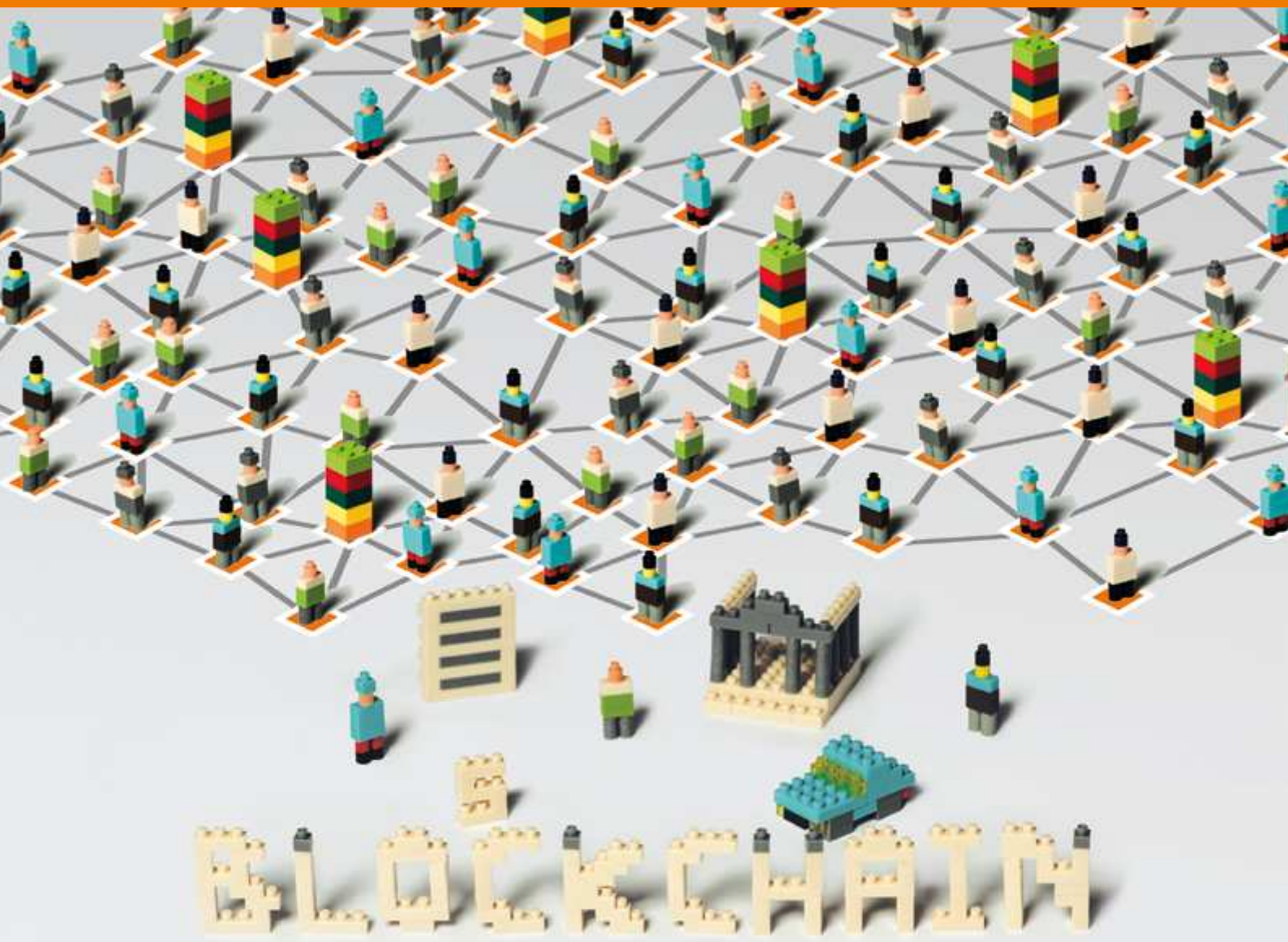
COMPRENDRE LA BLOCKCHAIN



ANTICIPER LE POTENTIEL DE DISRUPTION DE LA BLOCKCHAIN SUR LES ORGANISATIONS

PUISSANCE PUBLIQUE ■ ÉNERGIE ■ INTERNET DES OBJETS ■ CULTURE ■ COVOITURAGE
NOTARIAT ■ ASSURANCE ■ VIE PRIVÉE ■ LOGISTIQUE ■ CITOYENNETÉ ■ CROWD-EQUITY

Plateforme de transformation digitale

Conseil • Recherches externalisées • Relations startups • Opérations digitales

@Uchange_

Livre blanc édité en Janvier 2016 par U • uchange.co

COMPRENDRE LA BLOCKCHAIN

04_ ÉDITO
Guillaume Buffet, Président de U

06_ LE COMITÉ D'EXPERTS
Présentation des six membres

PARTIE I > COMPRENDRE **LE FONCTIONNEMENT** DE LA BLOCKCHAIN

11_ **PARTIE I – I**

Les trois propriétés de la Blockchain : désintermédiation, sécurité & autonomie

14_ FOCUS
La Blockchain et vie privée

15_ FOCUS
Comprendre le débat entre blockchain privée et blockchain publique

16_ **PARTIE I – II**

La Blockchain en mouvement
Les applications distribuées : smart-contract et organisation décentralisée autonome

20_ FOCUS
L'adoption des applications distribuées & Ethereum

PARTIE II > COMPRENDRE **LES APPLICATIONS** DE LA BLOCKCHAIN

22_ **PARTIE II – I**

Les trois défis pour l'adoption de la Blockchain

26_ FOCUS
La blockchain Bitcoin & le leadership français

30_ INTERVIEW
Jean-Baptiste Dezard : Smart-Contract, enjeux et perspectives

34_ **PARTIE II - II**

Onze exemples sectoriels

_ Puissance Publique
_ Énergie
_ Internet des Objets
_ Culture
_ Notariat
_ Covoiturage
_ Assurance
_ Vie privée
_ Logistique
_ Citoyenneté
_ Crowd-Equity

52_ **LEXIQUE**
Bitcoin • Clef publique/privée • Miners
Mining • Proof-of-work • Token

54_ **BIBLIOGRAPHIE**

ÉDITO

La Blockchain :
INTERNET, DE L'EXPRESSION À L'ACTION

A 47 ans, j'ai enfin passé plus d'années avec que sans internet. A l'aube des années 1990, ma fascination pour cette nouvelle technologie n'a pas été tant l'extraordinaire mine d'informations disponibles, que la possibilité offerte à tous de s'exprimer à tout moment.

IRC, forums, blogs, réseaux sociaux : ***ces évolutions du web « 2.0 »*** ont permis avec les années aux ***récepteurs*** citoyens numériques (vous vous souvenez, ceux que l'on appelait les internautes) d'utiliser leur voix avec une force équivalente à celle des ***émetteurs*** médias, élus, entreprises. Une véritable prise de pouvoir du peuple numérique ?

Pas tout à fait encore. Car l'expression n'est pas l'action. Se faire entendre n'est pas prendre les rênes. Le phénomène Blockchain porte en lui les germes d'une révolution plus importante encore que celle liée au web. La révolution qui va permettre à tous ceux qui le souhaitent de passer à l'action.

La technologie Blockchain que certains présentent comme ***« The world computer »*** permet en effet à tout développeur de concevoir et distribuer des projets qui repensent les organisations politiques (régulations, démocratie, ...), économiques (gouvernance d'entreprise, modèles économiques,...) et sociales (gestion des organisations, ...).

Les écueils majeurs – au-delà de l'idée originelle - de tout projet numérique sont liés aux coûts de structure, de développement, de déploiement et sécurisation du projet. Plus le projet est ambitieux, plus l'appel au capital est rendu indispensable (business angels, fonds d'investissements, ...). Le nombre de projets lancés est donc limité à ceux retenus par une élite économique installée, selon des critères quasi systématiquement liés à leur seule rentabilité économique court-terme (bien loin donc de critères d'ambition plus générale).

La Blockchain n'est qu'un socle technologique, mais un socle structurellement accessible, partagé ET sécurisé. Elle lève donc virtuellement la très grande majorité des écueils liés au lancement de projets numériques. En rendant tout projet possible et pérenne ***by design***, elle redistribue les cartes du pouvoir : seuls les développeurs d'un

> *« La Blockchain invalide tout pouvoir économique, politique ou social issu d'une mainmise technique (ou régulation) sans valeur ajoutée perceptible par l'utilisateur. »*

projet et ses futurs utilisateurs seront responsables de son adoption, de son succès (ou de son échec).

La Blockchain invalide tout pouvoir économique, politique ou social issu d'une mainmise technique (ou régulation) sans valeur ajoutée perceptible par l'utilisateur final, car elle rend possible le développement d'un service autonome équivalent à moindre coût. Elle permet donc une créativité sans contrainte (ou presque) et donc virtuellement sans limite (plus de 2 000 développeurs se sont retrouvés lors de Devcon One à Londres en novembre dernier). Parallèlement, elle va obliger tous les gestionnaires de rentes à se remettre fondamentalement en question sous peine de se faire « disrupter » : plus que jamais, l'antériorité n'est plus gage de légitimité, loin s'en faut.

Rendre accessibles les éléments clef de la transformation digitale de l'économie ; vous permettre d'appréhender les sauts technologiques et d'inventer des nouveaux modèles pour vos organisations, telle est la vocation de U. Nous sommes convaincus que la technologie Blockchain va servir la créativité indispensable à la remise en question des modèles établis et qu'elle nourrit l'innovation de rupture sans laquelle les grandes organisations ne pourront s'adapter au nouveau monde qui est le nôtre.

C'est pourquoi nous avons choisi de rédiger ce livre blanc, avec l'aide de nombreux acteurs de l'écosystème de la Blockchain.
Ce livre comprend deux parties ; la première explique la technologie, la seconde fournit des études de cas, ou ***verticales***.
Pour permettre à chacun de comprendre les enjeux liés à cette technologie.

Bonne lecture, et pour tout commentaire, merci d'utiliser feedback@uchange.co

Guillaume Buffet, Président de U

LE COMITÉ D'EXPERTS

Nous remercions les membres de notre comité d'experts pour avoir partagé leurs visions et leurs expertises. La rédaction a été menée par l'équipe de U, avec l'apport de Adli Takkal-Bataille, consultant fondateur du site référence Le-Coin-Coin.fr.

Primavera de Filippi

Chercheuse permanente au CNRS et professeure associée au Berkman Center de Harvard

—

Primavera est co-fondatrice de la société BackFeed.cc.

« La situation est analogue au début des années 1990 quand toutes les organisations voulaient leur .com : nous allons vivre la même ruée vers l'or avec la Blockchain. »

Richard Caetano

Auteur de Learning Bitcoin et CEO de Stratumn

« Les individus attendent davantage de preuves et de données. Ils demandent plus de transparence. Autant de nouvelles exigences auxquelles la Blockchain peut répondre. »

Florian Graillot

Contributeur pour TechCrunch

« Si Bitcoin est présent depuis plusieurs années, c'est son architecture sous-jacente – la Blockchain – qui est son innovation la plus intéressante et la plus disruptive. »

Dan Elitzer

Co-fondateur du Club Bitcoin du MIT et business-designer chez IDEO Futures

« L'écosystème Blockchain évolue dans le bon sens : l'effervescence des entrepreneurs est là, des acteurs traditionnels font preuve d'ouverture et les capitaux-risqueurs commencent également à manifester de l'intérêt. »

Jean-Baptiste Dézard

Fondateur de Deal-ex Machina

« L'erreur serait de croire que la Blockchain est une fintech, c'est une technologie qui va bien au-delà du secteur financier. »

Kariappa Bheemaiah

Consultant à U et professeur associé à Grenoble École de Management

« La Blockchain est un instrument inouï pour rationaliser les échanges de toutes sortes. »

INTRODUCTION

La Blockchain
une révolution transactionnelle

Depuis les toutes premières communautés, l'être humain vit en groupe. Cette vie en groupe, des caves paléolithiques aux mégalopoles, a un corollaire indépassable : la nécessité d'effectuer des transactions.

1. TIERS DE CONFIANCE, MONNAIE ET PROPRIÉTÉ

Jusqu'au XVII ème siècle avant notre ère, le modus-operandi est le troc, puis les premières pièces de monnaies sont battues au Moyen-Orient et des unités de compte interopérables sont mises en place. Viennent ensuite les monnaies fiduciaires où la valeur est détachée du support physique, et enfin, l'époque que nous connaissons avec la digitalisation des moyens de paiement.

Parallèlement, au tournant des Lumières, **la notion de propriété se développe**, portée par les écrits de Rousseau et Locke. La consolidation des États européens favorise la création des premiers registres nationaux, comme le cadastre napoléonien.

Ce cadastre répond au besoin d'un document de référence utilisable lors des transactions entre particuliers. Il est adopté car le pouvoir de l'Empire et de son administration le rend « digne de confiance ».

Comme le rappelle son étymologie latine, **la confiance est le cœur de la monnaie fiduciaire**. Contrairement à une pièce de métal, la valeur intrinsèque d'un billet de banque est nulle. C'est la confiance dans le fait que sa valeur nominale est partagée par tous qui compte. Pour que cette confiance soit maintenue, les monnaies fiduciaires sont adossées à des institutions (d'abord des villes puis des États et enfin des organisations internationales). C'est la naissance des banques centrales. **Un tiers de confiance est alors une condition sine qua non au développement de la monnaie et de la propriété**.

Monnaie du Duché de Lorraine et de la Maison d'Alsace, XIV ème siècle

2. LA VIRTUALISATION DES TRANSACTIONS

Les modalités de transaction se complexifient et suivent les évolutions de l'économie. Portés par les premiers accords GATT de 1947 et l'abandon de l'étalon-or à Bretton-Woods en 1948, le commerce international et la division internationale du travail s'accélèrent tout au long de la deuxième moitié du XX^{ème} siècle. **L'augmentation des transactions transfrontalières génère une augmentation du risque et, de facto, fait appel à de nouveaux tiers de confiance**. C'est le sens de la création du système interbancaire SWIFT en 1977 ou de l'OMC en 1995, par exemple.

La mission de ces tiers de confiance est double : apporter les conditions d'un échange sécurisé, sans risque de perte pour les acteurs économiques (principe d'une chambre de compensation), et fluide. L'échange doit être le moins coûteux et le plus rapide possible.

3. L'INNOVATION AU SERVICE DE LA CONFIANCE

Deux innovations vont bouleverser la manière dont la confiance est générée : **l'avancée de la cryptographie et les architectures informatiques distribuées**.

1976
La cryptographie asymétrique : la double clef publique / privée

En 1976, les chercheurs américains Whitfield Diffie and Martin Hellman présentent **le concept révolutionnaire de double clef publique et privée**. Le protocole Diffie-Hellman permet à deux agents d'échanger entre eux de manière cryptée sans avoir besoin d'un mot de passe.
Cette innovation constitue la genèse de la technologie Blockchain.

Cette innovation théorique va de pair avec une augmentation exponentielle de la puissance de calcul informatique associée à la disponibilité de ces unités de calcul (Cloud computing). La cryptographie à disposition de tous et virtuellement « incassable » est née.

1990
Les architectures distribuées : le Web

Parallèlement, **les architectures distribuées s'imposent comme une référence en termes de stabilité et de sécurité**. Le meilleur exemple de ces caractéristiques est né dans les laboratoires du CERN au début des années 1990 : le web (HTML). Réseau ouvert et décentralisé, il a prouvé sa robustesse en ne connaissant aucune rupture majeure depuis plus de 20 ans. En termes de sécurité, le fait qu'aucune attaque informatique ne soit parvenue à mettre à mal l'ensemble des noms de domaines souligne de manière empirique cette robustesse.

L'architecture mondiale de la gestion des noms de domaines et les serveurs de noms de domaine associés (DNS), distribués et répliqués dans les « nœuds » de l'Internet depuis la création de l'ICANN (1998) n'ont jamais failli depuis leurs créations.

Wikileaks est autre exemple de la sécurité des architectures distribuées. Les documents rendus publics par Julian Assange ont été répliqués à la vitesse de l'éclair dans plusieurs centaines de serveurs rendant leurs modifications ou destructions impossibles malgré la volonté affichée des plus grands représentants des pouvoirs établis dans le monde. Il est incontestable que s'ils avaient été concentrés dans un serveur unique, aussi sécurisé soit-il, une puissance (informatique) aurait pu briser cette protection.

Cryptographie et architectures distribuées sont génératrices de confiance *ex-nihilo*.
Elles vont converger pour former la couche technologique du Bitcoin : la Blockchain.

4. SOUS LES BITCOINS, LA BLOCKCHAIN : LA CONFIANCE « BY DESIGN »

2008
Naissance de la Blockchain

En 2008, Satoshi Nakamoto, la mystérieuse figure derrière l'invention de Bitcoin, publie « *Bitcoin: A Peer-to-Peer Electronic Cash System* ». Il y expose une méthode pour résoudre un problème cryptographique sur lequel achoppait la recherche depuis plusieurs décennies, *le problème du double paiement ou problème des Généraux Byzantins*. Celui-ci empêchait à deux agents d'échanger des actifs, comme une monnaie par exemple, sans le passage par un tiers de confiance.

La solution repose sur l'architecture décentralisée qui supporte Bitcoin : la chaine de blocs, ou blockchain. **Cette découverte est historique dans la mesure où elle autorise ce qui était auparavant impossible** : deux agents qui ne se connaissent pas peuvent échanger des actifs sans que la transaction ne doive être sécurisée et validée par une autorité centrale. Le besoin d'une chambre de compensation disparaît — une nouvelle désintermédiation.

Le premier type de transaction a été le Bitcoin mais Nakamoto prévoyait l'extension du champ d'application. **L'ensemble des actifs nécessitant un bureau central pour être échangés peuvent *a priori* être disruptés par la technologie Blockchain** : actifs financiers, titres de propriété… La confiance créée intrinsèquement par la Blockchain est un outil de désintermédiation. Celle-ci a pour effet de réduire les coûts et de fluidifier les échanges.

La puissance de la Blockchain ne se limite pas à des transactions statiques : les contrats passés entre deux agents peuvent inclure des variables, comme la performance ou valeur d'un actif par exemple. Dès lors, le contrat devient intelligent et capable d'opérer sans être adossé à une institution de référence. Et que se passe-t-il quand plusieurs contrats intelligents s'articulent les uns aux autres autour de règles communes ? **Des gouvernances totalement nouvelles peuvent être imaginées pour des organisations, existantes ou à venir !**

Paiements, transactions, contrats : la technologie Blockchain est le possible catalyseur d'une approche totalement disruptive — et non moins vertigineuse — de nos organisations humaines. Approche qui tire son potentiel d'un nouvel ordinateur géant programmé par tous ceux qui le souhaitent : le Monde.

LA GESTION DE TRANSACTIONS GRÂCE À LA BLOCKCHAIN

CONTRAT

ARGENT

PROPRIÉTÉ

1.

Deux personnes s'accordent sur une transaction.

2.

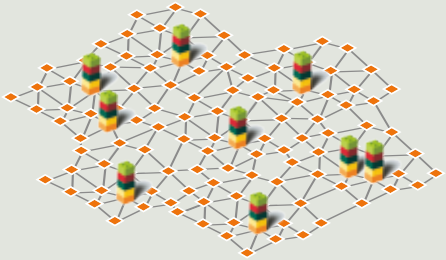
Grâce à la blockchain la transaction est encryptée et validée par consensus.

3.

Elle est ensuite inscrite puis verrouillée dans le dernier bloc de la blockchain.

4.

Enfin la blockchain est répliquée dans tous les nœuds du réseau.



PARTIE I – I

Les trois propriétés de la Blockchain :

désintermédiation, sécurité, autonomie

La Blockchain rassemble trois technologies : architecture décentralisée, protection cryptographique, émission de crypto-monnaie.

QU'EST-CE QUE LA BLOCKCHAIN ?

Littéralement, une blockchain désigne une *chaine de blocs*, des conteneurs numériques sur lesquels sont stockés des informations de toutes natures : transactions, contrats, titres de propriétés, œuvres d'art… L'ensemble de ces blocs forme une base de données semblable aux pages d'un grand livre de comptes. Ce **livre des comptes est décentralisé** ; c'est-à-dire qu'il n'est pas hébergé par un serveur unique mais par une partie des utilisateurs. Les informations contenues sur les blocs sont protégées par plusieurs **procédés cryptographiques innovants** si bien qu'il est impossible de les modifier *a posteriori*. Enfin, la Blockchain, par un mécanisme expliqué plus bas, est créatrice d'une **crypto-monnaie** qui lui permet de rémunérer certains nœuds du réseau qui supportent son infrastructure.

La sémantique est piégeuse. Il s'agit de distinguer **LA Blockchain** comme technologie, fruit des travaux de Natoshi Sakamoto, et **UNE blockchain** spécifique que chaque organisation pourra potentiellement déployer. Il y a fort à parier qu'on parlera un jour de la blockchain des agents immobiliers de telle ou telle région (pour enregistrer les titres de propriété par exemple) ou de la blockchain du gouvernement français (pour la déclaration des impôts par exemple). Dernière difficulté : aujourd'hui, l'expression « la blockchain » désigne souvent la blockchain utilisée par la monnaie Bitcoin, la plus utilisée à ce jour, mais déjà « concurrencée » par d'autres initiatives, à l'image de la blockchain Ethereum qui fédère déjà plusieurs milliers de développeurs et des applications de grande envergure [voir focus page 20].

> *« La conséquence […] est que, pour la première fois, il existe un moyen pour un utilisateur d'Internet de transférer de la propriété digitale à un autre utilisateur d'Internet, avec la garantie d'un transfert sans risque […] et sans que personne ne puisse contester son existence ou sa légitimité. »*
>
> **Marc Andreessen,**
> inventeur de
> l'explorateur Internet

Propriété 1

DÉSINTERMÉDIATION

Le consensus remplace la validation centralisée

La première propriété de la Blockchain est de produire la confiance nécessaire pour que des agents (utilisateurs) échangent sans le contrôle d'un tiers de confiance.

Exemple — Le système bancaire

Les virements internationaux sont coûteux et requièrent plusieurs jours de traitement pour être effectués. À l'opposé, un virement avec une crypto-monnaie comme Bitcoin est quasiment instantané[1], sécurisé et gratuit.

Explications techniques

— Pour qu'une transaction soit effectuée sur la Blockchain, ses informations (volume des fonds disponibles de l'émetteur, destinataire, volume transféré) doivent être intégrées à un bloc.

— Pour cela, la transaction doit être validée par plusieurs nœuds du réseau (appelés les « *miners* » ou mineurs en français) qui vérifient sa conformité en résolvant un problème cryptographique complexe (et consommateur de puissance informatique – [voir focus page 26] pour les impacts énergétiques de la Blockchain). Ce résultat est vérifiable collectivement grâce à « *Proof of Work* » [voir lexique page 52]. L'ensemble de cette opération, et c'est le mot clef, s'appelle le « *mining* » ou *minage* en français [voir lexique page 52].

— Une fois que l'ensemble des mineurs s'accordent sur la validité de la « Proof of Work », la transaction est intégrée à un bloc. Celui-ci vient s'ajouter à la « chaine de blocs ».

Propriété politique

L'ajout de nouveaux blocs est le résultat d'un consensus entre les acteurs du réseau, ce qui rend caduc le contrôle par une institution de référence. Ce consensus est le vecteur de désintermédiation et il s'incarne par la validation collective de la « Proof of Work » ou « Proof of Stake » [voir lexique page 52].

Propriété 2

SÉCURITÉ

L'architecture décentralisée et le code des blocs garantissent l'inviolabilité des informations

Deux mécanismes garantissent la sécurité structurelle des informations enregistrées au sein d'une blockchain : un procédé cryptographique et l'architecture décentralisée. Nous les expliquons séparément.

Exemple 1 — L'horodatage

Le site *proofofexistence.org* fait la démonstration de cette inviolabilité « by design ». Il permet de sauvegarder des documents sur la blockchain du réseau Bitcoin pour justifier de sa possession à un moment donné (le « time-stamping » en anglais, horodatage en français). Parce que le document est inscrit sur la blockchain, cela suffit à prouver que le document existe bien à l'instant T et qu'il n'a pas été modifié en T+n.

1 — Le temps de latence provient du temps de validation, règlé à 10 minutes sur la blockchain Bitcoin.

Explications techniques

Le code de chaque nouveau bloc est construit sur celui du bloc qui le précède dans la chaine de blocs, si bien que la modification d'un bloc impliquerait le changement de l'ensemble des blocs de la chaine, ce qui est impossible.

Exemple 2 — Wikileaks

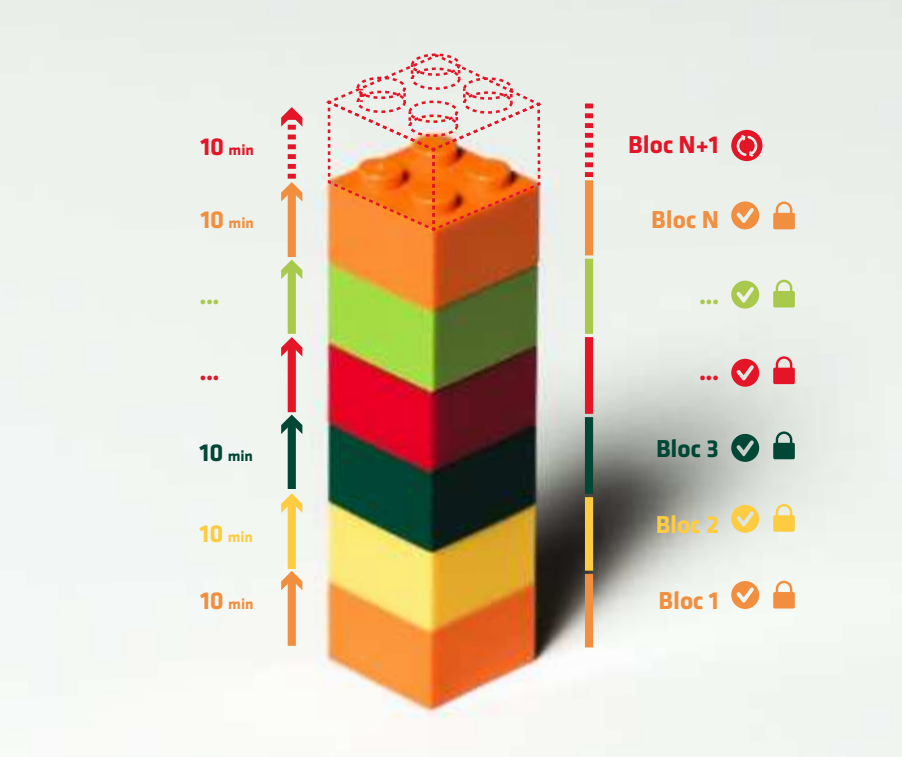
Avant leurs diffusions dans la presse à l'été 2010, Wikileaks a enregistré les documents confidentiels du Département d'État américain sur une multitude de serveurs à travers le monde [voir page 8]. Au lieu d'une « cookie jar » unique, la décentralisation de l'hébergement rend quasi-impossible la suppression de toutes les copies des documents [1bis]. La même logique est à l'œuvre pour Blockchain.

Explications techniques

Au sein d'une blockchain, l'ensemble des blocs est répliqué dans les nœuds du réseau[2], et non pas dans un serveur unique (à date le poids de la blockchain Bitcoin est de 45 Go[3]). Cette architecture décentralisée agit comme une défense structurelle face aux risques de vols de données.

Propriété politique

Ces deux mécanismes garantissent la sécurité des informations enregistrées sur une blockchain. La robustesse de la Blockchain autorise son utilisation pour des informations sensibles.



La chaîne de blocs, fondation de la sécurité Blockchain

1bis — France Info, *Eric Besson ne veut plus que WikiLeaks soit hébergé en France* : bit.ly/1OSNN7j

2 — Dans le cas de la blockchain Bitcoin, ces nœuds sont au nombre de 5 200 en moyenne, répartis tout autour de la planète. [voir focus page 26]

3 — Ce chiffre a doublé en un an. Cette croissance exponentielle du poids de la blokchain représente un défi pour son stockage : cette question est abordée dans la partie II.

FOCUS

La Blockchain et la vie privée

La liste des transactions d'une blockchain peut être consultée par tous : cette transparence est nécessaire pour que les membres du réseau valident les inscriptions sur les blocks et permet de lutter contre la fraude. Pour autant, l'identité de chaque utilisateur est dissimulée derrière un pseudonyme de 27 à 32 caractères. Une blockchain n'est pas anonyme mais pseudonyme.

Capture d'écran d'une transaction en bitcoin : à gauche, l'émetteur, **à droite** le destinataire.

Le degré de transparence d'une blockchain peut s'adapter à des besoins de confidentialité très élevés, on parle alors de blockchains opaques. Celles-ci font appel à des outils pour gagner en confidentialité : adresses furtives, mixing, etc... À l'inverse, si cela est nécessaire, l'identification peut nécessiter plusieurs preuves d'identité et être complètement transparente : la Blockchain est une technologie modulable.

Propriété 3

AUTONOMIE

La création d'une crypto-monnaie rémunère les coûts d'infrastructures

Aujourd'hui, les services en ligne (réseaux sociaux, paiement, hébergement, etc) sont adossés à des plateformes qui assument les besoins d'infrastructure. Dans le cas de Blockchain, la puissance de calcul (hash/seconde) et l'espace d'hébergement sont fournis par les nœuds du réseau eux-mêmes. L'investissement matériel, la puissance de calcul et l'espace de stockage consommés par le mining sont compensés par l'émission de bitcoins (ou autres crypto-monnaies).

PUISSANCE DE CALCUL

Exemple — BitShares.org

BitShares est une plateforme d'échanges et de services adossée à la blockchain Bitcoin. En juin 2015, BitShares est parvenu à effectuer plus de 100.000 transactions en une seconde, une performance au niveau des places boursières mondiales[4].

4 — https://bitshares.org/blog/2015/06/08/measuring-performance/
« Ces performances exceptionnelles sont liées à la technologie spécifique de BitShares et ne concernent pas l'ensemble des produits et services adossés à une Blockchain [voir page 23].

Explications techniques

— Les « miners » allouent une partie de la puissance de calcul (hash/seconde) de leur machine personnelle à la résolution des problèmes cryptographiques nécessaires à la validation des transactions (le « mining »). Cette activité est rémunérée.
— Le premier « miner » à valider un bloc (ensemble de transactions) remporte des « tokens » [voir lexique p. 52] dont la nature varie en fonction de la blockchain concernée.
— Cette opportunité de gains financiers entraine une compétition entre « miners » pour être le premier à résoudre le problème et à proposer une « Proof of work ». Cette situation de concurrence pousse les « miners » à investir dans des machines puissantes et, ainsi, augmenter la puissance de calcul de la blockchain.

De plus, comme vu au point précédent, l'hébergement des blocs constituants la blockchain est assuré par les nœuds du réseau : certains d'entre eux possèdent une copie locale, exhaustive et identique de l'ensemble de la blockchain concernée. D'où l'analogie avec un livre de compte partagé avec les acteurs du réseau.

Propriété politique

Au sein d'une blockchain, l'infrastructure n'est plus concentrée dans les mains d'une organisation mais est, au contraire, éclatée dans l'ensemble des points du réseau. De facto, une blockchain est autoportante et indépendante de services tierces.

FOCUS

Comprendre le débat entre blockchain publique et blockchain privée

Explications

La technologie Blockchain est adaptable : le degré d'ouverture d'une blockchain peut être limité pour créer une blockchain dite « privée » ou de « consortium ». Ce modèle s'oppose aux blockchains dites « publiques », comme celle à l'œuvre derrière Bitcoin, que n'importe qui peut consulter et utiliser. Au sein d'une blockchain « privée », la validation des blocs est effectuée par un nombre, au lancement, plus limité de nœuds du réseau. Pour rappel, seuls ces nœuds ont accès à l'ensemble des informations.

Exemple

Les institutions financières préparent le déploiement d'une blockchain « privée » où la validation des blocs nécessite uniquement l'approbation de 10 institutions, par opposition à une validation par l'intégralité du réseau. Si l'idée de consensus issu de la majorité est mise à mal, ce modèle présente des avantages en termes de rapidité de validation et de coûts d'infrastructure.

Enjeux

La situation est analogue à celle du réseau Internet où des intranets privés cohabitent avec l'Internet public : le débat blockchain publique/privée lie questions idéologiques et enjeux techniques. Certains membres de la communauté Bitcoin originelle voient d'un mauvais œil la privatisation d'une technologie pensée et conçue pour être ouverte.

@StacyHerbert + *« Big banks creating own blockchain is to Bitcoin what Che Guevara is to a tshirt of Che Guevara being worn by hipsters in Brooklyn. »*

PARTIE I – II

La Blockchain en mouvement :
les applications distribuées

Afin que humains et machines puissent inscrire leurs échanges dans une chaine de blocs, au-delà des échanges de crypto-monnaies, deux outils sont disponibles, les *« smart-contracts »* et les *« organisations décentralisées autonomes »*.

> *“Blockchain could be a supercomputer for reality.”*
>
> **Melanie Swan,**
> fondatrice de l'Institute
> for Blockchain Studies

1. LES SMART-CONTRACTS

1A — QU'EST CE QU'UN SMART-CONTRACT ?

Un smart-contract est un programme informatique de type « If This, Then that ». À la manière d'un distributeur de canettes ou bien d'un algorithme de trading à hautes fréquences, le smart-contract applique un contrat une fois que des paramètres donnés ont été atteints : une pièce de 2 € a été insérée ou bien la valeur de l'actif X a dépassé le seuil Y. **La vérification et l'application des termes du contrat ne sont pas effectuées par un tiers de confiance mais par la technologie elle-même**. Pas très « smart » ce premier contrat peut évidemment laisser la place à des options infiniment plus complexes multipliant les options et conditions.

Comment la Blockchain révolutionne-t-elle ce fonctionnement ? La limite historique des contrats autonomes était l'impossibilité de transférer des actifs, comme de la monnaie ou un titre de propriété. Ces échanges nécessitaient l'intervention d'une institution (tiers) de référence (une banque, un notaire).**Un smart-contract exécuté sur une blockchain rend possible transfert automatisé et sécurisé d'actifs digitaux.**

Prenons un exemple. Aujourd'hui, une startup A passe un contrat avec une entreprise B, spécialisée dans le référencement sur les moteurs de recherche. Les termes du smart-contract précisent les objectifs à atteindre (par exemple, être référencé sur la première page Google pour

6 Ce genre de smart-contract dit de «performance» est d'ores et déjà proposé par des sociétés spécialisées.

une requête donnée) et le montant de la prestation. **Les termes du contrat (des lignes de code) sont enregistrés sur la Blockchain et exécutés automatiquement : ils ne sont pas modifiables a posteriori (inviolables) mais restent consultables par les parties prenantes.** Dans notre exemple, le smart-contract vérifie si l'objectif est rempli et déclenche alors un transfert en bitcoins (ou toutes autres crypto-monnaie)[6].

L'utilisation de la Blockchain permet d'injecter une crypto-monnaie dans les termes du contrat[7] et démultiplie les possibilités de contrats privés indépendants du contrôle d'un tiers.

1B — LA SMART-PROPERTY : PONT ENTRE LE VIRTUEL ET LE PHYSIQUE

En plus du transfert de valeur monétaire, la Blockchain révolutionne les contrats grâce **à la Smart-Property, qui permet d'assigner et transférer la propriété d'un bien[8]**. Celui-ci peut être immatériel, dans le cas d'un titre de propriété ou d'une part d'actif financier, ou physique, comme l'accès à ordinateur de bord d'une voiture connectée. Un autre exemple serait un smart-contract qui lie le paiement d'un bien immobilier à une serrure connectée : quand les fonds ont été reçus, la clef privée correspondant à la serrure est transmise au propriétaire.

Au sein d'un smart-contract, les objets connectés fournissent une information prévue pour actionner le contrat. Par exemple, les données de géolocalisation d'un colis peuvent déclencher automatiquement un paiement quand il arrive à destination. À ce stade de développement de la technologie, tous les possibles semblent ouverts : un contrôleur d'humidité pourrait vérifier la qualité d'une cargaison et entrainer un paiement sans qu'aucun agent ne soit contraint d'intervenir, etc.

Les smart-contracts déploient toute la puissance de Blockchain : fluidité et sécurité. Ils sont un outil puissant pour connecter le monde numérique et le monde physique de manière fiable, sans passer par un contrôle humain coûteux et imparfait.

2. LES ORGANISATIONS DÉCENTRALISÉES AUTONOMES, INSTRUMENT DE COORDINATION

2A — QU'EST-CE QU'UNE ORGANISATION DÉCENTRALISÉE AUTONOME ?

Une organisation décentralisée autonome (DAO[9]) est un programme informatique qui scelle dans une blockchain l'ensemble des règles qui régissent une organisation. C'est un outil pour transférer à l'échelle d'une organisation les propriétés de la Blockchain : sécurité, transparence, fluidité. Elle peut s'apparenter à une matrice qui articule une multitude de smart-contracts entre eux.

Au sein d'une organisation traditionnelle, les protocoles de fonctionnement (appartenance, hiérarchie, rétribution ; fondés sur un système légal) sont exécutés par des interactions humaines. Dans une organisation décentralisée autonome, ces protocoles (ensemble de règles de fonctionnement, voire dysfonctionnement) sont définis en amont par la communauté à l'origine de l'organisation, puis inscrits dans une blockchain sous forme de lignes de code et exécutés automatiquement.

7 — Le mystérieux créateur de Bitcoins, avait envisagé ce type d'utilisation en 1997 : http://ojphi.org/ojs/index.php/fm/article/view/548/469

8 — La propriété du bien est déterminée par la connaissance de sa clef privée. La clef privée est une suite de 27 à 34 caractères, semblable à un code PIN, connue de son propriétaire seul. L'utilisation de la double clef privée et publique est explicitée dans le lexique page 52.

9 — DAO pour Decentralized Autonomous Organisation.

ORGANISATION CENTRALISÉE

Une institution, ou un représentant élu est chargé de faire respecter les termes de la « constitution ».

ORGANISATION DÉCENTRALISÉE

Le respect de la « constitution » est assuré par l'organisation décentralisée autonome.

Exemple d'une organisation décentralisée autonome

« La startup BoardRoom.to fournit des DAO à destination des conseils d'administration. Le passage par une DAO rend les règles de fonctionnement (respect du quorum, validation, procuration, etc) inaltérables, libres de toutes interventions humaines et transparente (chaque membre peut consulter le code informatique). En outre, à titre d'exemple, les cotisations annuelles sont transférées automatiquement à partir du compte Bitcoin des membres.

```
function Democracy(token _voterShareAddress, uint _minimumQuorum, uint _debatingPeriod) {
    founder = msg.sender;
    voterShare = token(_voterShareAddress);
    minimumQuorum = _minimumQuorum || 10;
    debatingPeriod = _debatingPeriod * 1 minutes || 30 days;
}


function newProposal(address _recipient, uint _amount, bytes32 _data, string _description) returns (uint
    if (voterShare.coinBalanceOf(msg.sender)>0) {
        proposalID = proposals.length++;
        Proposal p = proposals[proposalID];
        p.recipient = _recipient;
        p.amount = _amount;
        p.data = _data;
        p.description = _description;
        p.creationDate = now;
        p.active = true;
        ProposalAdded(proposalID, _recipient, _amount, _data, _description);
        numProposals = proposalID+1;
    }
```

Ces lignes de code sont un extrait d'une organisation décentralisée autonome, qui encadre le système de vote au sein d'un groupe.

À l'instar des smart-contracts, ces programmes sont auto-exécutoires (*self-enforced* en anglais) ; ce qui les rend autonomes vis-à-vis d'une intervention humaine.

Certaines organisations décentralisées autonomes[9bis] génèrent des « tokens » pour rémunérer les utilisateurs en fonction d'une activité donnée [voir lexique page 52].
Ici, la création monétaire ne provient plus (uniquement) du minage mais, par exemple, de la production d'énergie comme *SolarCoin* ou des kilomètres parcourus comme la solution de covoiturage *La'Zooz* [voir page 42]. Cette rémunération permet alors à l'organisation d'assumer seule ses besoins d'infrastructure [cf propriété 3 page 14].

9bis La terminologie précise des différents types d'organisations décentralisées autonomes est mouvante, comme en témoigne cet article du fondateur de Ethereum [voir page 21] : bit.ly/1OSPpxC

2B — À QUOI SERVENT LES ORGANISATIONS DÉCENTRALISÉES AUTONOMES ?

Les OD éliminent l'erreur et l'arbitraire humain dans les échanges. À la place, un programme informatique coordonne l'ensemble des situations : une OD ne peut pas être prise en défaut. Cette coordination entre agents n'est plus dépendante d'un bureau central.

Le projet **OpenBazaar.org** est une place de marché de petites annonces, semblable à Le Bon Coin ou Craigslist. L'ensemble de son fonctionnement est inscrit dans les lignes de codes d'une OD si bien qu'aucune autorité centrale n'est nécessaire pour administrer le projet. Celui-ci est entièrement décentralisé, ne génère aucun coût (les coûts d'infrastructure sont supportés par les nœuds du réseau, cf. propriété 3 de blockchain). Il est donc gratuit pour l'utilisateur[10].

À une autre échelle, une organisation comme la Sécurité Sociale santé pourrait adosser son fonctionnement à une OD. Celle-ci serait composée de milliers de smart-contracts pour répondre à la situation spécifique de chaque assuré[11]. L'automatisation des transactions générerait évidemment des gains de productivité (temps de traitement), éviterait la fraude et optimiserait la sécurité. La mise en place de smart-contrats ouvrirait de même la porte à une gestion plus individualisée et « raffinée », et pourquoi pas plus démocratique du fonctionnement de l'organisation[12].

A plus court terme, **l'Internet des objets** va devenir un champ majeur d'application pour les OD. La multiplication des objets connectés va augmenter le besoin pour des protocoles intelligents, automatisés, sécurisés et peu consommateurs de puissance informatique. **Les OD proposent le socle technologique adéquat pour ces échanges dits « Machine-to-Machine ».** Les plus visionnaires imaginent déjà, au-delà de l'intelligence artificielle, la conception de programmes qui pourraient inscrire dans le code l'ébauche des éléments de la conscience de robots, dans leurs décisions ou leurs interactions [voir fiche IoT page 37].

10 Cependant, la gestion de la réputation des utilisateurs peut entrainer des coûts marginaux. Ce point est en débat au sein de la communauté OpenBazaar.

11 Cette idée selon laquelle la Blockchain pourrait permettre de personnaliser les services publics, pour les rendre plus adaptés à la situation de chacun, est très présente dans les universités américaines, notamment portée par Alex Pentland, professeur au MIT.

12 L'enjeu – et les conséquences sociales économiques et politiques d'un tel projet sont évidemment considérables et ne peuvent être traitées dans ce document! Entendons-nous bien : il n'est pas question ici d'affirmer que la gestion de l'Assurance Maladie via une architecture de type Blockchain est souhaitable. En revanche, Il est certain qu'elle serait d'ores et déjà possible.

2C — L'ACTUALISATION DE « CODE IS LAW »

> *« This code (…) sets the terms on which life in cyberspace is experienced. […] It affects who sees what, or what is monitored.. »*
>
> **Lawrence Lessig,**
> Code et autres Lois du Cyberespace, 1999

En 1999, le juriste américain Lawrence Lessig prédisait dans Code et autres Lois du Cyberespace la puissance normative du code informatique : « This code (…) sets the terms on which life in cyberspace is experienced. […] It affects who sees what, or what is monitored. ».
Cette vision s'est répandue, autour du raccourci « code is law ».

Avec les organisations décentralisées autonomes et les smart-contracts, l'expression prend une dimension supplémentaire. Dans un monde où de plus en plus d'activités seraient régies par des applications distribuées, chaque situation et chaque interaction répondrait à des règles prédéfinies auxquelles il ne serait plus possible d'échapper. Il n'en est pas moins que ces règles doivent être définies en amont, et que les communautés à l'origine de ces organisations en ont la charge, selon des règles de gouvernance qui leur sont propres.

Primavera de Filippi, chercheuse au Berkman Center de Harvard, explique les difficultés à bâtir une régulation efficace des OD. **Leur autonomie radicale couplée à leur souveraineté sur les ressources (le stockage et le calcul sont effectués par les utilisateurs) semblent les mettre hors de portée des régulateurs**.

La chercheuse oppose alors la loi humaine, universelle et qui laisse une large place à l'interprétation, à la loi informatique, spécifique et rigide. Se dessine alors une opposition entre deux modèles : « Rules of Law » vs. « Tyranny of Code ».

FOCUS

L'adoption des applications distribuées & Ethereum

Des entreprises spécialisées se structurent pour répondre à la demande naissante d'entreprises privées ou d'organisations publiques [voir page 24]. La fondation Ethereum fondée par Vitalik Buterin, développeur de 22 ans, est en passe de prendre une avance décisive. Son avantage concurrentiel réside dans un langage de programmation dédié (dit « Turing-complete ») et dans une crypto-monnaie propre, l'Ether, qui permettent ensemble de construire ses propres applications décentralisées autonomes. **En structurant les couches d'accès à sa blockchain, Ethereum joue un rôle clef dans l'adoption de la technologie Blockchain.**

FOCUS (suite)

ethereum

Ethereum est une fondation à but non-lucratif dont le code source est ouvert. En 2014, l'équipe lève 14 millions d'euros et bat le record de financement sur une plateforme de crowdfunding. Le produit est disponible au grand public depuis le printemps 2015 et rassemble une communauté étendue de développeurs indépendants.

Illustration de cette avance sur le reste du marché, la majorité des projets Blockchain les plus aboutis sont écrits avec Ethereum. Cette domination va-t-elle se transformer en monopole ? Dans l'innovation numérique, les effets de réseau favorisent en effet leurs émergences, que l'on pense à Google pour les moteurs de recherche, Amazon pour l'e-commerce ou bien Facebook pour les réseaux sociaux[13].

Gavin Wood,
un des fondateurs et développeurs essentiels

« Ethereum, the world computer! »

Photographie prise lors du Devcon One à Londres organisé par Ethereum

En novembre 2015, Ethereum organisait le Devcon One à Londres, rassemblant plus de 2 000 développeurs (10 000 attendus pour la prochaine session dans 6 mois).
De multiples projets, politiques, sociaux et économiques ont été présentés. La couche intermédiaire que représente Ethereum ouvre des possibilités infinies de développement, objets connectés ou applicatifs dans des domaines aussi variés que l'industrie, le jeu, l'assurance, l'électroménager, etc...[14]

13 Dans le cas de Ethereum, qui dispose d'une blockchain publique propre, la multiplication de projets utilisant l'Ether va augmenter le nombre de mineurs. Dès lors, la puissance de calcul disponible croît et la blockchain est plus efficace.

14 Notons aussi la blockchain NXT qui ne dispose pas de la visibilité d'Ethereum mais présente de multiples applications concrètes.

PARTIE II – I

Trois défis pour l'adoption de la Blockchain

> *« La Blockchain repose sur trois piliers : un pilier technologique qui s'incarne dans la cryptographie, un pilier social à travers la viralité de la monnaie et un pilier économique avec l'attractivité du mining. Si un de ces trois piliers disparaît, la pleine puissance de la technologie sera bloquée. »*
>
> **Richard Caetano**
> Stratumn, CEO

Durant l'année 2015, la Blockchain a dépassé sa communauté Bitcoin originelle pour s'imposer comme l'une des technologies structurantes de la prochaine décennie. Couronnée par un nombre croissant de conférences, la visibilité de la technologie Blockchain se propage à l'ensemble des secteurs de l'économie et la compréhension de ses mécanismes progresse.

Cependant, ce large potentiel de disruption ne se traduit pas encore dans l'avancement palpable de la technologie : à ce stade, les seules utilisations massives de la technologie Blockchain se limitent au Bitcoin et à des expérimentations par des institutions financières[1]. Ce paradoxe -les attentes espérées sont supérieures à la capacité actuelle de la technologie- est récurrent et s'exprime dans le Hype Cycle de Gartner[2].

1 — Fin décembre 2015, le Nasdaq et la startup Chain ont utilisé une blockchain privée pour effectuer des transactions sécurisées. Cette preuve de concept est en ligne avec le projet « Citi Coin » portée par la banque américaine et l'entreprise Blockchain Ripple.

2 — Cet outil représente l'évolution de la perception d'une nouvelle technologie, qui commence par des attentes très élevées avant de « décevoir » puis d'aborder un « plateau de maturité ». http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

Avant d'explorer dix applications existantes de la Blockchain, nous nous arrêtons sur trois défis pour son développement :
– « scalability »
– expérience utilisateur
– régulation

Couverture de The Economist, 31 octobre 2015
The trust machine, How the technology behind bitcoin could change the world

1. LE DÉFI DU PASSAGE À L'ÉCHELLE

Florian Graillot
Contributeur
chez TechCrunch

« Les volumes d'investissement dans la Blockchain sont faibles : la technologie est palpitante mais la majorité des use-cases doit encore passer l'étape du prototype. »

À l'exception de Bitcoin, et dans une moindre mesure, de plusieurs projets sur la blockchain Ethereum et NXT, l'ensemble des initiatives blockchain sont à l'état de projets ou bien à des échelles relativement limitées si bien que la capacité de la Blockchain à monter en charge *-scalability-* reste à prouver.
Le poids global de la blockchain Bitcoin, aujourd'hui 45 Go, ainsi que le nombre limité de transactions par seconde (7 à l'heure actuelle) sont deux exemples des limites actuelles de la technologie Blockchain. Ils soulignent que des progrès doivent être opérés pour rendre la technologie accessible à tous[3]. Les solutions adéquates sont l'objet d'intenses débats au sein de la communauté blockchain[4].

Pour notre comité d'experts, ces difficultés techniques ne représentent pas une entrave au développement de la technologie sur le long-terme. La baisse du coût de stockage, la créativité historique de la communauté Bitcoins ainsi que l'afflux d'investissements permettront de faire évoluer la technologie Blockchain vers plus de « scalability ».

3 — https://blockchain.info/fr/charts/blocks-size?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=

4 — Les forums Reddit Bitcoin est de ce point de vue une source d'informations précieuses.

2. UN DÉFICIT DE VALEUR-PERÇUE POUR L'UTILISATEUR FINAL

> *« Le premier défi n'est pas la technologie, c'est l'humain. »*
>
> **Dan Elitzer,**
> fondateur du MIT Bitcoin Club

Dans le monde des services en ligne, la qualité de l'expérience utilisateur est déterminante pour la création de nouveaux usages. **La fluidité de la prise en main d'un nouveau service compte souvent davantage que son efficacité théorique ou un meilleur rapport qualité/prix.** À l'heure actuelle, les services Blockchain sont handicapés par un parcours utilisateur souvent trop complexe qui limite la valeur perçue par l'utilisateur.

À titre d'exemple, la participation à une organisation décentralisée autonome ou l'acquisitionde tokens [voir lexique page 52] implique l'installation d'un ou plusieurs logiciels dédiés, peu ergonomiques, et d'une compréhension a priori des mécanismes de la Blockchain. Pour l'utilisateur, ces difficultés à mettre en place un compte client prévalent sur les bénéfices concrets du service, comme la sécurité des données ou la gratuité. Ces prérequis forment une barrière à l'entrée qui limite encore l'adoption de services Blockchain à une population de *geeks* avertis.

Afin de créer des parcours utilisateurs inclusifs, l'écosystème Blockchain va se structurer autour de deux types d'entreprises : d'une part **les plateformes et outils de développement, semblables à des ESN (Entreprise de Services Numériques, anciennes SSII), et d'autre part, les entreprises dites « Blockchain-As-A-Service »** [voir schéma page 28]. Ces deux types d'entreprises mêlent une expertise technologique, avec des développeurs souvent issus de la communauté Bitcoin, et une approche marketing, au contact des problématiques de l'utilisateur, que ce soit en B2B ou en B2C. Écriture de smart-contracts, création d'applications décentralisées ou encore gestion des capacités de mining : ce nouveau type d'entreprise construit l'interface entre la Blockchain et l'utilisateur. Elles sont à la Blockchain ce qu'un logiciel est à un système d'exploitation.

3. UNE RÉGULATION À ÉCRIRE

> *« La croissance de l'écosystème est bien plus rapide que la réaction du régulateur et c'est un frein pour atteindre le plein potentiel de la technologie. Les grands groupes et les institutions ont un rôle décisif à jouer : apporter le cadre structurel et réglementaire pour rendre la Blockchain accessible et utilisable par tous. »*
>
> **Kary Bheemaiah,**
> professeur associé à Grenoble Ecole de Management, et Consultant U

Donner une valeur juridique aux innovations introduites par la Blockchain est indispensable pour l'adoption de la technologie. À titre d'exemple, afin que les services d'horodatage [voir page 12] puissent se généraliser, leur inviolabilité technique doit être

reconnue par le régulateur pour in fine constituer une preuve au regard de la loi.
Autre sujet : **quelle est la valeur juridique d'un smart-contract qui actionnerait le versement des dividendes au sein d'une entreprise ?** Que se passerait-il si un versement était contesté ? Fin 2015, cette régulation des services Blockchain est encore une page blanche.

Cependant, deux facteurs indiquent la prise de conscience du potentiel de la Blockchain par certains régulateurs nationaux.

En premier lieu, **en Europe, aux Etats-Unis et dans plusieurs pays développés, le Bitcoin est en voie de normalisation** comme en témoigne les décisions qui ont jalonnées l'année 2015, notamment les licences dédiées pour les entreprises de crypto-monnaies (État de Californie en mars, New-Jersey en juin, New-York en août) et l'entérinement du statu-quo (la décision, en octobre de la Cour de Justice Européenne de pas appliquer la TVA aux achats de bitcoins et le refus du gouvernement hongkongais de légiférer sur les crypto-monnaies)[5].
Ces décisions reconnaissent la spécificité du Bitcoin et, par ricochet, introduisent à la dynamique de désintermédiation produite par la Blockchain.

Parallèlement, **plusieurs États n'ont pas attendu des textes de loi pour lancer des expérimentations avec la Blockchain** [voir notamment la fiche Puissance Publique pour l'enregistrement du cadastre page 35]. La banque centrale de Singapour investit 225 millions de dollars pour construire un « centre financier intelligent » s'appuyant sur une blockchain. Répondant aux recommandations de la banque d'Angleterre, le Government Digital Service britannique envisage d'utiliser la Blockchain comme répertoire pour les données administratives. À une échelle moindre, l'île grecque de Agistri utilise la crypto-monnaie (distributeur de billets), appelée Nautiluscoin, pour maintenir son activité touristique face à l'absence de liquidités.

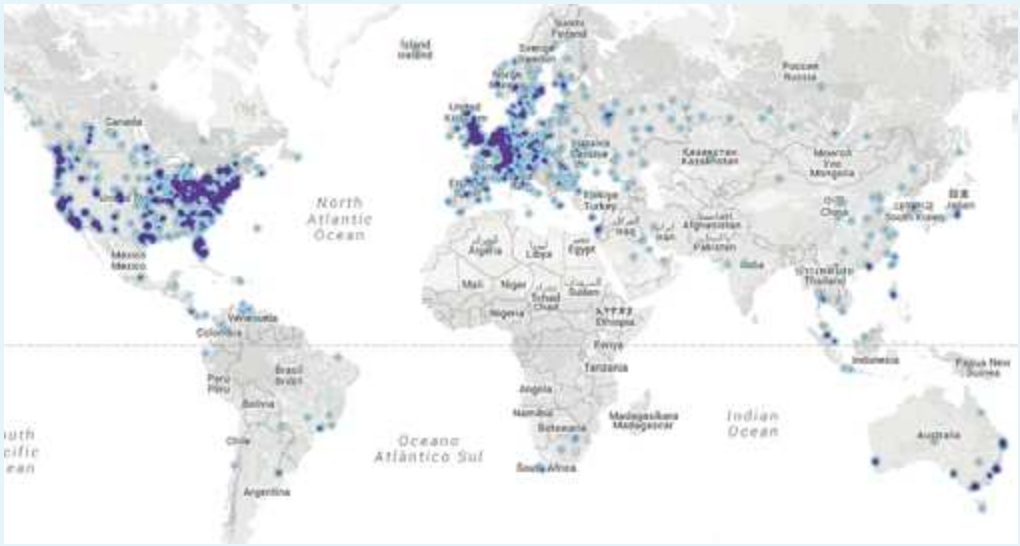
En France, une **initiative lancée en décembre 2015 par la Caisse des Dépôts et Consignations** rassemble plusieurs banques et entreprises spécialisées dans la Blockchain pour « anticiper les opportunités et les impacts induits par cette nouvelle technologie (…) notamment les banques et les assurances ». Cette approche sectorielle doit aller de pair avec une **réflexion plus large sur la régulation des programmes informatiques autonomes** [voir « actualisation de Code is Law », page 20] comme les organisations décentralisées autonomes ou les smart-contracts. Dans la mesure où le code de ces programmes informatiques autonomes est la propriété de leurs créateurs, comment articuler le respect de la propriété intellectuelle et la nécessité d'auditer ces outils pour vérifier leur conformité avec les lois existantes (discrimination, rétention d'informations…) ?
L'obligation de transparence des algorithmes publics incluse dans le projet de loi « Pour une République numérique » va dans cette direction mais laisse entière la question des programmes informatiques autonomes privés.

5 — L'utilisation du Bitcoin reste punie par la loi dans de nombreux pays et sa massification pâtit encore de ses liens avec l'argent sale : https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country#cite_ref-EUPARANNEX_8-0

FOCUS

La blockchain Bitcoin & le leadership français

La première blockchain en activité a été celle de la monnaie électronique Bitcoin, la blockchain Bitcoin. Le premier bloc (appelé « Genesis Block ») a été « miné » le 1er mars 2009 et la blockchain en compte aujourd'hui presque 400 000[6]. À ce jour, c'est la blockchain la plus active avec 5 200 mineurs [voir lexique page 52] en moyenne. En outre, sa consommation énergétique (l'électricité nécessaire pour faire fonctionner le hardware de minage ainsi que, dans certains cas, les systèmes de refroidissement) est très élevée (les estimations divergent en fonction des installations des mineurs : par exemple, une ferme de minage dans l'état de Washington brûle 240kWh par bitcoin miné)[7].



Carte en temps-réel des nœuds du réseau Bitcoin qui valident les transactions. La taille de ces nœuds peut varier fortement (bitnodes.21.co).

La France bénéficie d'un écosystème Bitcoin développé, grâce des startups à succès et une communauté dynamique, à l'image de la place constante de la France dans le top 5 des pays avec le plus grand nombre de mineurs.

Ces cinq startups sont parmi les locomotives de cet écosystème :

- **Blockchain**, le nom de l'entreprise créée par Nicolas Cary, Peter Smith et Ben Reeves, est le premier portefeuille de Bitcoin au monde. Basée à Paris et à New York, l'entreprise affiche plus de 3,7 millions d'utilisateurs et 50 000 transactions par jour. Elle a levé 30 millions de dollars auprès de fonds anglo-saxons. **BLOCKCHAIN.INFO**

6 — Sources : https://blockchain.info/fr/stats, http://realtimebitcoin.info, http://bitnodes.21.co

7 — http://www.coindesk.com/carbon-footprint-bitcoin/ & https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf /

FOCUS (suite)

■ **Paymium** est la première plateforme européenne d'échange Bitcoin/Euro, fondée par Gonzague Grandval, Pierre Noizat et David François. L'entreprise a levé 1 million d'euros durant l'été 2015. **PAYMIUM.COM**

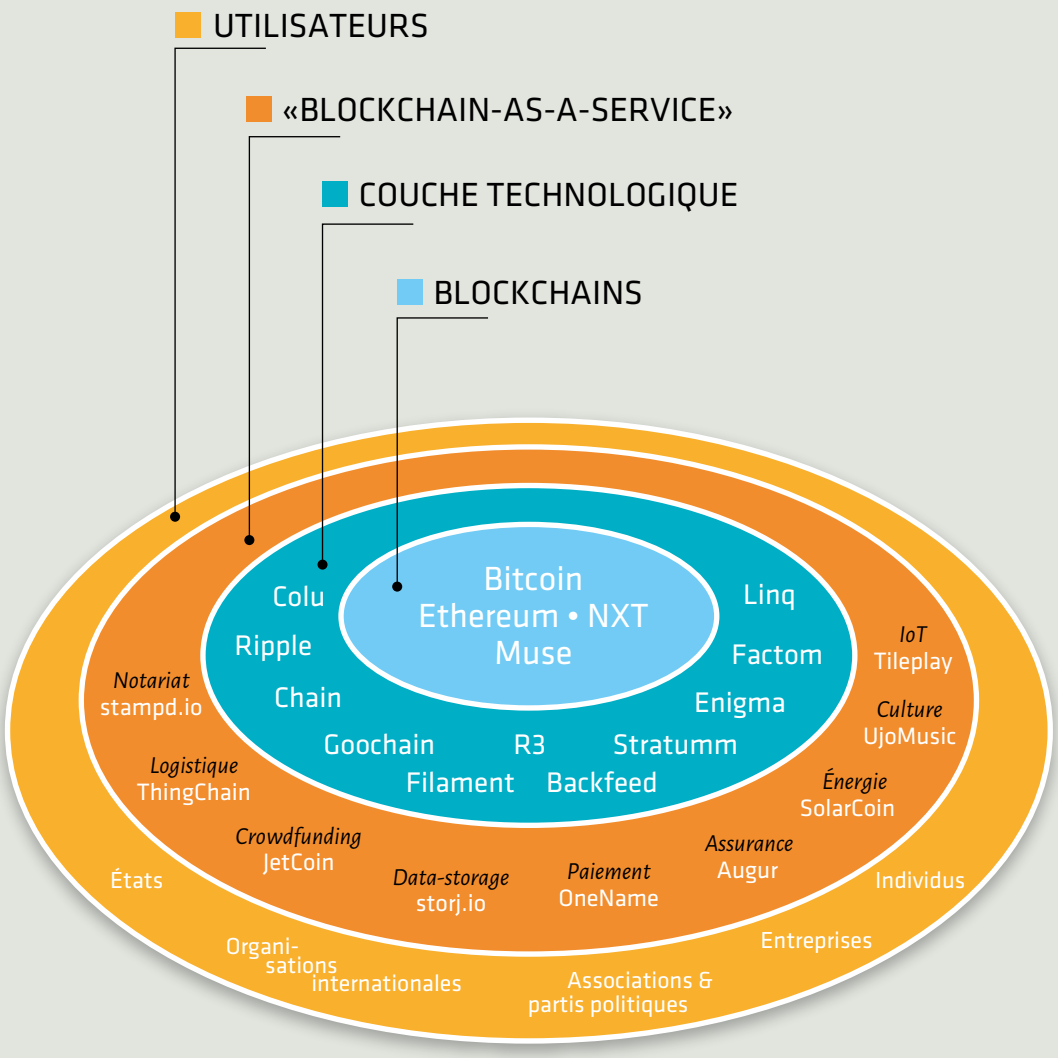
■ Ledger produit des cartes à puces sécurisées pour les portefeuilles Bitcoin et l'identification en ligne. Née de la fusion de la Maison du Bitcoin, **BT Chip et Ledger**, l'entreprise facilite le parcours-utilisateur pour l'acquisition et l'utilisation de bitcoins. Après plus de 5 000 produits vendus et l'ouverture d'un bureau à San Francisco, Ledger (CEO, Éric Larchevêque) a levé 1,3 million d'euros. En outre, la Maison du Bitcoin, où se trouve le bureau parisien de Legder, propose des introductions ludiques et efficaces au fonctionnement de la crypto-monnaie Bitcoin. **LEDGERWALLET.COM**

■ **E-mProvement**, fondée par Alain Cauderlier, développe des produits et services pour la démocratisation du Bitcoin, notamment BTCname qui transforme une adresse bitcoin [voir focus page 14] en un identifiant facile à mémoriser. Fondée en 2013, l'entreprise propose également des formations et des prestations de conseils. **FR.E-MPROVEMENT.COM**

■ **UtoCat** propose une application gratuite pour que les commerçants puissent recevoir les paiements en bitcoins sans subir les variations du taux de change. **UTOCAT.COM**

Par ailleurs, les nombreux échanges, sous la forme de MeetUp, de rencontres informelles comme *Le Repas du Coin*, ou d'associations comme *Le Cercle du Coin* dans plusieurs villes de France et plusieurs médias francophones continuent de fédérer et d'élargir cette communauté Bitcoin. Celle-ci constitue un atout majeur pour le développement de la Blockchain en France.

L'ÉCOSYSTÈME BLOCKCHAIN



Crowdfunding > Secteur
JetCoin > Entreprise

Cette liste d'entreprises n'est évidemment pas exhaustive. Elle reflète la diversité des solutions et applications de l'écosystème Blockchain.

L'ÉCOSYSTÈME BLOCKCHAIN

Les blockchains

Les différentes blockchains sont les « livres de comptes » qui enregistrent les utilisateurs et les transactions d'un service donné : par exemple, les détails des transactions de la monnaie Bitcoin sont enregistrés sur la blockchain Bitcoin [voir focus page 26].
Une blockchain peut posséder des spécificités techniques qui favorisent des types d'applications particulières ; c'est le cas de la Blockchain MUSE pour la rémunération des droits d'auteurs [voir fiche Culture page 39].

La couche technologique

Ces entreprises agissent comme l'interface technique entre une blockchain et les services qu'elles proposent. Elles traitent les informations contenues dans une blockchain pour les rendre actionnables par des services tiers.
Cependant, la croissance du modèle de blockchain privée [voir focus page 15] tend à brouiller la séparation entre une blockchain et cette couche technologique, à l'instar d'entreprises comme Ripple ou Linq.

« Blockchain-as-a-Service »

Il s'agit d'applications utilisées directement par l'utilisateur final : leur fonctionnement technique est transparent.

Les utilisateurs

Les structures étatiques, acteurs privés, associations et particuliers qui bénéficient de services Blockchain.

Smart-contracts : ENJEUX & PERSPECTIVES

Jean-Baptiste Dézard
Fondateur de Deal-ex Machina

Au sein de la technologie Blockchain, quel est le rôle des smart-contracts ? Comment pourraient-ils intervenir dans notre vie quotidienne ?

JBD : Le rôle des smart-contracts est d'effectuer des opérations en fonction d'instructions totalement auditables par les parties prenantes de ces contrats, en assurant une exécution non biaisée, puisque tous les contributeurs du réseau vérifient que personne n'a pu modifier le programme et la machine (virtuelle) qui l'exécute. Ces contrats sont éventuellement déclenchés à partir de la validation de conditions (les oracles), qui peuvent être d'autres programmes informatiques, d'autres contrats. Autant dire que le champ d'application est très, très vaste.

> *« L'un des avantages périphériques de cette technologie est qu'elle rend l'audit des contrats et transactions trivial. »*

Le fait d'exécuter ces instructions dans la blockchain apporte une sécurité sans précédent. En particulier, pour tout crédit ou prélèvement différé, les conditions, le montant et la date des opérations sont certaines. C'est un élément capital pour accélérer et fiabiliser les échanges, à coût minimal, dans le monde entier. L'un des avantages périphériques de cette technologie est qu'elle rend l'audit des contrats et transactions trivial.

Aujourd'hui, dans notre vie quotidienne, nous gérons des contrats dès qu'il s'agit de réserver, commander, louer, payer en plusieurs fois, etc. Ce sont les applications évidentes des smart-contracts. Mais nous parions aussi, nous souscri-

vons à des cagnottes, dont les conditions d'utilisation des fonds doivent être connues, vérifiées. Nous utilisons des tickets, des bons, des chèques qui sont autant d'éléments de valeurs dont l'émission et l'utilisation doivent être connus, vérifiés, régulés.

Quand vous vendez quelque chose sur une place de marché, et c'est une habitude de plus en plus fréquente, un tiers collecte de l'argent pour vous et doit vous le restituer. Quand vous laissez une caution, un compte de cantonnement doit être créé pour protéger cet argent dont le versement est suspendu à l'exécution de conditions. Aujourd'hui, ce genre d'opération est relativement manuel et nécessite un fort contrôle interne, comme le rappelle régulièrement le régulateur.

On voit bien que les smart-contracts vont, à notre insu ou non, s'inviter dans notre vie quotidienne. Mais allons plus loin. Comment stockons-nous nos droits, en face de nos contributions et cotisations ? Pouvons-nous vérifier la logique de collecte, la logique d'allocation des fonds collectés, et la décollecte ? **Tous ces produits financiers ou de prévoyance qui utilisent des « unités de comptes » sont des objets qu'il faut traiter avec des smart-contracts,** pour lever le doute et renforcer la confiance que nous accordons à ceux qui les opèrent. Par exemple, la manière dont les plus-values des assurances vie en euros sont en ce moment transférées dans des fonds ***euro croissance*** mériterait un smart-contract, et un consensus « proof of stake » [voir lexique page 52] par l'ensemble des souscripteurs. Si une part suffisante des souscripteurs votait « non », cela donnerait lieu à un « fork » , soit une scission parmi les souscripteurs.
Nous voyons que les assurances, les réservations et locations de biens et de services, les copropriétés, les produits et charges mutualisés, les opérations financières, les transferts de propriété, les « démembrements » de propriété, la constitution de sociétés, les registres civils, les greffes, la protection de la propriété intellectuelle et culturelle et des ayant droits, sont des champs d'opportunités, à l'échelle mondiale.

Comment les entreprises pourraient bénéficier des smart-contracts ? Comment les mettre en place ?

JBD: De mon point de vue, il y a des aspects assez évidents. En premier lieu, **revoir l'ensemble de sa relation client ou de sa relation fournisseur, c'est-à-dire les fameux processus « Order to Cash » et « Purchase to Pay » à la lumière de cette technologie.** Il faut aussi revoir la gestion de trésorerie, en particulier si l'on a des transferts fréquents à l'international, avec des montants faibles et des frais importants. A cette occasion, évaluer comment mettre en place une vraie gestion de délégation et des systèmes de multi-signatures. Enfin, cette technologie permet de redéfinir comment faire un « onboarding » express de clients ou de fournisseurs.

> *« L'erreur serait de croire que la Blockchain est une FinTech, c'est une technologie qui va bien au-delà du secteur financier, c'est une machine à confiance qui va se diffuser dans tous les domaines de l'économie. »*

···>

Un autre aspect mérite une réflexion : la rémunération. Comment gérer ses salariés et ses dirigeants, le contrat de travail, les contributions, les heures supplémentaires, les congés, les objectifs commerciaux, les bonus et commissions ?

Enfin, il faut commencer à **intégrer les smart-contracts à la comptabilité automatique.** C'est un moyen radical de réaliser un « Fast Close ».

Si l'on veut vraiment prendre de l'avance, on peut aussi imaginer une gouvernance rendant l'entreprise transparente pour ses actionnaires, avec les droits de vote, les résolutions, les élections de ses représentants via des smart-contracts. On approche là le domaine de la science-fiction mais nous pouvons être certains que des entreprises seront créées et administrées via une blockchain.

Et je ne parle pas ici de toutes les implications concernant la sphère publique et l'exercice d'une démocratie plus directe, plus transparente. Je n'aborde pas non plus tous les leviers de simplification de l'administration.

Quelles sont les principaux défis pour la généralisation des smart-contracts ? Sur quel timing ?

JBD : Le premier secteur à adopter la Blockchain est sans conteste la finance, en particulier pour toutes les opérations de versements (remittance), de clearing & settlement (compensation). On voit d'ores et déjà des banques « bypasser » les systèmes de compensation interbancaires avec des technologies de ce type.

L'erreur serait de croire que la Blockchain est une FinTech, c'est une technologie qui va bien au-delà du secteur financier, c'est une machine à confiance qui va se diffuser dans tous les domaines de l'économie.

L'émergence des blockchains et des smart contracts, c'est un peu pareil que l'internet dans les années 90. Même niveau de déni, de « vous n'y pensez pas », de défiance parce que c'est la porte ouverte à tous les trafics, de débats picrocholins concernant les tailles de blocs, les protocoles de consensus etc. Pendant ce temps, les GAFA ont conquis la planète et ont construit leurs jardins murés, capturant les données pour capter des rentes.

> *« Certains resteront dans le déni, d'autres innoveront à un niveau inimaginable pour inventer le réseau mondial de transfert de valeur. »*

On voit ce que l'internet a fait au commerce, à la pub, aux médias, au voyage, etc.
Pour les smart-contracts, ce sont toutes les professions fiduciaires qui vont devoir se réinventer : auditeurs, comptables, notaires, huissiers, avocats.

Certains resteront dans le déni, d'autres innoveront à un niveau inimaginable pour inventer le réseau mondial de transfert de valeur.

Un Facebook assemblant les contrats et les opérant avec de l'intelligence artificielle, et un système international, une CyberLaw mondiale transposant en numérique ce qui existe aujourd'hui (Lettre de crédit, Connaissement, Bill of Lading, procédures d'arbitrage …). Les formats sont prêts, issus des Nations Unies, il ne manquait que des registres partagés infalsifiables pour per-

mettre une simplification radicale des processus d'échange.

Cela pose immanquablement la question de la souveraineté dans l'exercice du droit. Les tendances lourdes de réglementations extra territoriales vont pouvoir se matérialiser plus rapidement : c'est une opportunité et une menace pour les États.

Cette vision doit nourrir les dirigeants de nos institutions, qui doivent évaluer l'ensemble des services de l'État (police, justice, fiscalité et contributions, prestations sociales, droit du travail) et les repenser à la lumière de cette innovation remarquable, mondiale, sans frontières.

Exemple : prélèvement à la source, via un smart-contract, de la TVA. Incitation fiscale pour tous les échanges inter-entreprises à base de smart-contracts opérés dans une blockchain souveraine, mais dont les « miners » seraient tous les participants enregistrés au greffe (lui-même disponible sous forme de smart-contract).

> *« Il est temps de s'y mettre, au lieu d'avoir peur du Bitcoin. »*

Il est temps de s'y mettre, au lieu d'avoir peur du Bitcoin.

Quelles seront les premiers secteurs concernés ?

Tous les secteurs qui échangent dans un contexte de confiance minimale. C'est vaste, la question est : quels sont les acteurs qui vont agir et emporter la mise. Pas ceux qui en auraient l'usage le plus direct : ils sont prisonniers de leurs rentes et de leurs modèles. Leurs dirigeants n'ont pas la moindre idée de ce qui les guettent, les administrateurs des entreprises qui peuvent disparaître n'en sont pas conscients. On l'a déjà vu avec la transformation numérique, l'économie du partage, la vente sur internet, il n'y a aucune raison que cette fois-ci cela soit différent.

La Blockchain va créer des méga-licornes, les GAFA ont intégré ces technologies et vont accélérer leur emprise sur l'économie mondiale. Les conséquences de cette vague d'innovation vont casser les modèles d'assurances, les modèles bancaires, tous les intermédiaires du commerce. On peut assister, et ce n'est pas certain, à l'émergence de structures coopératives à l'échelle mondiale ou chaque participant est simultanément actionnaire, client, fournisseur, contributeur.
Les guildes de marchands n'auront plus besoin de banquiers, ou bien les banquiers auront mué pour intégrer les marchands dans leur gouvernance (mutualité).

Le secteur du droit doit évoluer. **Il faudra de nouveaux moyens de traiter les litiges, d'arbitrer les conflits, de réconcilier les parties « hard »** (« machine readable » : exécutables, intangibles) **d'un contrat avec les parties « soft »** (consentements, négociations, décisions humaines). L'économie ne se résumera pas à des échanges programmés dans des blockchains, heureusement.

Jean-Baptiste Dézard
Fondateur de Deal-ex Machina

PARTIE II – II

Onze exemples sectoriels

Les onze fiches suivantes donnent à voir comment la Blockchain peut bouleverser l'ensemble des secteurs de l'économie. Chacune d'elle s'appuie sur une réalisation concrète, de la startup au projet académique.

01 _ Puissance Publique :
Etablir la confiance dans les données administratives

02 _ Énergie :
Faciliter l'achat et la vente d'énergie autoproduite

03 _ Internet des Objets :
Créer de nouveaux business-models

04 _ Culture :
Mieux rémunérer les droits d'auteurs à l'ère numérique

05 _ Notariat :
Fluidifier la création « d'actes authentiques »

06 _ Covoiturage :
Réduire le coût d'un trajet

07 _ Assurance :
Faciliter la création de mutuelles à taille humaine

08 _ Vie privée :
Redonner à l'utilisateur le pouvoir sur ses données

09 _ Logistique :
Garantir la traçabilité des produits alimentaires

10 _ Citoyenneté :
Faciliter l'exercice du droit de vote

11 _ Crowd-Equity :
Transformer les supporters en actionnaires

FICHE SECTORIELLE

01

Puissance publique

Etablir la confiance dans les données administratives

LE CONTEXTE

Les bases de données administratives sont indispensables à l'activité économique

L'absence de bases de données administratives fiables génère de la défiance, au risque de peser sur les opportunités de croissance. C'est le cas dans certains pays en développement : l'absence de cadastre fiable renforce **l'incapacité de l'État à assurer le respect de la propriété**, ce qui handicape les échanges. Cette difficulté à mettre en place une base de données officielle a deux causes majeures : le niveau d'investissement nécessaire pour développer une technologie ad-hoc et la corruption endémique des agents publics qui souhaitent préserver leur pouvoir sur ce cadastre.

L'ENJEU

Les cadastres peuvent être manipulés à dessein

Au Honduras, **60% du territoire n'est pas répertorié par l'État,** suite à la redistribution dans les années 1990 des terres paysannes aux élites urbaines. Plus encore, le système actuel n'est pas protégé contre les interventions frauduleuses, comme l'explique un responsable du gouvernement, « la base de données nationale est simplement piratée. Des membres de l'administration peuvent la pénétrer pour s'offrir une propriété en bord de mer ».

L'INNOVATION BLOCHAIN

Les données deviennent inviolables

Le Honduras fait appel aux entreprises Factom et Epigraph pour développer un registre de propriété sur une blockchain. Le passage par une blockchain garantit **l'absence de « backdoors »** qui permettrait « d'institutionnaliser » de futures atteintes frauduleuses au cadastre. Contrairement aux bases de données « traditionnelles » dont les informations sont stockées dans un serveur unique, les informations que contient une blockchain sont distribuées, et dès lors infalsifiables [cf. propriété 2 page 12].
Le choix entre rejoindre une blockchain existante et construire une blockchain gouvernementale n'est pas encore connu. Le démarrage du projet est prévu pour la fin 2016.

À VOIR AUSSI

Une petite dizaine de pays où la structure étatique est faible, de l'Ukraine au Ghana, ont annoncé des investissements dans des infrastructures Blockchain pour sécuriser leur registre de propriété.

Titre de propriété hondurien

FICHE SECTORIELLE

02

Énergie

Faciliter l'achat et la vente d'énergie autoproduite

LE CONTEXTE

La production d'énergie n'est plus le monopole des entreprises

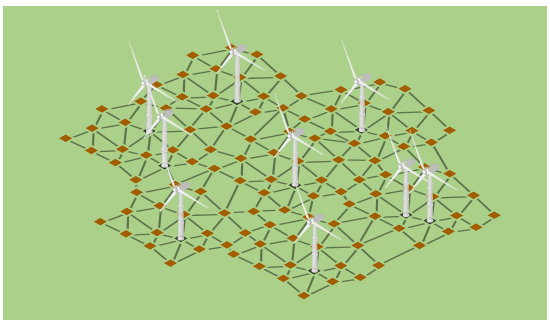
L'accroissement de l'autoproduction d'énergie par les particuliers (panneaux solaires et énergie éolienne) et les projets de Smart-Cities dessinent des nouveaux circuits décentralisés dans l'achat et la vente d'électricité.

L'ENJEU

Cette autoproduction d'énergie cherche son *business-model*

Aujourd'hui, les particuliers producteurs d'énergie peuvent revendre leur surplus (l'énergie produite par leur panneau solaire ou leur éolienne mais qui n'est pas consommée) à EDF qui l'intègrera au flux d'énergie disponible sur le marché. Le prix d'achat par EDF est défini chaque trimestre par arrêté et varie en fonction du type d'installation, de la quantité produite et de la période de l'année.

Comme le note l'Agence Internationale de l'Énergie, **le développement de l'autoproduction repose sur « l'équilibre économique du dispositif »** entre le producteur et le consommateur. Or, la Blockchain apporte le lit technologique pour faciliter l'intégration économique de ces nouveaux usages.



Vers une énergie P2P ?

L'INNOVATION BLOCHAIN

Un marché désintermédié d'achat et vente d'électricité

Lancé en janvier 2014, la fondation **SolarCoin** préfigure ce que serait un marché d'achat/vente d'énergie inscrit sur une blockchain. Présent dans 17 pays, SolarCoin est une monnaie numérique similaire à des Point-Miles pour les passagers aériens : les auto-producteurs reçoivent des SolarCoin (§SLR) en fonction de l'électricité que l'installation photovoltaïque génère. En l'état, 1 SolarCoin récompense la production d'un MWh d'énergie verte et peut être échangé contre des Bitcoins (ou autre crypto-monnaie) sur une place de marché. Contrairement à un modèle centralisé, la valeur de rachat d'un SolarCoin est définie par le marché. Dans cette phase d'expérimentation, le volume du marché reste faible : moins de 1 000 euros de transaction par jour.

« SOLARCOIN.ORG »

À terme, **SolarCoin pourrait être utilisé pour acheter de l'électricité entre particuliers sans intermédiaire.** Prenons un exemple : pendant une période donnée, la météo empêche un producteur A de faire fonctionner son installation photovoltaïque, il utilise alors ses SolarCoins pour acheter l'énergie alors nécessaire au producteur B, qui bénéficie d'un meilleur ensoleillement. **SolarCoin est présent dans 17 pays.**

Au-delà de SolarCoin, la Blockchain change le mécanisme de fixation du prix de l'énergie autoproduite : celui-ci n'est plus fixé par une agence de tutelle mais par le marché lui-même. À terme, cela peut pousser les producteurs d'électricité à s'aligner sur ce nouveau prix de marché.

FICHE SECTORIELLE

03

Internet des Objets

Créer de nouveaux business-models

LE CONTEXTE

Les objets connectés, du produit au service

La **démocratisation de l'Internet des objets** est en marche : 20 milliards d'objets connectés devraient être en service d'ici à 2020. Une des ambitions des acteurs de cet écosystème est la création de nouveaux business-models qui capitalisent sur les données générées par ces objets connectés, en passant d'une **logique de produit à une logique de service**.

L'ENJEU

Faciliter la revente de données

Une fois vendu, un objet connecté ne crée actuellement plus de valeur marchande, alors que son utilisation vient de commencer : comment monétiser les données qu'il produit ? C'est la démarche **« Sensing-as-a-service »** où les propriétaires d'objets connectés vendent les données des objets issus de leurs capteurs (station de qualité de l'air, outils de quantified-self ...). Des acteurs privés et publics (centres de recherches, collectivités locales, agences ministérielles) sont prêts à payer pour exploiter ces données d'un grand niveau de précision et de détail.
Cependant, **ce concept « Sensing-as-a-service » (S2AAS) n'a pas trouvé son équilibre** pour deux raisons : d'une part, le partage de valeur entre la plateforme et les utilisateurs et, d'autre part, des frais de structures (développement, maintenance de plateforme, frais bancaires...) potentiellement supérieurs à la valeur des données vendues.

L'INNOVATION BLOCKCHAIN

La crypto-monnaie pour partager ses données sans intermédiaire

La Blockchain est un accélérateur de cette approche qui introduit **les paiements désintermédiés via une crypto-monnaie**[1]. La startup **Tilepay** travaille sur un logiciel pour que les particuliers puissent partager les données issues de leurs objets connectés et être rémunérés en bitcoins. L'utilisateur maîtrise précisément chaque usage de ses données (catégories de données et organisations auxquelles il les vend). Son identité est protégée derrière un pseudonyme chiffré.

Capture d'écran de tilepay.org

À VOIR AUSSI

D'autres projets « Machine to Machine » exploitent le potentiel de la Blockchain comme architecture permettant à des objets connectés d'exécuter des smart-contracts et d'échanger des crypto-monnaies. L'entreprise **Filament** propose une solution logicielle et des transmetteurs (appelés Tap) pour connecter des objets entre eux. Cette infrastructure intégrée dans une blockchain a levé 5 millions de dollars dans 9 fonds différents durant l'été 2015.

[1] Cela a été théorisé en 2014 par 4 chercheurs de l'université de Zurich dans l'article « When Money Learns to Fly: Towards Sensing as a Service Applications Using Bitcoin »

FICHE SECTORIELLE

04

Culture

Mieux rémunérer les droits d'auteurs à l'ère numérique

LE CONTEXTE

La traçabilité de l'usage des œuvres numériques est la clef de la rémunération des ayants-droits

L'accès à la culture, notamment la musique, a radicalement changé par rapport à l'ère pré-numérique : 70% des français utilisent Internet au moins une fois par semaine pour accéder à du contenu musical ; en streaming sur des plateformes gratuites, comme Youtube, ou payantes, comme Spotify et Deezer, ou bien en téléchargeant des morceaux sur iTunes, par exemple. En France, ces quatre plateformes affichent 48,7 millions de visiteurs uniques par mois.

Malgré ce nouveau mode de consommation digitale continue, la rémunération des artistes continue de se faire par les acteurs traditionnels : majors et sociétés en noms collectifs.

L'ENJEU

La mise en place de cette traçabilité est limitée et dépendante d'une foule d'intermédiaires

À l'ère du vinyle, quelques milliers d'artistes se disputaient les *charts* alors qu'à l'ère numérique le catalogue est devenu virtuellement infini. Les intermédiaires sont dès lors confrontés à une mission infiniment plus complexe.

Dans le cas du streaming, la plateforme doit être capable de répartir les revenus de chaque écoute à chacun des auteurs, compositeurs et interprètes d'une œuvre. Ces revenus par écoute sont extrêmement faibles, (estimés sur Spotify à 0,0001 euro en flux gratuit et 0,002 et 0,004 euro en flux payant). Il en découle une traçabilité particulièrement complexe à mettre en place et nécessitant de très lourds investissements (pas de procédure standard). C'est ce que souligne Benji Rogers, fondateur de PledgeMusic[2] : *« Les morceaux peuvent avoir plusieurs auteurs, interprètes, éditeurs, plusieurs licences et tout cela différemment d'un pays à un autre. Une simple chanson peut demander plusieurs paiements à une multitude de personnes, à différents moments, dans différents pays et dans différentes organisations. Pour ne rien faciliter, il n'existe pas de base de données mondiale pour tracer la propriété »*. Le projet de **Global Repertoire Database**, initié en 2010 par la commissaire européenne chargée de la société numérique Neelie Kroes, s'est soldé par un échec suite au retrait de certaines majors partenaires en 2014, craignant notamment une baisse de leurs revenus due à une meilleure traçabilité.

L'INNOVATION BLOCKCHAIN

Des outils pour un traçage et une rémunération automatique des écoutes et des téléchargements

UJOMUSIC.COM

La Blockchain apporte des moyens pour créer des outils capables d'assurer la traçabilité d'une œuvre et mettre en place des paiements automatisés et désintermédiés, via une cryptomon-

[2] PledgeMusic fait partie des 10 entreprises les plus innovantes de l'industrie musicale dans le classement Fast Company 2015.

FICHE SECTORIELLE

04

Culture (suite)

Mieux rémunérer les droits d'auteurs à l'ère numérique

Capture d'écran de ujomusic.com

naie qui rend possible des échanges directs entre fans et artiste.

Le test-case lancé par la startup UjoMusic, construit au sein de la Blockchain Ethereum [voir focus page 20], en partenariat avec la chanteuse *Imogen Heap* et son morceau *Tiny Human*, donne à voir le potentiel de la Blockchain pour assurer la traçabilité et rémunérer une œuvre.

L'utilisateur peut acheter le morceau pour l'équivalent de 0,6$ en Ether (la monnaie de la blockchain Ethereum). Ce montant est réparti automatiquement à l'ensemble des contributeurs, sans passer par une plateforme tierce. La répartition des droits d'auteurs et les conditions de réutilisation (streaming, fichiers des pistes séparés, plusieurs licences) du morceau sont accessibles en un clic. Contrairement aux plateformes actuelles qui doivent passer par l'ensemble des intermédiaires et le système bancaire, le coût de distribution de droits d'auteurs sur UjoMusic est nul. La rentabilité de la distribution de montants même faibles devient possible.

Ce prototype ne résout pas le chantier de la constitution d'une base de données mondiale des droits d'auteurs mais il fournit les outils pour le faire.

À VOIR AUSSI

MUSEBLOCKCHAIN.COM

La blockchain **MUSE** est une blockchain taillée pour être la base de données mondiale de la musique à l'ère numérique. Décentralisée, son fonctionnement diffère légèrement de la blockchain Bitcoin (notamment avec l'utilisation de Smart-Coins qui ne sont pas sensibles à la volatilité du cours). Cela facilite l'enregistrement de morceaux et la rémunération des artistes avec des smart-contracts.

Dans sa version Bêta, la startup **PeerTracks.com** prévoit le développement de *Notes*, sortes de « pass VIP » (réductions sur les sorties de l'artiste, cadeaux privilégiés, rencontres, ...) que les fans pourront acheter. Ces *Notes* seront échangeables et leur valeur changera en fonction de la popularité de l'artiste.

FICHE SECTORIELLE

05

Notariat

Fluidifier dans la création « d'actes authentiques »

LE CONTEXTE

L'immobilier est le cœur de l'industrie notariale française

Les 10 000 notaires français établissent chaque année plus de 4 millions « d'actes authentiques » qui ont valeur de preuves incontestables (appelés aussi actes notariés, définis par l'article 1337 du code civil). Les actes authentiques qui régissent le transfert de propriétés représentent 49% du chiffre d'affaires évalué à 6,2 milliards d'euros. Depuis 2007, ils peuvent être dressés sur support électronique .

L'ENJEU

Un tiers de confiance coûteux pour le client final

En France, les notaires possèdent le monopole de la certification des actes authentiques relatifs à la propriété. Ils sont le tiers de confiance incontournable des transactions immobilières. En plus d'un travail de conseil juridique, ils authentifient un acte de transaction en garantissant 4 caractéristiques : une « date certaine », une « force probante » (i.e. les faits constatés sont incontestables), une « conservation garantie » (durant 75 ans avant archivage public) et « une force exécutoire » (i.e. l'acte a valeur de jugement). Aujourd'hui, le coût de ce travail de certification est porté par le client final.

L'INNOVATION BLOCKCHAIN

L'inviolabilité des informations inscrites dans un bloc

Une dizaine de startups proposent l'enregistrement de documents via la technologie Blockchain, généralement la blockchain Bitcoin, à l'instar de Bitproof.io, CryptoPublicNotary.com, Stampd.io ou Stampery. En quelque clics et contre l'équivalent de quelques centimes d'euros, nécéssaires à la rémunération des miners, [cf. propriété 3 page 14], l'utilisateur peut produire une preuve de propriété.

La Blockchain valide 3 des 4 caractéristiques d'un acte authentique, la quatrième restant dépendante du législateur :

1. La « date certaine » et la « force probante » sont garanties par le fait que le contenu un bloc (les informations qu'il recèle et ses métadonnées) ne peut pas être modifié *a posteriori* [cf. propriété 1 de la blockchain page 12]. Le code de chaque nouveau bloc est construit sur celui du bloc qui le précède dans la chaine de blocs de telle sorte qu'il soit impossible de manipuler l'information sans modifier l'ensemble d'une blockchain, ce qui est techniquement impossible.

2. La « conservation garantie » est permise parce qu'une copie cryptée du document est partagée par une foule d'utilisateurs : plusieurs milliers pour une blockchain publique comme Bitcoin ou une dizaine dans une blockchain privée. Cette copie n'est plus sécurisée dans les armoires ou serveurs d'un notaire mais dans une multitude de disques durs.

FICHE SECTORIELLE

05

Notariat (suite)

Fluidifier dans la création « d'actes authentiques »

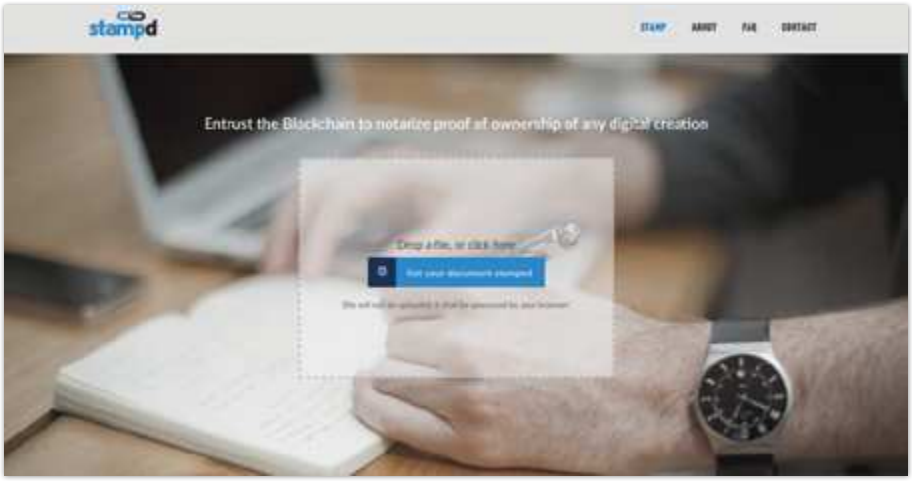
3. La « force exécutoire », en revanche, dépend d'une décision qui donnerait une valeur juridique à l'enregistrement d'un document sur une blockchain. En France, cela est du ressort du Conseil d'État. En l'état, aucune startup française ne propose ce service Blockchain.

En outre, la confidentialité des documents est assurée par la chiffrement du document original, dont seul le propriétaire détient la clef de décryptage.

En l'état, ces startups ne couvrent pas la maitrise juridique et le travail de conseil indispensables que fournissent les notaires. En revanche, elles montrent que la Blockchain a des propriétés techniques susceptibles de disrupter le monopole séculaire du notariat sur la certification de documents, quelque soit son cadre juridique.

Au-delà de l'immobilier, la certification via la Blockchain est transposable dans l'activité de constat des huissiers de justice, les diplômes universitaires (exemple : Holberton Uni à San Francisco) ou l'état civil.

Capture d'écran de stampd.io



FICHE SECTORIELLE

06

Covoiturage

Réduire le coût d'un trajet

LE CONTEXTE

Le covoiturage s'est généralisé

Le covoiturage n'est plus une lubie d'auto-stoppeur attardé, loin s'en faut ! 1 français sur 5 a déjà effectué un trajet partagé et l'âge moyen du passager recule. Portée par le succès de BlaBlaCar (95% du marché français et présent dans 20 pays), la France est l'un des leaders mondiaux de cette nouvelle forme de mobilité. Elle est aussi le signe de la montée en puissance de l'usage comme alternative à la propriété.

L'ENJEU

La rémunération des plateformes représente un coût pour l'utilisateur

La mission des plateformes de covoiturage (Blablacar, donc ou Ridester aux USA ou encore RoadSharing en Europe) est de mettre en relation des voyageurs avec des conducteurs qui disposent de sièges inoccupés. Afin de financer cette activité de « place de marché », ces entreprises prélèvent des frais sur chaque transaction entre deux utilisateurs : chez BlaBlaCar, un montant fixe de 0,89€ HT et une part variable de 9,90% HT. Cette facturation des transactions est la première source de revenus pour les entreprises de « l'économie collaborative » (chez AirBnB, par exemple, les frais varient de 6 à 12% pour le locataire et 3% pour l'hôte). Cette facturation a vocation à couvrir les frais d'infrastructure et financer le rôle d'intermédiaire de la plateforme (mise en relation et confiance…).

L'INNOVATION BLOCKCHAIN

La Blockchain permet des échanges directs entre passagers et conducteurs

L'autonomie de la Blockchain [voir propriété 3 page 14] change la donne dans la mesure où l'infrastructure (espace de stockage et puissance de calculs) est fournie par les utilisateurs eux-mêmes, notamment au travers du minage [voir lexique page 52]. C'est le sens du service de covoiturage proposée par la startup israélienne *La'Zooz*. Grâce à sa communauté de mineurs [voir lexique page 52], aucun frais de fonctionnement n'est nécessaire et le prix payé par l'utilisateur est uniquement en fonction de la distance parcourue.

Pendant qu'ils conduisent, les conducteurs sont rémunérés en tokens [voir lexique page 52] appelés Zooz. De leur côté, les passagers peuvent gagner ces tokens en allouant une partie de leur processeur ou bien en agissant pour faire gagner de nouveaux utilisateurs à la communauté[4]. Pour régler leurs courses, ils utilisent ces tokens.

Afin de se prévenir d'un détournement de la valeur des utilisateurs vers les actionnaires, La'Zooz est une organisation à but non-lucratif. En outre, le code source est public.

Capture d'écran de La'Zooz

[4] Les mécanismes d'acquisition de tokens évolueront au fur et à mesure de la croissance de la communauté : http://lazooz.org/whitepaper.html#page_3

FICHE SECTORIELLE

07

Assurance

Faciliter la création de mutuelles à taille humaine

LE CONTEXTE

Le décalage entre la croissance du marché et l'insatisfaction des utilisateurs

Pilier de la solidarité entre « citoyens », l'assurance permet aux victimes de sinistres de recevoir une indemnisation couvrant tout ou partie des dommages subis. Depuis le XVIIè siècle, l'assurance a connu un développement et une complexification considérable pour atteindre un chiffre d'affaires de près de 1200 milliards d'euros en Europe en 2014 (Source FFSA). Malgré sa taille et sa « maturité », ce secteur évalue cependant les fraudes à près de 2,5 milliards en France en 2012 (environ 5% des primes collectées) et l'insatisfaction chronique des assurés est souvent pointée du doigt par le régulateur.

L'ENJEU

Transformer les investissements Big Data en valeur perçue pour l'utilisateur

La recherche en statistiques et en mathématiques a permis, année après année, d'affiner des modèles d'analyse de risque qui anticipent de mieux en mieux la fréquence et la portée des sinistres. L'avènement du numérique et les récentes évolutions réglementaires ont assoupli et simplifié l'accès des assurés à des produits toujours plus ciblés. Mais force est de constater que ces évolutions ne garantissent pas un accès généralisé au meilleur prix pour tous les citoyens. Quand les profits des sociétés d'assurance se développent, les « exclus de l'assurance » et l'incompréhension du public face à des produits obligatoires et méconnus restent un reproche récurrent fait aux acteurs de cette industrie, assureurs comme mutuelles.

L'INNOVATION BLOCKCHAIN

Des produits d'assurance désintermédiés

Ces derniers mois, plusieurs publications de recherche et rencontres brossent les contours envisageables d'un futur modèle d'assurance – ou mutuelle – s'appuyant sur la Blockchain qui redéfinirait toutes les composantes de l'assurance.
Cette nouvelle approche permettrait en premier lieu l'identification de nouveaux modèles de risk management, au-delà de celui de la mutualisation du risque. Il faciliterait ensuite l'optimisation de la lutte contre la fraude, que ce soit dans l'identification des assurés, ou pour les déclarations de sinistres.
Enfin, ces travaux dépassent la seule question du « produit » assurance, pour se pencher sur un rôle nouveau des sociétaires ou assurés, organisés en DAO qui participeraient activement à la gouvernance de leur mutuelle d'un nouveau genre, ou encore à l'évaluation collective des sinistres et des remboursements.
L'automatisation inhérente à la Blockchain et l'utilisation des smart-contacts optimiseraient l'efficacité et la rapidité de traitement.En parallèle, la désintermédiation limiterait aussi les coûts de façon considérable. Des assurances moins chères et plus efficaces pourraient ainsi voir le jour dans un avenir proche.
Le sujet de la responsabilité reste cependant à traiter, une DAO n'ayant pas représentation légale [cf. Les travaux de Primavera de Filippi, page 20].

« La Blockchain a le potentiel d'améliorer la façon dont les assureurs enregistrent le risque, d'accélérer la vitesse de déploiement et de rendre les procédures plus transparentes. »

Shirine Khoury-Haq,
directrice des opérations, Lloyd's

FICHE SECTORIELLE

08

Vie privée

Redonner à l'utilisateur le pouvoir sur ses données

LE CONTEXTE

L'exploitation des données personnelles aussi vieille que l'Internet

Le web est nativement une organisation décentralisée : majoritairement produits par la multitude, les contenus sont accessibles à tous par défaut. Pourtant, la volonté de « re-centraliser » l'accès aux contenus est presque aussi vieille que le web lui-même. Compuserve, puis AOL, ou MSN ont été les précurseurs de cette approche, avant que Facebook, Apple ou Google ne proposent de nouveaux modèles appelant toujours le pilotage centralisé (ou propriétaire) de l'accès aux données, aux utilisateurs, aux contenus, aux services.

Alors que ces acteurs centraux captent la majorité de la valeur économique contre l'usage de services innovants devenus (presque) indispensables, **de plus en plus d'organisations ou de citoyens s'interrogent sur l'acceptabilité du modèle service (gratuit) contre données personnelles** et s'inquiètent de l'exploitation parfois opaque qui y est associée (selon la dernière étude PewInternet, 90% des internautes américains considèrent comme important de contrôler leurs informations personnelles).

Image extraite de l'article "The End of Internet Advertising as We've Known It", par Doc Searls, décembre 2015, MIT Techonlogy Review

L'ENJEU

Le mécontentement des utilisateurs en passe de changer la donne

Google, Facebook, Twitter, … le modèle est simple ! Accès à un service innovant et vite indispensable contre cession de la propriété de ses données. Une fois les conditions générales d'utilisation (CGU) signées, la plateforme est alors libre de commercialiser les données personnelles de l'utilisateur comme bon lui semble et à qui elle le souhaite. En associant, en général, cette commercialisation à un certain anonymat : ce sont des profils qui sont proposés aux annonceurs, et non une identité.

Mais plus le temps passe et moins l'utilisateur perçoit cet anonymat supposé. Il laisse la place au sentiment d'être traqué dans ses activités les plus intimes, activités qu'on lui rappelle au gré de sa navigation. Sans qu'il ne se sente capable de maitriser ce partage de données, ou d'en tirer lui-même profit. Les récentes plaintes répétées d'internautes désespérés de voir leurs projets secrets de cadeaux de Noël soudain partagés avec tous les membres de la famille grâce à la « magie » du « retargetting » en sont un exemple concret.

Le vol massif de données personnelles d'utilisateurs de services majeurs du web (Ashley Madison, Sony, …) vient de plus renforcer l'inquiétude de voir sa vie (très) privée vendue malgré soi au plus offrant.

FICHE SECTORIELLE

08

Vie privée (suite)

Redonner à l'utilisateur le pouvoir sur ses données

L'INNOVATION BLOCKCHAIN

Héberger les données personnelles sur une blockchain

Alors que de plus en plus d'organisations et de « startups » travaillent à mettre en place des outils et solutions visant à « rendre les clefs » aux utilisateurs dans la gestion de leur vie privée sur Internet, celles-ci peinent à s'imposer.
Le projet Enigma du MIT (http://enigma.media.mit.edu) décrit une possible solution en proposant d'utiliser la sécurité du cryptage de la Blockchain pour maitriser l'accès aux données personnelles. Ces dernières étant « hachées » (découpées) puis stockées sur plusieurs nœuds d'un réseau parallèle (le réseau Enigma), largement moins distribué qu'une blockchain, afin de résoudre les enjeux de volume de données trop importants. Sans le couple clef privée / clef publique, pas d'accès aux données.
Chaque utilisateur maitrise dès lors de façon certaine ses données personnelles. Le partage d'une clef publique pouvant toutefois donner un accès maîtrisé à certaines données pour des tiers.

Cette initiative (annoncée en prochaine Beta), est un exemple de travaux déjà avancés.
U, à l'origine de ce livre blanc, travaille en parallèle à d'autres options de gestion de la vie privée s'appuyant sur la Blockchain.

ENIGMA DU MIT

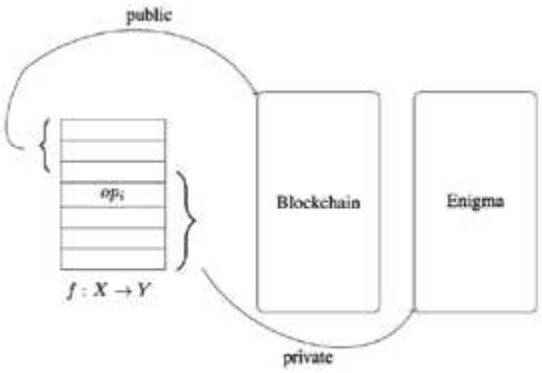


Figure 1: Code execution model.

Schéma du fonctionnement de Enigma

FICHE SECTORIELLE

09

Logistique

Garantir la traçabilité des produits alimentaires

LE CONTEXTE

La confiance dans la chaine agro-alimentaire repose sur la traçabilité des produits

La consommation responsable n'est plus une habitude de niche. En 2014, 55% des français déclarent avoir payé au moins une fois plus cher pour acheter « responsable » tandis que la pratique est régulière pour 39% de la population. Dans ce contexte, la traçabilité est primordiale : l'origine et les modalités de production de chaque produit doivent être accessibles pour que le consommateur puisse effectuer son choix d'achat.

Le texte européen « *Accounting Directive* » suit cette évolution des usages. Il imposera plus de transparence sur l'impact environnemental de chaque produit et service ainsi que sur les conditions de travail des salariés (transposition en droit français prévue pour l'année 2016).

L'ENJEU

Les garde-fous juridiques ne suffisent pas

Les pays européens se sont d'ores et déjà dotés de solides procédures pour tracer les biens de consommation, notamment après l'éruption de l'affaire de la vache folle en 1996. Cela étant, quelque soit le cadre juridique, la traçabilité repose in fine sur des agents humains qui sont faillibles et corruptibles. Le scandale des lasagnes à la viande de cheval a souligné les limites du système actuel de traçabilité des biens alimentaires.

L'INNOVATION BLOCKCHAIN

La clef privée pour assurer la traçabilité à chaque étape de la vie du produit

La startup ThingChain met en action l'inviolabilité des informations inscrites dans une blockchain. À l'aide de QR-codes appelés PopCodes (Proof-Of-Provenance), ThingChain garantit le parcours et la transformation d'un bien tout au long de la chaine logistique.

THINGCHAIN.COM

Chaque produit est lié à un PopCode, un identifiant digital unique inscrit dans la blockchain Bitcoin et modifiable avec un jeu de clefs publique/privée **[voir lexique page 52]**. Celui-ci contient des informations scellées dans la blockchain : unité de mesure, quantité, provenance, date. Elles sont isolées (via une adresse publique unique) et sont alors infalsifiables [propriété 2 de la Blockchain page 12]. Pour pouvoir mettre à jour ces informations à chaque étape de la vie du produit (par exemple, de la grappe de raisins à la palette de bouteilles de vin), l'agent doit posséder la clef privée. Une fois les informations inscrites sur la blockchain, l'agent peut transférer la clef privée au prochain intermédiaire sur la ligne logistique.

FICHE SECTORIELLE

09

Logistique (suite)

Garantir la traçabilité des produits alimentaires

Pour contrer la fraude (rien n'empêche techniquement l'agent d'entrer de mauvaises informations), tous les acteurs en contact avec le PopCode peuvent ensuite être tracés grâce à l'API Thingchain. Dans un cas comme F** (viande roumaine, surgelée à Chypre, fournie par S** et transformée par F**), une traçabilité inscrite dans une blockchain aurait *a priori* facilité l'identification de l'intermédiaire fautif.

À VOIR AUSSI

PROVENANCE.ORG

Les anglais de Provenance.org proposent une mise en avant de chaque producteur inscrit sur la plateforme. Celui-ci dispose d'un profil qui détaille ses processus de fabrication et met en valeur l'authenticité de son produit, certifiée par des outils Blockchain.

Producteurs indépendants utilisant les outils Provenance

FICHE SECTORIELLE

10

Citoyenneté

Faciliter l'exercice du droit de vote

LE CONTEXTE

Le vote en ligne, un levier de consultation citoyenne

Le vote en ligne lève la quasi-totalité des contraintes du vote (déplacement, temps) pour le citoyen. Il simplifie évidemment le décompte des voix pour l'organisateur. Il est donc présenté comme un instrument essentiel du renouveau démocratique et diminue en outre le coût de l'élection (à titre d'exemple, les frais de mises sous plis de la présidentielle 2012 s'élèvent à 51 millions d'euros). Cependant, le bien-fondé politique du vote en ligne reste sujet à débat : est-il un accélérateur de l'engagement citoyen ou désacralise-t-il le vote au risque de le banaliser ? Ses partisans soutiennent qu'il permettrait de multiplier les consultations et donc, de se rapprocher les habitudes de « participation » de la génération Y - les likes et les RTs ne sont-ils pas un « vote » permanent ?

Aujourd'hui, le vote en ligne est pratiqué dans certaines organisations (partis politiques, fondations caritatives, projets open-source ...) et collectivités locales (plusieurs dizaines de municipalités au Canada, aux USA, en Suisse et dans les pays scandinaves). Cependant, seule l'Estonie , un des pays leaders de la transformation numérique de l'État, utilise le vote en ligne pour des élections à grande échelle (corps électoral de l'ordre du million de personnes).

L'ENJEU

Une procédure lourde et des garanties de sécurité imparfaites

En plus de la controverse sur sa pertinence politique, l'adoption du vote en ligne est freinée par la complexité de sa mise en place. En effet, sécuriser un vote en ligne impose le passage par un certificat à la mise en œuvre complexe (voire coûteuse), tant pour l'organisateur que pour l'utilisateur. En outre, aucune technologie n'a complètement éliminé le risque de fraude (manipulation) ce qui remet en cause l'incontestabilité du vote, pierre angulaire du processus démocratique.

BITCONGRESS.ORG

L'INNOVATION BLOCKCHAIN

Sécuriser et rendre accessible le vote en ligne

La technologie Blockchain revitalise l'idée d'un vote en ligne à grande échelle, simple à mettre en place et sécurisé. La double clef publique/privée garantit l'identité de l'électeur et résout la faille de l'identification en ligne tandis que l'inviolabilité des informations inscrites prévient toutes manipulations a posteriori.

FICHE SECTORIELLE

10

Citoyenneté (suite)

Faciliter l'exercice du droit de vote

La fondation **BitCongress** produit un outil de vote utilisable par tous et extensible à des millions de votants. Adossé à la blockchain Bitcoin, BitCongress est fort d'une centaine d'utilisations par de nombreuses organisations. Ce vote à moindre coût et absolument fiable est un vecteur de développement démocratique. **Il peut devenir le chaînon manquant dans la prise de décision collective, notamment au niveau local et dans le monde syndical.**

> *« I firmly believe that in the future, voting will be done from our smartphones and our votes will be stored securely on the Blockchain. »*
>
> **Adam Ernest,**
> CEO de FollowMyVote

À VOIR AUSSI

FOLLOWMYVOTE.COM & V-INITIATIVE.ORG

Ces deux projets utilisent également la Blockchain au service d'un vote à distance, sécurisé et anonyme. FollowMyVote sera notamment adopté par la mairie à Sacramento en 2016.
Par ailleurs, le parti Libéral Danois est le premier parti a avoir utilisé un outil Blockchain, construit en interne sur Ethereum, pour des élections internes, comme l'explique son porte-parole :
« the Blockchain removes the need for trust,(...) and it is open source and transparent ».

FICHE SECTORIELLE

11

Crowd-Equity

Transformer les supporters en actionnaires

LE CONTEXTE

La Crowd-Equity est une tendance forte du crowdfunding

Le financement participatif ou **crowdfunding se normalise en France** : 152 millions ont été collectés en 2014 (soit le double de l'année 2013) pour plus de 20 000 projets sur une cinquantaine de plateformes. Né dans le domaine artistique, le crowdfunding concerne désormais les initiatives culturelles ou solidaires (« don contre don » à l'instar de KissKissBankBank ou MyMajorCompany), l'innovation technologique et, plus récemment, le sport, à l'instar de Sponsorise.Me.

Autre tendance clef, la formule initiale du « don contre don » est complétée par l'émergence du **« CrowdEquity » où un entrepreneur échange des actions contre du financement venant d'une foule d'actionnaires.** Leader européen, l'entreprise britannique Crowdcube a récolté plus de 126 millions de livres de plus de 237000 investisseurs pour financer des projets de startups (technologie, retail, immobilier, santé, loisirs…). En France, le **« CrowdEquity »** est favorisé par des mécanismes de défiscalisation[5] et bénéficie du dynamisme de la plateforme dédiée Wiseed[6].

L'ENJEU

Transformer les investissements Big Data en valeur perçue pour l'utilisateur

Les initiatives culturelles et sportives restent pour le moment exclues de la « CrowdEquity », qui concerne presque exclusivement des projets technologiques ou de services. En effet, si cela est possible pour la propriété d'une entreprise, comment répartir des « actions » d'un artiste ou d'un sportif ? Et quel véhicule utiliser pour distribuer cette valeur ?

L'INNOVATION BLOCKCHAIN

La crypto-equity transforme les droits d'auteurs et d'images en actifs

La Blockchain introduit le concept de **crypto-equity : l'achat d'une partie des droits d'artistes ou de sportifs via une crypto-monnaie.** La propriété de ces droits s'incarne dans des tokens **[voir lexique p. 52]**. Le supporteur parie alors sur le succès futur de de l'artiste ou du sportif qu'il soutient, et non plus sur un projet de court-terme.

JETCOININSTITUTE.COM

Un sportif prometteur, comme le propose l'entreprise **JetCoin** par exemple, choisit de céder une partie de ses droits à des supporteurs, « JetCoin contract », qui les achètent via une crypto-monnaie dédiée, le JetCoin. Ces JetCoins peuvent être achetés via des dollars ou bien en promouvant des artistes sur les réseaux sociaux. Les fans propriétaires de JetCoin Contract reçoivent des dividendes si le sportif soutenu connaît le succès, alors que sur les plateformes traditionnelles dans l'univers de la culture ou du sport, les fans sont rémunérés en casquettes dédicacées. Lancé en Juin 2015, JetCoin est adossé à la blockchain NXT .

[5] 18% pour l'impôts sur le revenu et jusqu'à 50% pour les assujetis à l'ISF

[6] 40M€ levés et 94 projets financés

BIBLIOGRAPHIE DES 11 FICHES SECTORIELLES

01_ Puissance Publique

DEVEX, ***Bitcoin technology for land administration,*** 2015
https://www.devex.com/news/bitcoin-technology-for-land-administration-86362,

GOV.UK, ***Digital Currencies : response to the call for information,*** 2015
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

02_ Énergie

SELECTRA, ***Parts de marché des fournisseurs d'énergie en France,*** 2015
http://selectra.info/Parts-de-marche-des-fournisseurs-d-energie-en-France.html

EDF, ***Prix de revente de l'électricité et nouveau tarif,*** 2015
http://www.les-energies-renouvelables.eu/9702prix-de-revente-de-lelectricite-nouveau-tarif-edf.html

03_ Internet des Objets

IBM, ***Device Democracy,*** 2015
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=XB&infotype=PM&appname=GBSE_GB_TI_USEN&htmlfid=GBE03620USEN&attachment=GBE03620USEN.PDF

04_ Culture

ADAMI, ***Études***
https://www.adami.fr/defendre-les-droits-des-artistes/etudes-et-donnees.html

05_ Notariat

NOTAIRES ÎLE DE FRANCE, ***Qu'appelle-t-on un acte authentique ?***
http://www.notaires.paris-idf.fr/role-attribution-et-statut-du-notaire/quappelle-t-acte-authentique

06_ Covoiturage

LE FIGARO, ***Le covoiturage en plein boom,*** 2014
http://www.lefigaro.fr/secteur/high-tech/2014/07/31/32001-20140731ART-FIG00017-le-covoiturage-un-secteur-en-plein-boom.php

07_ Assurance

FFSA, ***Le marché de l'assurance en 2014,*** 2014
http://www.ffsa.fr/sites/jcms/p1_1474941/fr/le-marche-de-lassurance-francaise-en-2014?cc=fn_7345

08_ Vie privée

COMMISSION EUROPÉENNE, ***Barometer,*** 2015
http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm

09_ Logistique

ENCYCLO-ECOLO, ***Français et consommation responsable,*** 2014
http://www.encyclo-ecolo.com/Français_et_consommation_responsable#Les_Fran.C3.A7ais se_mettent_.C3.A0_la_consommation_respon- sable_en_2014

10_ Citoyenneté

BERKMAN CENTER, ***Three Case Studies from Switzerland : E-voting***
http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf

11_ Crowd-Equity

FINANCE PARTICIPATIF FRANCE, ***Baromètre de l'année 2014***
http://financeparticipative.org/barometres/annee-2014/

B

Bitcoin

Selon la définition de son créateur, Satoshi Nakamoto, Bitcoin est « un système de monnaie électronique entièrement de personne à personne permettant d'effectuer des paiements en ligne, sans passer par une institution financière ». Créée en 2009, Bitcoin est la première application développée sur une blockchain et, à ce jour, la plus massive. C'est un logiciel open-source dont le code est visible et modifiable par tous.
Après son apparition en 2009, le potentiel technologique de Bitcoin a été éclipsé par ses usages illégaux. Cependant, la communauté n'a cessé de grandir et la valeur d'un bitcoin a même dépassé les 1000$ courant 2013. Depuis Novembre 2014, elle oscille entre 230$ et 400$.

Pour aller plus loin : le-coin-coin.fr/dossiers/quest-ce-que-le-bitcoin/

C

Clef publique/privée

Le jeu de clef publique/privée est le mécanisme d'identification de la Blockchain. Cette innovation décisive provient de travaux sur la cryptographie asymétrique dans les années 70.

Les deux clefs sont liées mathématiquement de sorte que la clef publique (connue de tous) permet de coder un message tandis que la clef privée (connue par l'utilisateur seul) permet de le décoder. En somme, une clef privée permet de calculer la clef publique mais l'inverse est impossible.

Crypter un message
Alice souhaite envoyer un message à l'utilisateur Bob. Elle utilise alors la clef publique de Bob pour crypter son message. La clef privée de Bob lui permet de décrypter le message.

S'identifier
Alice souhaite s'identifier sur un service Blockchain. Elle utilise sa clef privée pour « signer » son identité. Le service, qui connaît la clef publique d'Alice, vérifie si les deux clefs correspondent. Dans ce cas, la clef privée est dite « de signature » et la clef publique « de vérification »

La clef publique/privée s'oppose au mot de passe unique, partagé entre l'utilisateur et le service. En cas de piratage des serveurs du service, l'ensemble des mots de passe utilisateurs peuvent être volés. Dans le cas d'une clef publique / privée, l'identité de l'utilisateur est menacée uniquement si sa clef privée est subtilisée.
En revanche, en cas de perte, une clef privée ne peut pas être régénérée.

Pour aller plus loin : bitcoin.fr/qu-est-ce-qui-relie-la-cle-publique-a-la-cle-privee/

M

Miners

Les miners, ou mineurs en français, sont les nœuds du réseau qui valident les transactions et alimentent la puissance de calcul de la Blockchain. Ce sont eux qui opèrent la validation des transactions à la place d'une instance centrale.

Ce sont des individus ou des organisations qui apportent le matériel informatique nécessaire pour résoudre des problèmes cryptographiques en temps réel. Le premier des mineurs à trouver cette solution est rémunéré en crypto-monnaie, ce qui génère une compétition entre les mineurs et les pousse à acquérir du matériel plus puissant *[voir Proof-of-Work]*.
Une carte en temps réel des miners de la blockchain Bitcoin est disponible sur https://bitnodes.21.co.

Mining

Le mining, ou minage en français, est l'action de validation des informations inscrites sur une blockchain (1). C'est aussi l'acte de création monétaire (2).

1. Le minage est l'activité de résolution de problèmes cryptographiques [voir Proof of Work] qui permettent la validation des blocs. Effectué par certains nœuds du réseau, c'est l'instrument qui remplace la vérification d'un office unique par un travail décentralisé. Cette opération collective produit un consensus sur la validité ou non d'une transaction.

2. Chaque validation est rémunérée par quelques milli-centimes de crypto-monnaie : c'est le mécanisme de création monétaire des crypto-monnaies sur une blockchain.

Ferme de minage Bitcoin en Chine (Crédits Photos : ©VICE)

P

Proof-of-Work

Lire d'abord Mining

La Proof of Work (PoW) est le résultat du problème cryptographique à résoudre pour qu'une nouvelle information soit ajoutée dans un bloc. Ce résultat est difficile à obtenir et nécessite beaucoup de puissance informatique. En revanche, sa vérification est peu consommatrice de ressources ce qui peut être effectué par le plus nombre.

La Proof-of-Stake (preuve d'intérêt) est une autre méthode de validation des blocs. Celle-ci est basée sur les avoirs (ainsi que leur temps de conservation) de la personne et se définit généralement par un pourcentage de création monétaire. C'est une méthode parallèle pour atteindre un consensus décentralisé et qui a l'avantage de consommer peu d'énergie (Peercoin, NeuCoin ou BlackCoin sont des monnaies PoS).

Les deux méthodes de ne sont pas exclusives et sont parfois utilisées conjointement.

Pour aller plus loin : cryptocoinsnews.com/bitcoins-future-proof-of-stake-vs-proof-of-work/

T

Token

Le token (jeton en anglais) est l'unité de base d'une blockchain. C'est cette unité transférable qui devient donc une preuve de propriété : le token est possédé sur un compte, une adresse au sein du système (par exemple, le token de la blockchain bitcoin est le Bitcoin). De plus, il est possible d'adosser des informations à des tokens et de les utiliser au-delà d'application monétaires : un titre de propriété, un bulletin de vote, une preuve d'antériorité..

Un moyen d'affecter une valeur spécifique à un token est la coloration de coins : des tokens taggés (colorés) qui seront comme un sous-sytème monétaire au sein d'une blockchain. Cela peut servir à émettre et gérer des actions pour un moindre coût, le site Coinprism permet de tester cette fonction assez facilement.
Les tokens sont l'unité transactionnelle et informationnelle sur une blockchain.

BIBLIOGRAPHIE

SWAN Melanie, ***Blockchain: Blueprint for a New Economy,*** O'Reilly Editions, 2015

CLIPPINGER John H, BOLLIER David, ***From Bitcoin to Burning Man: the quest for identity and autonomy in the digital society,*** Institute for Institutional Innovation by Data-Driven Design, 2014

Z/YEN GROUP, ***Chain of a Lifetime: How Blockchain Technology Might Transform Personal Insurance,*** 2014

SANTANDER, INNOVENTURES, OLIVER WYMAN, ANTHEMIS GROUP, ***The Fintech 2.0 Paper : Rebooting Financial Services***, 2015

WORLD ECONOMIC FORUM, ***Deep Shift Technology Tipping Points and Societal Impact,*** 2015

CELLABZ, ***Blockchain & Beyond,*** 2015

SATOSHI NAKAMOTO, ***Bitcoin: A Peer-to-Peer Electronic Cash System***, 2008
https://bitcoin.org/bitcoin.pdf

ETHEREUM, ***White Paper,*** 2015
https://github.com/ethereum/wiki/wiki/White-Paper

ETHEREUM, ***On Public and Private Blockchains,*** 2015
https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

PATRICK MURCK, ***Property law and the Blockchain,*** Berkman Center for Internet & Society, 2015
https://cyber.law.harvard.edu/events/luncheon/2015/10/Murck

BENJI ROGERS, ***How the Blockchain and VR Can Change the Music Industry,*** 2015
https://medium.com/cuepoint/bc-a-fair-trade-music-format-virtual-reality-the-blockchain-76fc47699733

INSIDE BITCOINS, ***How Blockchain Technology could Revolutionize the 1.1 Trillion Insurance industry,*** 2015
http://insidebitcoins.com/news/how-blockchain-technology-could-revolutionize-the-1-1-trillion-insurance-industry/28516

CRYPTOCOINNEWS, ***How The Blockchain can Digitize Regulation,*** 2015
https://www.cryptocoinsnews.com/block-chain-can-digitize-regulation/

TECHCRUNCH, ***Using The Blockchain To Fight Crimes And Save Lives,*** 2015
https://www.cryptocoinsnews.com/block-chain-can-digitize-regulation/

SILICON ANGLE, ***Honduras to Use Bitcoin Blockchain Tech to Run its Land Registry,*** 2015
http://siliconangle.com/blog/2015/05/17/honduras-to-use-bitcoin-blockchain-tech-to-run-its-land-registry/

DRÉAN Gérard, ***Contrepoints.org, Qui gère le Bitcoin ?***, 2015
http://www.contrepoints.org/2015/09/16/221958-qui-gere-le-bitcoin

KHAN ACADEMY, ***Bitcoin What Is It?,*** 2014
https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it

SWAN Melanie, ***Bitcoin and Blockchain Explained,*** 2015
http://fr.slideshare.net/lablogga/bitcoin-and-blockchain-technology-explained-not-just-cryptocurrencies-economics-and-markets-applications-in-art-health-and-literacy

EPICENTER BITCOIN, Brian, Meher & Sebastien, ***The Big Chain Powwow,*** 2015
https://soundcloud.com/epicenterbitcoin/eb-108

uchange.co
@Uchange_

Plateforme de transformation digitale
Conseil • Recherches externalisées
Relations startups • Opérations digitales

Livre Blanc v1.0 – Janvier 2016

D.A. et maquette : Pauline Rigaud & Structure Bâtons