la mesure où tout le monde - *certains de bonne moralité, d'autres non* - peut réaliser une transaction ou la valider. Dans un tel contexte, comment s'assurer qu'une

transaction n'est pas frauduleuse ?

Cette problématique n'est pas nouvelle et connue sous la terminologie du « *Paradoxe des généraux byzantins* ». Comme le décrit siecledigital.fr, imaginez à l'époque byzantine plusieurs armées prêtes à attaquer en commun une même ville, le seul moyen de communiquer des informations et de synchroniser les différentes armées, pour déterminer s'il faut attaquer ou battre en retraite, est de faire circuler un messager à cheval. Chaque général mandate un chevalier, inconnu de l'autre armée, pour porter le message « attaque » ou « retraite ». Chacune des armées n'ayant aucune connaissance de ce chevalier va rencontrer un problème, comment lui faire confiance ? Comment être sûr que le message qu'il apporte est le bon ?[4]

Avec la blockchain, le problème à résoudre est l'association d'éléments distincts, travaillant tous de concert pour éviter une défaillance du système. Elle s'appuie pour cela sur plusieurs méthodes qui sont des formes de mise en œuvre de la solution du « *Paradoxe des généraux byzantins* ».

LA PREUVE DU TRAVAIL

La méthode historique de consensus est la preuve de travail (*en anglais proof-of-work ou PoW*). Elle utilise l'énergie comme moyen de vérification que le « mineur » a bien réalisé un travail et celui-ci est rémunéré en conséquence. Le minage - *proposer un nouveau bloc* - est de ce fait une activité lucrative qui pousse les industriels comme les particuliers à investir de gros moyens afin de disposer de la puissance de calcul nécessaire. Le temps et l'énergie mis à la disposition par chaque mineur constituent un gage de bon fonctionnement du réseau, pourvu que « *aucun opérateur hostile ne détienne, à aucun moment, plus de la moitié de la puissance de calcul de la chaîne* »[5].

Le travail consiste à trouver par une fonction de hashage l'identifiant d'un nouveau bloc. Par définition, une fonction de hashage est une fonction à sens unique (pratiquement impossible à inverser) qui prend en entrée une chaine de caractères de longueur quelconque et qui donne en sortie une chaine de caractères de longueur fixe. On passe donc en entrée de la fonction de hashage un fichier contenant toutes les transactions à valider ainsi que l'identifiant du bloc précédent. Les blocs sont ainsi liés les uns aux autres et toute tentative de modification d'une transaction nécessiterait la modification de toute la blockchain. Le niveau de difficulté est défini en avance et détermine le temps nécessaire pour réaliser l'opération. Avec Bitcoin, les conditions sont faites pour qu'une solution soit trouvée environ toutes les 10 minutes et pour espérer résoudre ce problème, il faut répéter l'opération des centaines de milliards de fois. Au fur et à mesure que le réseau grandi et que la puissance de calcul augmente, on ajuste le niveau de difficulté pour conserver cette moyenne de 10 minutes.

Cette méthode fait de la blockchain une technologie infalsifiable tant que plus de 50 % de la puissance de calcul mise à disposition sur le réseau par l'ensemble des nœuds n'est pas sous contrôle d'un tiers malveillant. A titre de comparaison, on estime que même si Google engageait tous ses serveurs dans le minage de Bitcoins, sa puissance de calcul ne représenterait que 1% de la puissance de calcul du réseau. Il semble donc improbable pour une seule entité de détenir plus de 50% de la puissance de calcul.

Les seules faiblesses associées à cette méthode sont le gain décroissant des mineurs et le temps de latence nécessaire pour valider une transaction. En effet, selon bitcoin.fr le minage n'est plus du tout une activité rentable pour les particuliers à cause de

la concurrence énorme due à l'agrandissement du réseau. Seuls certains sites industriels parviennent encore à tirer profit de cette activité. Par ailleurs, c'est une technologie très énergivore. Une étude de 2014 estimait que la consommation du réseau destiné au bitcoin était probablement de l'ordre de grandeur de la consommation électrique d'un pays comme l'Irlande, soit environ 3 GW. Une généralisation du bitcoin devrait donc élever la consommation énergétique correspondante à 4000 GW, soit 8 fois la consommation électrique de la France, et deux fois celle des États-Unis.[6]

Ces constats poussent la communauté blockchain à adopter d'autres méthodes de consensus.

LA PREUVE DE PARTICIPATION

La preuve de participation (*en anglais proof-of-stake ou PoS*) se présente comme une alternative à la preuve du travail trop gourmande en puissance de calcul et en énergie. C'est une méthode qui repose sur la preuve de la possession d'une certaine quantité de crypto-monnaie pour prétendre à pouvoir valider des blocs supplémentaires dans la chaîne.

EXEMPLES D'APPLICATIONS BLOCKCHAIN

LES BLOCKCHAIN PUBLIQUES

Dans une blockchain publique, tous les nœuds du réseau d'échange sont régis par le réseau peer-to-peer et accessible à tous : chaque entité a un libre accès au registre. De plus, chacun peut entamer des enregistrements tout en espérant qu'ils soient pris en compte et participer au processus de validation. Bitcoin et Ethereum constituent les deux principales blockchains publiques. D'autres existent également, de moindre ampleur : Litecoin, Dogecoin, etc.

- Bitcoin

En 1998, Wei Dai, membre de Cypherpunk, une mouvance d'activistes sur le web, décrit des procédures de création et de gestion d'une monnaie électronique, dont l'utilisation est non traçable et le fonctionnement autonome. Il publie le « B-money Proposal », article qui renferme les fondements des monnaies électroniques actuelles.

Dix ans plus tard, Satoshi Nakamoto publie en 2008 un Livre Blanc (*White Paper en anglais*) décrivant le principe de fonctionnement du Bitcoin. Il faut préciser que Satoshi Nakamoto est un pseudonyme. Les nombreuses tentatives d'identification de qui se cache derrière ce pseudonyme sont jusque-là restées vaines. Le mystère demeure donc entier tandis que la valeur du Bitcoin ne cesse de grimper jusqu'à dépasser celle de l'or.

Figure 3 - Evolution du cours du Bitcoin depuis sa création

Début juillet 2017, un Bitcoin s'échange contre plus de 2500 USD pour environ 16 500 000 Bitcoins en circulation[7]. Au total, c'est l'équivalent de près de 41 milliards de dollars qui circulent à l'heure actuelle en Bitcoins sur les marchés.

A noter qu'à côté de Bitcoin, d'autres monnaies virtuelles comme Ethereum ou Ripple sont en plein essor.

- Ethereum

Créé en 2013 par Vitalik Buterin à seulement 19 ans, Ethereum est une blockchain qui s'appuie sur les smart contracts (ou contrats intelligents en Français). Les smart contracts sont des programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.[8] Ethereum est donc une blockchain sur laquelle les utilisateurs peuvent construire et financer des projets dans tous types de domaines, de la banque à l'assurance, en passant par la santé ou l'énergie.

Figure 3 - Evolution du cours de l'Ether

De cette plateforme découle une unité monétaire, l'Ether, plus rapide que le Bitcoin et économique. En effet, l'Ether permet des paiements en quelques secondes alors que les modalités de minage du Bitcoin ne permettent des transactions qu'à la minute. Par ailleurs, l'Ether s'est positionné sur toutes les transactions, mêmes celles de quelques dollars, ce que Bitcoin, dont chaque transaction coûte en moyenne deux dollars, n'a pas tenté de capter.

Au vu de ses potentialités et de ses nombreuses applications, l'Ether a su séduire les entreprises et se positionne comme un potentiel concurrent du Bitcoin. Sa valeur actuelle est d'environ 400 dollars[9] pour une valorisation globale d'environ 36 milliards de dollars.[10]

Les blockchain privées

La notion de blockchain privée renvoi tout simplement à un réseau privé et fermé contrairement à une blockchain publique ouverte à tous. On ne peut donc participer à une blockchain privée sans y être invité.

On parlera de consortium ou de blockchain hybride lorsqu'il y a un regroupement de plusieurs acteurs. Le consortium est plus adapté aux acteurs qui opèrent dans des contextes régulés. C'est la raison pour laquelle les banques, les assureurs, etc. font le choix de ce type de blockchain, pour le moment pour des besoins d'expérimentation afin de mieux appréhender les contours de la technologie.

A titre d'exemple, le consortium R3[11] regroupe 80 institutions financières et a pour vision de tirer profit de la technologie blockchain. En mai, R3 a levé 107 millions de dollars et espère lever en tout 150 millions de dollars d'ici la fin de l'année.[12]

POTENTIELS DE LA BLOCKCHAIN

UNE ÉCONOMIE POTENTIELLE POUR LES BANQUES

Bien que des pronostics, avancés de la blockchain sont parfois en défaveur des banques, elle ouvre un champ de métiers pour l'ensemble des activités bancaires. « *L'infrastructure bancaire de demain va se reposer, sans conteste, sur des blockchain qui vont réduire les coûts, améliorer la réactivité des systèmes d'information et optimiser la sécurité des échanges* », augure Frédéric Dalibard, Responsable du digital de la Banque de Grande Clientèle chez Natixis.

Selon silicon.fr[13], faisant lui-même référence au rapport d'une étude de Accenture[14], la technologie blockchain a le potentiel de réduire les coûts d'infrastructure en moyenne de 30% pour huit des dix plus grandes banques d'investissement du monde. Soit des économies annuelles de 7,5 à 11,3 milliards d'euros par an d'ici à 2025.

Ce gain s'explique par le coût énorme de la réconciliation de données que la blockchain permettrait de supplanter. En effet, les Banques aujourd'hui conservent des bases de données indépendantes de transactions et d'informations sur les clients rendant ainsi les processus de réconciliation et de confirmation de données complexes.

Pour silicon.fr, la technologie peut également déboucher sur des économies dans plusieurs autres domaines clés comme le reporting financier dont les coûts pourraient être réduits de 70 % en raison de l'amélioration de la qualité des données. Des économies de 50% peuvent également être faites sur les coûts de conformité en raison de la transparence améliorée des transactions.

SERVICES D'ASSURANCE POUR TOUS

Tout comme le secteur bancaire, le secteur de l'assurance s'intéresse de près à la blockchain. Des entreprises comme Lloyds ou Allianz France ont exprimé leur volonté de lancer des expérimentations sur la blockchain, et début 2016, Axa a investi 55 millions de dollars[15] dans la startup Blockstream, qui doit permettre, entre autres, une interopérabilité entre différentes blockchain.

L'enjeu pour les entreprises d'assurance est de construire de nouveaux systèmes d'assurance via Internet sans intermédiaire. Ce qui constitue une aubaine pour les populations à faible revenu qui n'ont pas accès aux services d'assurance traditionnels beaucoup trop chers, en partie à cause des coûts administratifs élevés. Par exemple[16], pour chaque dollar de prime d'assurance récolté, les coûts administratifs s'élèvent à 0,28 $ au Brésil, 0,54 $ au Costa Rica, 0,47 $ au Mexique et 1,80 $ aux Philippines. Comme conséquence, les personnes vivant avec moins d'un dollar par jour n'ont pas la capacité de payer une assurance.

Consuelo[17] est un service de micro-assurance mexicaine basé sur la technologie blockchain. Il permet aux clients de souscrire à une assurance et de payer de petits montants. Pour s'affranchir des systèmes traditionnels, la blockchain donne un nouvel élan grâce à des systèmes d'assurance automatisés à base de smart contracts.

Les smart contracts, en automatisant l'exécution des contrats, permettent aux assurés comme aux assureurs de s'émanciper des phases déclaratives : formulaires, réclamation, vérification, déclenchement de l'indemnisation… la blockchain faisant office de tiers de confiance automatisé.

La blockchain et les smart contracts ouvrent donc la voie à de nombreuses applications innovantes qui permettront de créer une assurance recentrée sur ses utilisateurs. En effet, outre l'autonomisation des

processus permise par les smart contracts, une nouvelle tendance d'assurance dite peer-to-peer (P2P) émerge. Ce nouveau modèle permettra de créer des systèmes d'assurance quasi-autonomes et autorégulés, où polices d'assurance et réclamations des assurés seraient automatiquement gérées grâce à des organisations décentralisées autonomes (DAO) - *entités autonomes dans la blockchain, sans statut juridique formel. Leurs règles de fonctionnement sont inscrites dans du code informatique*.[18]

CONNECTER LES PLUS PAUVRES À L'ÉCONOMIE MONDIALE

L'accès au service financier dans des conditions équitables demeure problématique dans les pays en développement avec un fort taux de pauvreté. Dans certaine région de l'Afrique par exemple, l'ouverture d'un compte chèque nécessite un dépôt minimum qui parfois dépasse ce qu'une personne gagne en moyenne sur une année.[19]

En 2016, 442 milliards de dollars[20] ont été transférés par les expatriés à leur famille. Ce qui contribue fortement à l'amélioration des conditions de vie dans les pays en développement. Malheureusement, faire un mandat international coûte extrêmement cher.

Par exemple, pour un transfert de 50$ des États-Unis vers le Ghana, il faut payer 10 $ de frais. En 2015, les coûts de transaction et les taux de commissions ont été en moyenne de 10,96% pour les envois de fonds via les banques et de 6,36% via les opérateurs de transfert d'argent.[16] Si ces coûts se justifient en partie, ils n'en demeurent pas moins élevés.

Selon la Fondation Bill & Melinda Gates[21], « *le système financier moderne ne fonctionne pas pour les pauvres… Mais il existe une autre option - un écosystème financier numérique. Les transactions numériques sont efficaces et peuvent être très peu coûteuses…*» A travers son initiative Level One Project[22], la Fondation Bill & Melinda Gates entend utiliser les technologies blockchain pour aider les deux milliards de personnes dans le monde qui n'ont pas un compte bancaire.

Les blockchain peuvent contribuer à l'inclusion financière des plus démunis en contournant les réseaux bancaires existants et les systèmes traditionnels de paiement et de transfert de fonds. Même si le Mobile Money a beaucoup contribué à l'inclusion financière en Afrique, le service demeure fermé. Une plateforme de paiement interopérable à laquelle tout le monde peut avoir accès, même ceux vivant avec quelques dollars par jour, est possible grâce à la blockchain.

Basé à Hong Kong, Bitspark propose pour des transactions en bitcoin inférieures à 150 $ vers les pays comme le Vietnam, les Philippines, l'Indonésie, etc. des coûts d'environ 2$ et 1% pour des montants plus importants.[23]

Les technologies blockchain peuvent aussi contribuer à rendre efficaces les aides humanitaires. Les organisations humanitaires doivent faire face à la fraude, la corruption, la discrimination et la mauvaise gestion qui rendent inefficaces les actions visant à réduire la pauvreté et à améliorer les conditions de vie des populations. C'est dans cette optique que le Programme Alimentaire Mondial (PAM) a lancé en début d'année 2017 le projet blockchain appelé « Building Block »[24] en vue de fournir, dans sa première phase, de l'aide alimentaire aux familles nécessiteuses de la province de Sindh au Pakistan.

Pour le PAM, « *la technologie Blockchain… offre des opportunités uniques aux humanitaires afin d'améliorer [leur] capacité à fournir une assistance*

efficace aux personnes… et à économiser des millions de dollars. »[24]

Le PAM espère ainsi réduire ses frais généraux de 3,5% à moins de 1%.[25] Par ailleurs, la blockchain peut faciliter, en cas de catastrophes, les interventions dans les zones difficiles d'accès où les infrastructures financières n'existent pas en permettant aux organisations d'aide humanitaire, commerçants et bénéficiaires d'échanger de l'argent par voie électronique et sécurisée. La blockchain offre aussi la possibilité à des particuliers de contribuer à l'aide humanitaire. En Afrique du Sud, la plateforme blockchain Usizo permet à quiconque d'aider à payer des factures d'électricité pour les écoles communautaires. Les donateurs peuvent suivre la quantité d'électricité utilisée par une école, calculer la quantité d'énergie que leur don achètera et transférer le crédit directement en utilisant bitcoin.[26]

Au demeurant, selon le PAM, la technologie blockchain ouvre la porte à un avenir où la communauté humanitaire se réunit autour d'une infrastructure neutre et interopérable pour harmoniser et optimiser l'effort mondial d'aide aux personnes en situation de détresse.

INTERNET DES OBJETS

Le contenu de cette section a été publié pour la première fois à l'adresse suivante : https://theinternetofallthings.com/blockchain-technology-what-does-it-have-to-do-with-iot-142017/

La blockchain ne se limite pas seulement aux transactions financières. Par exemple, les 100 000 000 d'unités du Bitcoin sont programmables et peuvent être liées à des propriétés numériques autres que des devises telles que des crédits ou des votes numériques. Cela donne lieu à l'utilisation de la blockchain pour supporter les applications IoT. Au lieu d'auditer l'échange d'unités d'une monnaie numérique, la blockchain pourrait vérifier la validité des transactions numériques entre les machines et les choses.

L'Internet des objets est propulsé par la prolifération d'appareils connectés à Internet, qui communiquent de plus en plus fréquemment. Les wagons connectés qui échangent de l'information sur le trafic, les réfrigérateurs qui commandent des articles pour le réapprovisionnement et les capteurs de plantation communiquant avec des robots dans des chaînes de montage sont quelques exemples de ces communications. Ces dernières interactions doivent être sécurisées et fiables. Dans ce contexte, la blockchain offre un mécanisme robuste, digne de confiance, sécurisé et hautement évolutif pour assurer la confiance numérique dans toutes ces transactions.

L'intégration de la blockchain dans l'Internet des objets en est encore à ses balbutiements. Cependant, il existe déjà des produits et services précoces, notamment :

- Modum (https://modum.io), qui utilise la technologie blockchain pour la sécurité des médicaments. Il exploite le registre afin de s'assurer que les médicaments restent dans des conditions appropriées tout au long de leur cycle de vie (c'est-à-dire de la production en usine à l'utilisation par le patient).
- Tilepay (http://www.tilepay.org), qui utilise la blockchain afin de permettre le commerce des données produites par les périphériques IoT sur un marché en ligne sécurisé. Il ouvre de nouveaux horizons dans la gestion et l'exploitation des données personnelles par leurs producteurs (c'est-à-dire les utilisateurs finaux).
- Blockhainofthings (http://blockchainofthings.com/), qui a créé une infrastructure blockchain afin de faciliter la mise en œuvre des applications IoT sécurisées.

De plus, il existe des projets open source qui permettent aux entreprises de développer leurs propres infrastructures blockchain de gestion des ressources et d'échanger des données en toute sécurité. Les exemples incluent les projets Openchain (https://www.openchain.org/) et Hyperledger (https://www.hyperledger.org/).

GESTION DE L'ÉNERGIE

Les TIC sont de plus en plus utilisées pour répondre à la demande toujours croissante d'une utilisation intelligente et plus efficace de l'énergie. L'énergie est donc l'un des domaines dans lequel la blockchain pourrait avoir un impact majeur.

Alors que la consommation en énergie croit, plusieurs approches sont proposées afin de faire face à la demande. Par exemple, les particuliers peuvent produire leur électricité et vendre sur le réseau électrique leur surplus d'énergie. Chose qui

serait facilitée avec un système décentralisé comme la blockchain.

Cependant, le réseau électrique reste l'un des plus sensibles et donner la possibilité à quiconque de s'y connecter constitue un gros problème de cybersécurité.

Développement de services publics innovants

Environ 1,5 milliard de personnes – 20% *de la population mondiale* - n'ont pas de documents permettant de vérifier leur identité.[27] Cela limite leur capacité à utiliser les banques, mais peut également les empêcher d'accéder à leurs droits fondamentaux, comme voter, avoir accès aux soins de santé, aller à l'école et voyager.

Pour pallier cela, des projets comme le digital ID network[28] - *projet développé par Microsoft et Accenture en partenariat avec le HCR pour aider les réfugiés à prouver leur identité dans le but d'avoir accès à des services de base comme l'éducation ou la santé* - voient le jour afin de faciliter la création et la vérification de l'identité des individus. A l'aide d'un simple smartphone, une personne peut capter ses données biométriques. Puis une fois enregistrées sur la blockchain, ses données peuvent être consultées ultérieurement par toute personne qui doit vérifier l'identité de cette personne.

Sans courrier électronique, téléphones, passeports ou même des certificats de naissance, une blockchain pourrait être la seule façon pour beaucoup de personnes de prouver leur identité. Cela pourrait vraiment améliorer leur vie et élargir leurs opportunités.

Autres champs d'application de la blockchain

Il serait prétentieux de chercher à aborder toutes les possibilités offertes par la blockchain tellement les champs d'applications sont immenses. Outre les exemples susmentionnés, on peut citer la santé où la blockchain pourrait servir à la traçabilité des médicaments, à la sécurisation des données de santé, et à la gestion des données des patients, les transports, le vote en ligne, l'immobilier, les cadastres, etc.

La blockchain va aussi créer un système de cloud distribué où les Data Center seront remplacés par les disques durs des particuliers sur lesquels des bouts de nos données seront stockés de façon sécurisée. Certains même parlent de l'ubérisation des applications de type Uber…

De façon générale, des blockchain pourraient remplacer la plupart des « tiers de confiance » centralisés par des systèmes informatiques distribués.

Autres champs d'application de la blockchain

Le potentiel de la blockchain est énorme mais c'est une technologie qui soulève beaucoup de questions qu'elles soient économiques, juridiques, de gouvernance, ou encore écologiques.

Pour nous donner une idée des défis à relever avant que la blockchain puisse être utilisée, notamment dans le domaine des services financiers, Javier Sebastian, manager de la régulation digitale chez BBVA (Banco Bilbao Vizcaya Argentaria) a publié un rapport intitulé « *Blockchain in financial services : Regulatory landscape and future challenges for its commercial application* ».[29] Dans ce rapport, l'expert de la BBVA identifie sept nouveaux enjeux règlementaires face à cette nouvelle technologie.

- ***La définition d'un cadre juridique pour la technologie blockchain et les registres distribués***

Les registres distribués n'ont, par définition, aucune localisation précise donc cela peut soulever des problèmes concernant la juridiction et la loi applicable en cas de litige. La territorialité constitue donc un problème puisque chaque nœud de réseau peut être soumis à des exigences juridiques différentes. La responsabilité constitue donc une préoccupation, puisqu'aucune partie n'est responsable en dernier ressort du fonctionnement des registres distribués et des informations qui y sont contenues.

- ***Un cadre juridique pour la reconnaissance des blockchain comme des nœuds inviolables et immuables***

Il y a le besoin d'une définition d'un cadre juridique pour utiliser la technologie blockchain comme une source d'identité fiable et unique, surtout pour l'identité numérique. Avant cela, une réglementation est nécessaire en matière de protection des données et d'authentification de l'identité des personnes morales. Bien qu'il existe un large consensus parmi la communauté cryptographique et informatique en ce qui concerne l'immuabilité d'une blockchain, ce consensus n'a pas encore été reconnu légalement et par conséquent, ne peut être utilisé comme argument juridique devant des tribunaux.

- ***Le droit à l'oubli***

Le « droit à l'oubli » permet à tout citoyen de disposer des données stockées dans une base de données extérieure, qu'il peut supprimer suivant sa volonté. L'immuabilité d'une blockchain peut alors poser problème puisqu'elle serait en conflit avec des droits reconnus par les gouvernements. Il pourrait être nécessaire de remplacer le droit de supprimer des informations par un droit d'interdire l'utilisation des renseignements personnels par des tiers. Une combinaison de cryptage automatique des données dans certaines conditions ou de solutions alternatives pour désactiver l'accès à l'information à volonté pourrait atteindre cet objectif.

- ***Un cadre juridique relatif à la validité juridique des documents stockés dans une blockchain comme preuve de possession ou d'existence***

Un deuxième niveau de reconnaissance est nécessaire avant que les blockchain puissent être utilisées dans certaines entreprises. Il ne s'agit pas seulement de reconnaître que l'information ne peut être modifiée, mais aussi de reconnaître que l'inclusion dans une blockchain d'un acte déclarant la propriété ou l'existence d'un bien constitue une véritable preuve de propriété ou l'existence réelle dudit bien.

- ***Un cadre juridique de validité des instruments financiers émis par une blockchain***

Utilisée comme plateforme pour la définition d'instruments financiers « natifs » comme les dérivés ou les obligations, il faut reconnaître la validité juridique de ces instruments par les autorités de contrôle et les autorités de réglementation. L'argent est un instrument financier clé quant à la conduite de politiques monétaires et qui peut être désormais émis grâce à la technologie blockchain. Ces monnaies digitales peuvent présenter de sérieux problèmes macroéconomiques et concernant la politique monétaire ce qui justifie une analyse plus large.

- ***Un cadre juridique pour les smart contracts***

En général, et en particulier pour le commerce international y compris la territorialité et la

responsabilité. Les questions mentionnées au premier point concernant la territorialité et la responsabilité sont également applicables aux contrats intelligents mais exigent des considérations supplémentaires.

- ***La réglementation sur l'utilisation de blockchain comme un registre règlementaire valide pour l'IoT***

La blockchain pourrait être vraiment utile pour l'Internet des Objets. En effet, dans l'IoT, tous les appareils connectés ont une identité. Il serait donc vraiment utile d'établir un registre distribué partageant l'identité et les détails de chaque objet connecté tout en leur permettant de mener des transactions entre eux, y compris des paiements M2M (machine-to-machine). L'idée d'avoir un ou plusieurs «registres distribués partagés» pour l'Internet des Objets semble gagner en popularité et nécessiterait un cadre juridique reconnaissant les registres distribués comme des registres réglementaires valides. Tous les défis ci-dessus concernant la territorialité, la responsabilité et l'applicabilité des contrats intelligents sont évidemment aussi pertinents pour toute blockchain associée au fonctionnement de l'Internet des Objets.

CONCLUSION

Le potentiel de la blockchain va se démultiplier au regard de ses apports dans les secteurs tels que la finance, la distribution, la santé, l'énergie, etc.

L'attrait de la blockchain repose sur sa capacité à faire coopérer des acteurs autour d'activités communes nécessitant l'échange d'informations, sans la garantie que tous les membres du réseau soient honnêtes ou dignes de confiance ; ceci grâce à des mécanismes cryptographiques.

Il est difficile de dire avec exactitude l'impact à long terme de la blockchain. Cependant, il est indéniable que la technologie blockchain ouvre des perspectives innovantes et pourrait engendrer de profonds bouleversements. Cette technologie pourrait démocratiser notre société en facilitant par exemple le processus de vote en ligne par la sécurité et la transparence qu'elle apporte.

Les domaines d'application de la blockchain sont innombrables. Elle suscite donc assez de convoitise mais en même temps beaucoup d'interrogations d'ordre économiques, juridiques, de gouvernance, ou encore écologiques.

In fine, selon la *Tribune* d'*Alexandre Stachtchenko* et *Claire Balva* publiée dans *Challenges*[30] pour le *Positive Economy Forum*, la blockchain « … *permettrait d'enrayer les inégalités, en permettant à la moitié de la population mondiale, non bancarisée, d'accéder à des services financiers. Elle permettrait la transition énergétique, en favorisant l'échange d'énergie local sur des réseaux micro-grids, préparant l'avènement des producteurs-consommateurs. Elle permettrait la révolution de l'Internet des Objets, en fournissant aux objets un moyen de communication machine à machine sans intermédiaire ni capture des données. Dans un monde où le citoyen cherche à connaître l'histoire des produits et services qu'il achète, elle permettrait enfin de garantir l'origine et l'authenticité des produits de manière irréfutable.* »

Il est donc du reste indispensable que tous les acteurs travaillent de concert et en toute intelligence afin de mener les réflexions nécessaires pour que le potentiel de la blockchain puisse pleinement se réaliser au profit de toute la société.

Notes et références

1. https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/
2. http://www.latribune.fr/opinions/tribunes/la-blockchain-une-revolution-qui-va-changer-le-monde-547576.html
3. https://theinternetofallthings.com/blockchain-technology-what-does-it-have-to-do-with-iot-142017/
4. https://siecledigital.fr/2016/11/07/utilite-consensus-blockchain/
5. http://www.revue-banque.fr/risques-reglementations/chronique/blockchain-question-preuve-par-consensus-au-coeur
6. http://theconversation.com/le-bitcoin-et-la-blockchain-des-gouffres-energetiques-62335
7. https://blockchain.info/fr/charts
8. https://blockchainfrance.net/2016/01/28/applications-smart-contracts/
9. https://coinmarketcap.com/currencies/ethereum/#charts
10. https://www.lesechos.fr/finance-marches/marches-financiers/030379798997-ether-la-principale-menace-du-bitcoin-2095198.php
11. http://r3members.com/
12. http://www.agefi.fr/fintech/actualites/quotidien/20170523/consortium-blockchain-r3-leve-107-millions-dollars-219148
13. http://www.silicon.fr/blockchain-economie-potentielle-10-mde-an-banques-167550.html?inf_by=5755456d2ad0a1777d82a51e
14. https://www.accenture.com/us-en/insight-banking-on-blockchain
15. https://www.axa.com/fr/newsroom/actualites/axa-strategic-ventures-blockchain
16. http://theconversation.com/can-blockchain-technology-help-poor-people-around-the-world-76059
17. https://cointelegraph.com/news/consuelo-offers-blockchain-powered-microinsurance-to-migrant-workers
18. https://blockchainfrance.net/2016/02/17/assurances-et-blockchain/
19. http://siteresources.worldbank.org/DEC/Resources/Banking_Services_for_Everyone.pdf
20. http://www.worldbank.org/en/news/press-release/2016/10/06/remittances-to-developing-countries-expected-to-grow-at-weak-pace-in-2016-and-beyond
21. http://www.impatientoptimists.org/Posts/2014/09/Your-Ideas-Needed-The-Grand-Challenge-of-Digital-Financial-Inclusion
22. https://leveloneproject.org/
23. http://www.scmp.com/lifestyle/technology/article/1679904/bitcoin-transactions-cut-cost-international-money-transfers
24. http://innovation.wfp.org/blog/blockchain-crypto-assistance-wfp
25. http://innovation.wfp.org/project/building-blocks
26. http://theconversation.com/can-blockchain-technology-help-poor-people-around-the-world-76059
27. http://www.worldbank.org/en/programs/id4d
28. https://news.itu.int/blockchain-refugees/
29. https://www.bbva.com/en/7-regulatory-challenges-facing-blockchain/
30. https://www.challenges.fr/economie/positive-economy-forum/l-enjeu-de-la-blockchain-pour-nos-societes_425939

Gros plan sur la DOA

Cet article est une traduction du document en anglais élaboré par Chip Sharp en collaboration avec les experts de Internet Society et publié le 25 octobre 2016 à l'adresse : https://www.internetsociety.org/doc/overview-digital-object-architecture-doa

INTRODUCTION

L'architecture d'objet numérique, en anglais Digital Object Architecture (DOA) et le « Handle System » associé sont issus de la Corporation for National Research Initiatives (CNRI) au début des années 1990, sur la base des travaux sur les bibliothèques numériques pour le compte de la Defense Advanced Research Projects Agency (DARPA).[1] L'une des motivations à l'origine de sa conception était la nécessité d'identifier et récupérer des informations sur de longues périodes de temps (de l'ordre de dizaines ou de centaines d'années), dès lors la persistance des données était une exigence de conception critique. À l'époque où elle a été développée, la DOA était une tentative de passer d'un Internet organisé autour d'un ensemble de machines et de la communication entre elles à un Internet organisé autour de la découverte et la livraison d'informations sous la forme d'objets numériques.

QU'EST CE QUE LA DOA ?

La DOA est une architecture générale pour un système distribué de stockage, de localisation et de récupération de l'information via Internet. Elle décrit les composants essentiels pour le fonctionnement, mais permet également une flexibilité dans la façon dont elle est utilisée pour fournir un service, en particulier dans la façon dont les données et les métadonnées sont représentées. Les composantes fondamentales de la DOA comprennent :

- ***Objet numérique***

C'est un enregistrement structuré contenant des données, des informations sur l'état des données et des métadonnées. Les objets numériques peuvent contenir des pointeurs vers les endroits où des informations connexes peuvent être trouvées.

- ***Entrepôts***

Ce sont des systèmes où l'information est stockée.

- ***Handles***

Ce sont des identifiants pour les objets numériques

qui sont uniques, persistants et indépendants du système physique ou logique sous-jacent.

- ***Systèmes de Résolution et Registres***

C'est le système de résolution des Identifiants ou Handles en information sur l'emplacement de l'information et ses référentiels. Les registres définissent des collections d'objets disponibles dans les entrepôts.

Alors que la DOA avait été à la base autorisée pour la définition et l'utilisation des différents systèmes de résolution[2], elle est devenue au fil du temps, presque exclusivement lié au « Handle System ».

Qu'est ce que le Handle?

Un Handle ou Identifiant est défini comme

Préfixe "/" identifiant unique local

où le *Préfixe*[3] est unique dans le « Handle System » et « l'identifiant unique local » est attribué et unique dans le Préfixe.

Les préfixes sont structurés de manière hiérarchique où un gestionnaire de préfixe peut allouer des sous -préfixes (séparés par un « . ») aux organismes subsidiaires. Ceci est similaire au système de noms de domaine (DNS), mais la hiérarchie du « Handle System » est écrite de gauche à droite (xxx.yyy) là où la hiérarchie pour le DNS est écrite de droite à gauche (yyy.xxx) où xxx est le niveau supérieur. Par exemple, la Bibliothèque du Congrès des États-Unis a reçu le préfixe Handle « loc ». La Bibliothèque du Congrès peut alors allouer le sous-préfixe « natlib » pour ses propres fins. Le préfixe Handle complet serait « loc.natlib ». Dans le DNS, la Bibliothèque du Congrès a le nom de domaine de loc.gov. Il a été créé le sous-domaine pour natlib dont le nom de domaine est « natlib.loc.gov ».

Résolution Handle

Le « Handle System » fournit une méthode permettant à un client de résoudre un Identifiant/ handle dans l'emplacement d'un objet numérique.

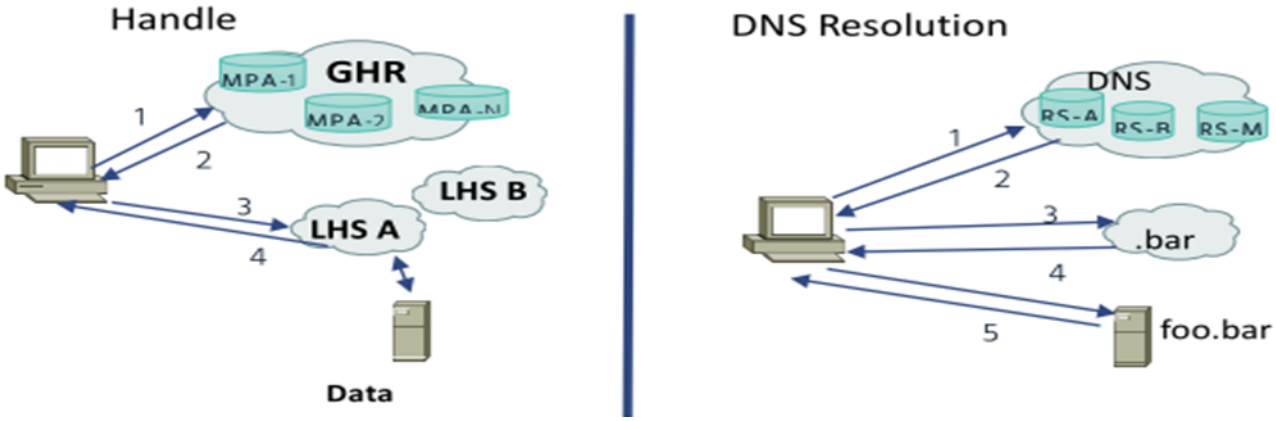

Figure 1 - Résolution Handle

Handle System	DNS
Le client envoie une requête handle au GHR pour 0.NA/bar.foo	Le client envoie une requête DNS au serveur-racine pour foo.bar
Le GHR retourne une information de service pour le 0.NA/bar.foo indiquant que LHS A gère ce préfixe Handle.	Le serveur-racine retourne l'emplacement du serveur DNS pour le « .bar ».
Le client interroge LHS A pour bar.foo/1234.	Le serveur DNS A interroge le serveur DNS .bar pour foo.bar
Le LHS A identifie le server pour le bar.foo/1234. Dans cet exemple, il accède à l'objet numérique et retourne l'information demandée au client	Le serveur DNS B retourne l'information demandée pour foo.bar (adresse IP, serveur de messagerie, etc.).
Le client prend des dispositions relatives à l'information retournée	Le client agit alors sur l'information retournée (Exemple : accède à une page web).

utilise un modèle de service hiérarchique avec le Global Handle Registry (GHR) au niveau de la racine et le Local Handle Services (LHS) sous la racine. Chaque LHS peut contenir sa propre hiérarchie de « Handles Services ». Le GHR contient des informations de mappage pour un préfixe Handle au LHS qui dessert les Handle pour ce préfixe.

La figure 1 illustre cette opération pour le Handle « bar.foo/1234 » où le préfixe de niveau supérieur est « bar » et dont l'information de service est contenue dans LHS A. Le « Handle System » prend en charge les informations de service de mise en cache afin qu'un client n'ait pas toujours à interroger le GHR de la même manière que la résolution DNS met en cache les informations afin qu'il ne soit pas toujours nécessaire d'interroger la racine. Pour comparaison, la figure 1 montre également la résolution de noms DNS pour le nom de domaine foo.bar où bar est le domaine de premier niveau (TLD).

QUI EST RESPONSABLE DU GHS ?

Le Global Handle Registry (GHR) est responsable de la gestion de la racine de la hiérarchie du « Handle System » allouant des préfixes uniques et fournissant un service global pour le mappage des préfixes au LHS pour ce préfixe. Pendant plus de 20 ans, le CNRI a agi comme racine du GHR allouant les préfixes Handle de premier niveau. En 2015, le CNRI a transféré la responsabilité de la racine du GHR à la Fondation DONA (http://www.dona.net).

L'Union Internationale des télécommunications (UIT) a joué un rôle important dans la création de la Fondation DONA en 2014, en collaboration avec le CNRI par le biais de protocoles d'entente pour élaborer les premiers plans pour la transition. Après sa fondation, la Fondation DONA a signé un mémorandum d'entente avec l'UIT dans lequel l'UIT a accepté de fournir le soutien de secrétariat à la Fondation DONA, de détenir les droits de propriété intellectuelle et les licences sur la technologie GHR et les logiciels de la Fondation DONA et fournir des conseils à la Fondation DONA en matière de politique publique. En plus des opérations de la GHR, la Fondation DONA a accepté de contribuer à ses droits de propriété intellectuelle à l'UIT et de soumettre des questions liées à Politique publique à l'UIT.[4]

Lorsque la Fondation DONA a pris en charge la gestion du GHR, elle a également fait le choix d'une architecture dans laquelle l'opération GHR est répartie entre un ensemble d'organisations appelées Administrateurs Multi-Primaires (AMP). Chaque AMP reçoit un préfixe de niveau supérieur à partir duquel il peut allouer des sous-préfixes et collectivement avec les autres AMP et la Fondation DONA réalise les fonctions du GHR. Chaque AMP vérifie et réplique tous les préfixes attribués par les autres AMP. Ainsi, chaque AMP porte une réplique de l'intégralité du GHR.

Dans ce système, la Fondation DONA autorise les AMP et leur attribue des préfixes. La Fondation

Organisation	Date	Préfixe
Corrporation for National Research Initiatives (CNRI) - US	3 avril 2015	20
Coalition for Handle Services (ETRI, CDI and CHC) - China[5]	9 décembre 2014	86
Gesellschaft für Wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG)/ePIC	9 février 2014	21
International DOI Foundation (IDF) - UK	1er janvier 2016	10
Communications and Information Technology Commission (CITC) – Saudi Arabia	1er juillet 2016	?

DONA et les AMP se coordonnent pour maintenir et améliorer les opérations du GHR, mais la prise de décision pour les politiques et les processus se trouve au niveau du conseil d'administration de DONA. Les AMP actuels énumérés par la Fondation DONA se trouvent dans le tableau 1.

Notez que si tous les AMP utilisent des préfixes de niveau supérieur, les organisations disposant d'un préfixe de niveau supérieur ne sont pas toutes des AMP. La documentation actuellement disponible sur le site Web de la fondation DONA ne fournit pas d'information sur le rôle que les préfixes de niveau supérieur non AMP joueront dans le nouveau système.

L'UIT (Handle 11) a été initialement désigné AMP comme indiqué dans le procès-verbal de la réunion du Conseil de la fondation DONA de 2014, mais n'est pas répertorié comme AMP sur la page Web de la Fondation DONA. Selon une communication lors de « African IGF » en octobre 2016, la Fondation DONA a signé un accord AMP avec la République d'Afrique du Sud, mais cela n'a pas encore été reflété sur le site web de DONA.

Quelques exemples de systèmes basés sur la DOA / « Handle Sytem »

Plusieurs systèmes ont basé leur fonctionnement sur le « Handle System » et le GHR. Chaque organisation exploitant un préfixe de niveau supérieur peut définir comment elle utilise le « Handle System », par exemple, la sémantique et la syntaxe de ses Handles et quel business model elle utilise. On s'attend à ce que chacun des AMP détermine les processus d'exploitation et les politiques pour l'utilisation de son préfixe. Des exemples de tels systèmes sont :

- *Système DOI® - http://www.doi.org*

Le système DOI est géré par la Fondation Internationale DOI (IDF), une société à but non lucratif basée au Royaume-Uni créée en 1998 par plusieurs associations professionnelles internationales d'édition pour soutenir l'édition numérique. Bien qu'il utilise le GHR et « Handle System », fonctionnant sous le préfixe 10, il définit sa propre syntaxe et sémantique pour les Handles, les métadonnées à utiliser dans son système, de nombreux aspects opérationnels de l'utilisation de son système et de son modèle d'entreprise. De nombreux services fonctionnent sous le système DOI tel que EIDR (http://eidr.org) et CrossRef (http://www.crossref.org).

- *Persistent Identifier Consortium for eResearch (ePIC) - http://www.pidconsortium.eu/*

ePIC fournit un système d'identification persistant pour la communauté européenne de la recherche et est basé sur le « Handle System », fonctionnant sous le préfixe 21. Il développe ses propres politiques pour l'attribution de ses identifiants.

Normes et « Handle System »

Un aperçu du « Handle System », la description des définitions de l'espace de noms du « Handle System » et des définitions de service et la version 2.1 du protocole Handle sont spécifiées dans trois RFC[6 7 8] d'information publiés en 2003. En outre, « hdl » est enregistré sous le schéma URI « info » (info : hdl) qui est défini dans RFC 4452[9].

Les composants fonctionnels et la syntaxe du système DOI sont normalisés dans ISO 26324:2012 pour l'opération sous le préfixe 10. Il impose une syntaxe spécifique au format Handle au-dessus et au-delà des RFC du « Handle System » et définit des métadonnées supplémentaires à utiliser dans le système DOI. La Fondation internationale DOI est l'autorité d'enregistrement pour l'ISO 26324:2012[10]

pour le préfixe 10. La syntaxe DOI a également été normalisée aux États-Unis par l'Organisation nationale des normes d'information (NISO) en 2005 sous le numéro Z39.84-2005 (révisé en 2010)[11].

En 2013, l'UIT-T a publié la Recommandation X.1255[12] décrivant un cadre général pour la découverte d'informations sur la gestion d'identité. Aucun protocole n'est normalisé dans le cadre de X.1255. Bien qu'il soit basé sur l'architecture des objets numériques, X.1255 ne spécifie pas les Handles ni les protocoles du « Handle System ». Il existe des propositions pour utiliser la DOA dans la Commission d'études 20 (SG20) pour Internet des objets et pour un mécanisme contre la contrefaçon.

CONSIDÉRATIONS POLITIQUES

Le « Handle System » a fonctionné depuis plus de 20 ans, principalement pour une utilisation spécialisée dans les bibliothèques numériques et la recherche. Avec le passage de la GHR à la Fondation DONA, certaines organisations ont manifesté leur intérêt à devenir un système de résolution d'identifiant général sur Internet. Cependant, il soulève un certain nombre de questions liées à la gouvernance et à la politique.

- Persistance

La persistance des identifiants et des objets a été l'un des principaux objectifs de la DOA et du « Handle System ». Bien que l'utilisation des Handles permette la persistance, l'expérience a montré que la principale exigence pour la persistance est dans l'opération et l'administration du système. Par exemple, il importe peu que le système permette la persistance si l'administrateur oublie de mettre à jour l'objet.

- Conflits d'espace de noms

Le « Handle System » permet aux préfixes de contenir des caractères alphanumériques, par exemple « loc », « cnri ». Le « Handle System » fait face à plusieurs des mêmes problèmes auxquels sont confrontés les registres DNS concernant les marques déposées, les noms protégés, etc. On ne sait pas très clairement comment ces conflits seront abordés par la Fondation DONA et les AMP.

- Gouvernance

Transparence : La gestion des ressources Internet nécessite un modèle de gouvernance avec un haut niveau de transparence pour tous ses processus et ses politiques, par exemple, comment sont prises les décisions, comment les AMP sont-elles sélectionnées et leur accord avec la Fondation DONA, comment les préfixes de niveau supérieur sont-ils attribués? Sans une telle transparence, il sera difficile d'obtenir la confiance des utilisateurs du système. La récente transition de IANA Stewardship illustre le rôle crucial que joue la transparence dans l'exploitation des systèmes d'identificateurs Internet mondiaux. Jusqu'à présent, ce niveau de transparence n'a pas été mis en œuvre par la Fondation DONA dans le fait que très peu d'informations sont disponibles sur leur site web (https://www.dona.net/documents/).

Processus de développement des politiques (PDP) : Le fonctionnement d'un système d'identifiant global pour Internet requiert un processus de développement de politique ouvert, multipartite, bien défini et transparent. Le processus doit être ouvert pour examen et doit refléter les intérêts de tous les participants du système ainsi que de la communauté Internet. A ce jour, sur la base de la documentation accessible au public, le processus d'élaboration des politiques pour le GHR est opaque et limité au Conseil et aux AMP sans examen public ni consultation avec la communauté des utilisateurs plus large.

Protection contre la capture : Le système doit être

protégé de la capture par un groupe particulier de parties prenantes. Un système légitime doit être protégé de la capture par un groupe particulier de parties prenantes. En raison de la relation spéciale que la Fondation DONA a avec l'UIT (un organisme intergouvernemental et conventionnel), comme en témoigne leur protocole d'accord de 2014, il est préoccupant que le système soit récupéré par les gouvernements et soumis aux contraintes géopolitiques plutôt qu'à l'efficacité technique, en particulier dans le cas d'un événement de reconstitution.

- Standardisation

A ce jour, la plupart des spécifications du « Handle System » ont été sous contrôle du CNRI. Les spécifications pour les systèmes d'identifiants Internet globaux doivent être développées par un organisme de normalisation multipartite ouvert qui suit les principes de OpenStand[13].

- Economie / Modèle d'entreprise

Alors que le « Handle System » a été utilisé pendant de nombreuses années dans les systèmes de publication et de bibliothèque, la généralisation à d'autres applications, l'Internet des objets par exemple, générera probablement des problèmes économiques liés au modèle d'entreprise du système, en particulier au GHR. Les organisations seront-elles facturées pour chaque identifiant? Les organisations qui acquerront un préfixe pourront-elles créer des sous-préfixes illimités ou seront-elles facturées pour chaque sous-préfixe? Comment ces politiques seront-elles développées? Comment l'argent circulera-t-il? Quel sera l'impact sur les pays en développement ou les petites entreprises?

- Sécurité, stabilité et résilience

L'exploitation d'un système d'identifiant global pour Internet implique d'exposer à la fois le registre des identifiants et le système de résolution à un degré d'attaque potentiellement élevé par différents acteurs, spécialement d'autant plus que la valeur du système augmente. La sécurité, la stabilité et la résilience d'un tel système doivent être comprises et le système doit être capable d'opérer sous des attaques sévères. Par exemple, pendant le fonctionnement normal, le serveur-racine DNS J, l'un des 13 serveurs-racine, voit plus de 6 milliards de requêtes par jour. Nous n'avons aucune preuve à ce jour que le GHR puisse gérer une charge similaire en plus de se protéger contre les attaques massives de déni de service distribué (DDoS) vues sur Internet aujourd'hui.

Notes et références

1. Kahn, R. & Wilensky, R., "A Framework for Distributed Digital Object Services", Int J Digit Libr (2006) 6: 115.
2. Kahn, R. & Wilensky, R.,op. cit.
3. Prefix was called "Naming Authority" in RFC 3651.
4. Briefing from ITU Secretary General to ITU Council in 2015 (C15/95-E) Coalition for Handle Services (ETIRI / CDI / CHC) Consortium is jointly funded by the Institute of Electronic Science and Technology Information echnology (ETIRI) of the Ministry of Industry and Information Technology (CDI), Beijing Zhongxin Innovation and Technology Co.
5. Sun, S., Lannom, L., and B. Boesch, "Handle System Overview", RFC 3650, November 2003.
6. Sun, S., Reilly, S., and L. Lannom, "Handle System Namespace and Service Definition", RFC 3651, November 2003.
7. Sun, S., Reilly, S., Lannom, L., and J. Petrone, "Handle System Protocol (ver 2.1) Specification", RFC 3652, November 2003.
8. Van de Sompel, H., Hammond, T., Neylon, E., and S. Weibel, "The "info" URI Scheme for Information Assets with Identifiers in Public Namespaces", RFC 4452, April 2006.
9. International Organization for Standardization (ISO), "ISO 26324:2012 Information and documentation -- Digital object identifier system", ISO Standard 26324, June 2012.
10. ANSI/NISO Z39.84-2005 (R2010) Syntax for the Digital Object Identifier. (revised 2010)
11. ITU-T Recommendation X.1255, Framework for discovery of identity management information, ITU-T, 2014

—> METADATA ou METADONNEE

Le terme métadonnée (en anglais : metadata) est apparu dans le cadre de la description de ressources sur Internet dans les années 1990 et s'est ensuite généralisé. Aujourd'hui, dans le domaine des services du numérique/TIC, les métadonnées sont devenues incontournables, leur implémentation sont diverses et s'étendent aux fichiers et documents (.pdf, .html, .docx,...), aux logiciels et système libres comme propriétaires (MS Office, Libre Office, OpenOffice, Linux, Windows, Mac OS), et même sur le matériel.

Composé du préfixe « Méta » (du grec « meta » signifiant « après » ou « ce qui dépasse » ou encore « ce qui englobe ») et du suffixe anglais « Data » (donnée en français), les MetaData ou « métadonnées » sont donc des renseignements structurés décrivant les données. Ainsi, les métadonnées sont développées à partir et en fonction de données et c'est pourquoi on les désigne souvent comme des « données sur des données » ou de « l'information sur de l'information ».

Autrement dit, les métadonnées sont des informations servant à définir une ressource quel que soit son support (papier ou électronique) et à en présenter les caractéristiques. Elles ont pour but de favoriser l'utilisation et la diffusion de la donnée en précisant les caractéristiques et les précautions d'emploi à respecter.

Structurellement parlant, les métadonnées sont constituées de mots, formules, etc. Elles sont créées de façon automatique ou manuelle et peuvent avoir plusieurs niveaux de complexité puisqu'elles sont destinées à être exploitées par différents utilisateurs (expert, non expert, machine, etc.).

Si leur utilisation est vulgarisée, c'est notamment parce que leur implémentation donne une réelle valeur ajoutée à la Data. En effet, elles présentent de multiples intérêts plus importants les uns que les autres.

Elle permet une recherche plus simple et plus intuitive des données et une interopérabilité des objets sur un réseau. De plus, les métadonnées aident à l'authentification des objets, la gestion et la protection des droits.

Ainsi, cette omniprésence des métadonnées dans multiples domaines et particulièrement dans le domaine de l'informatique a irrévocablement conduit à une standardisation, une normalisation. A cet effet, plusieurs ont été produites dans les domaines de l'archivage informatique, du patrimoine culturel, du commerce électronique etc.

ARTCI

AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

L'ARTCI scrute le paysage des TIC afin de déterminer de nouveaux sujets d'informations. Ces sujets permettent d'analyser l'actualité du secteur, de mieux comprendre les enjeux de la régulation et l'impact des TIC dans la vie de tous les jours.

Juillet 2017

Abidjan, Côte d'Ivoire