

n°59

59 euros

archimag.com

[STRATÉGIES & RESSOURCES DE LA MÉMOIRE & DU SAVOIR]

guide pratique

serda

une publication du groupe

blockchain : le nouveau
cadre de confiance

préface

dans le domaine des technologies de l'information, les révolutions se cumulent et donnent le tournis : cloud, intelligence artificielle, blockchain, pour n'en citer que trois récentes. À chaque fois, des phases similaires s'enchaînent. D'abord du buzz, plutôt enthousiaste. Ensuite, des échanges d'arguments, de type « *forces, faiblesses, opportunités, menaces* » - le fameux « *swot* ». Puis l'on se demande ce que l'on peut vraiment en faire, et comment. C'est dans cette phase printanière que semble se situer la blockchain, faite de promesses, de tentatives et de jeunes pousses !

Mais il faut d'abord comprendre ce qu'est la blockchain. Ce guide pratique Archimag fait le choix d'exposer longuement son mécanisme et ses origines, sous des angles tour à tour technologiques, historiques, sociologiques et économiques. Parce que la blockchain est encore loin d'avoir atteint sa maturité et que diverses questions se posent encore, qu'il est utile de comprendre. Parce que, s'agissant d'une construction à la fois purement technologique et intellectuelle,



Michel Remize

elle peut paraître abstraite, difficile à se représenter, et de la pédagogie est donc nécessaire pour la démystifier. Le but est de permettre d'au moins la situer pour évaluer l'intérêt qu'elle peut revêtir dans son activité. Et d'apporter de la confiance dans ce concept puisque celle-ci est sa raison d'être.

Dans un avenir proche, cette confiance pourra se voir renforcée par des interventions législatives et normatives. Elle est déjà présente à travers de nombreux cas opérationnels de par le monde. Dans l'Hexagone, différents secteurs ou domaines réfléchissent à la blockchain

ou se lancent : notamment la finance, l'immobilier et l'environnement, l'identité, le vote ou le stockage.

Transfert, registre, smart contrat sont les trois directions prises par les sociétés de services ou les éditeurs proposant des offres construites sur la blockchain. Des retours d'expérience apportent de premiers enseignements.

Et pour réviser vos connaissances en blockchain acquises dans la lecture de ces pages, ou les approfondir, ce guide vous propose un quiz et différentes sources à consulter.

Au bout du compte, y aura-t-il révolution ? Prenons-en le pari en répondant par l'affirmative. ■

Michel Remize

[Rédacteur en chef]

nous faisons les guides pratiques Archimag

Serda édition-IDP
24, rue de Milan, F-75009 Paris
Tél. : +33 (0)1 55 31 92 30
Fax : +33 (0)1 44 53 45 01
infos@archimag.com
www.archimag.com

contacts e-mail
prenom.nom@archimag.com

rédaction
rédacteur en chef
Michel Remize
directrice de la rédaction
Louise Guerre
directeur de la publication
Pierre Fuzeau

l'équipe de rédacteurs
Clémence Jost, Éric Le Ven,
Bruno Texier
auteurs et experts
voir page 3
site web, newsletter
Clémence Jost
conception graphique
Julio Arias-Arriaz Arcoat
maquette
Bruno Daléle. Exeterra
Solutions Graphiques

publicité
Cathy Potel
01 55 31 92 30
responsable marketing et commercial
Alexandre Corbier
01 44 53 45 00
vente au numéro
service abonnement
Suzanne Amia
suzanne.amia@archimag.com
réclamations
suzanne.amia@archimag.com
BP 95-92244 Malakoff Cedex
tarifs et conditions d'abonnement
valables jusqu'au 31-12-2017
France : 1 an, 125 euros
France : 2 ans, 228 euros
Tarif étudiant : 1 an, 30 euros

Tarif demandeur d'emploi :
1 an, 54 euros
Vente au numéro : 18 euros
Plus d'informations :
www.archimag.com/boutique
imprimeur
Inore Groupe Impression
4 rue Thomas Edison
58640 Varennes Vauzelles
éditeur
IDP Sarl, au capital
de 40 000 euros Information,
documentation, presse
N° de commission paritaire :
1216 T 85484
ISSN : 2260-1708
Dépôt légal à parution
du numéro

crédits photos
Couverture : Fotolia
Intérieures : droits réservés,
sauf mentions différentes
annonceurs
IDP : 2^e de couverture, 2, 21,
33, 39, 49, 3^e de couverture,
4^e de couverture
Serda Formation : 17



Archimag est une publication
du groupe Serda.
Toute adaptation ou reproduction
même partielle des informations
parues dans Archimag est
formellement interdite sauf
accord écrit d'IDP SARL.
© IDP juin 2017



Ce document est imprimé
sur papier certifié PEFC

Annoncez-vous sur Archimag et Archimag.com
Contactez Cathy Potel : 01 55 31 92 30, cathy.potel@archimag.com
Abonnez-vous à Archimag : www.archimag.com/le-kiosque

sommaire

[éclairages]

- 04 la blockchain, enfant prometteur du digital
- 16 petite histoire du bitcoin
- 18 une autre histoire de la blockchain
- 21 les enjeux juridiques soulevés par la blockchain
- 23 un marché prometteur ?
- 25 les tiers de confiance face à la blockchain
- 26 quand la blockchain se tourne vers le pouvoir régalien



28

- 28 la blockchain, vue de l'étranger

[usages]

- 30 blockchain : bientôt des normes
- 31 comment envisager la blockchain pour son système d'information
- 32 les banques investissent dans la blockchain
- 34 données cadastrales et données de conformité

- 35 les nouvelles énergies de la blockchain
- 36 nos futures identités sur la blockchain
- 37 une blockchain pour les élections ?
- 38 blockchain à valeur probante

[offres]

- 40 la blockchain au service des transferts d'argent
- 42 blockchain : une machine à preuves
- 44 smart contracts : infalsifiables, sans tiers et à exécution automatique

[expériences]

- 46 en voiture la blockchain !
- 47 conteneurs à la chaîne... et en blockchain !
- 48 une blockchain pour la smart grid de Lyon Confluence
- 50 la blockchain pour mieux gérer les droits d'auteur

[quiz]



51

- 51 la blockchain décortiquée... quiz
- 52 sources



+ nos auteurs et experts

Laurence Allard

maître de conférences, sciences de la communication, IRCAV-Paris 3/Lille 3, sociologue des usages numériques

Polyanna Bigle

avocat, directeur du département sécurité numérique, Lexing Alain Bensoussan Avocats

Bertrand Copigneaux

senior innovation consultant, Idate Digiworld

Fabrice Croiseaux

animateur du groupe de travail blockchain de la FNTC

Christophe Dutheil

journaliste

Sébastien Kurt

explorateur pirate

Éric le Ven

journaliste Archimag

Pierre Lorcery

trésorier de l'association la Chaintech

Kévin Palop

consultant en transformation digitale

Jean-Louis Pascon

expert, Demat-conseil.fr

Michel Remize

rédacteur en chef Archimag

Adrian Sauzade

cofondateur de Czam, expert en cryptomonnaie

la blockchain, enfant prometteur du digital

La blockchain est à la mode. La scène numérique en a fait l'une de ses marottes, et pour cause : elle représente l'une des ruptures technologiques et conceptuelles majeures de notre temps.

I. un concept d'une grande élégance

Le concept techno-intellectuel qui sous-tend la blockchain n'a pas surgi ex nihilo. Elle est l'élégante association de technologies (cryptographie asymétrique, protocole d'échange pair-à-pair...), de théories (mathématiques, politiques et économiques) et d'un besoin dans l'air du temps de l'internet (la confiance dans l'échange dématérialisé entre deux parties prenantes).

La blockchain, comme concept, est donc la fille d'un intellect humain parfois millénaire, nourri des possibilités techniques et des usages sociétaux d'aujourd'hui. C'est ce qui fait son élégance, car l'association est complexe. Son histoire est d'ailleurs mouvementée, et si aujourd'hui la blockchain a prouvé son intérêt, sa cohérence et son applicabilité, cela s'est fait au fil d'une expérience pionnière et absolument visionnaire : bitcoin.

l'exemple bitcoin

On usera souvent de l'exemple bitcoin dans les lignes qui suivent, parce que sa valeur illustrative est forte et donne aux concepts une existence concrète. On prendra toutefois garde à ne pas confondre blockchain et bitcoin comme deux entités

interchangeables. Bitcoin est une implémentation, parmi d'autres, des concepts de blockchain. La première, cependant, qui fut réussie et source de nombreux enseignements.

L'objectif des lignes qui suivent est de brosser un portrait accessible de ce qu'est la blockchain, de son fonctionnement et de ses potentielles applications. Pas de panique ! L'important pour nous, commun des mortels, non-ingénieurs, non-mathématiciens, simples utilisateurs potentiels, est avant tout d'en comprendre la nature, d'en démystifier le fonctionnement, pour être capable d'y placer sa confiance.

Car tout est là : la blockchain est une technologie dont l'objectif premier est d'établir sans intermédiaire centralisé une confiance entre deux parties prenantes.

1. pour faire confiance à la blockchain, il faut d'abord la comprendre

L'ambition de la blockchain est gigantesque : ni plus ni moins de remettre en question le monopole de tous les

intermédiaires qui centralisent les échanges entre personnes en contrepartie d'une garantie absolue. Pensez aux systèmes monétaires des États, aux banques et aux organismes de certifications, mais aussi à Facebook, Twitter, Tinder, Uber...

La confiance indispensable que ces acteurs génèrent repose intégralement sur un concept centralisateur de contrôle. Avec la blockchain, l'idée est de passer d'un système centralisé à un système distribué (voir schéma 1).

Deux avantages principaux à cela :

❶ la confiance ne repose plus sur un seul acteur dont la compromission, volontaire ou accidentelle, a pour conséquence l'effondrement de la confiance pour toutes les parties prenantes qui gravitent dans son orbite ;

❷ deux parties prenantes peuvent opérer un échange sans intermédiaire, c'est-à-dire sans captivité, technique ou financière.

Lorsque l'on parle d'échange entre deux parties prenantes, on pense immédiatement aux flux financiers. C'est parfaitement logique puisque le principe de

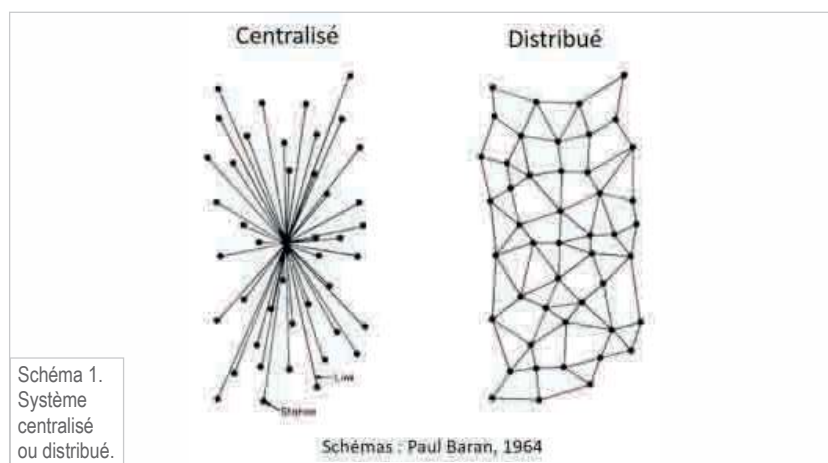


Schéma 1. Système centralisé ou distribué.

un marché prometteur ?

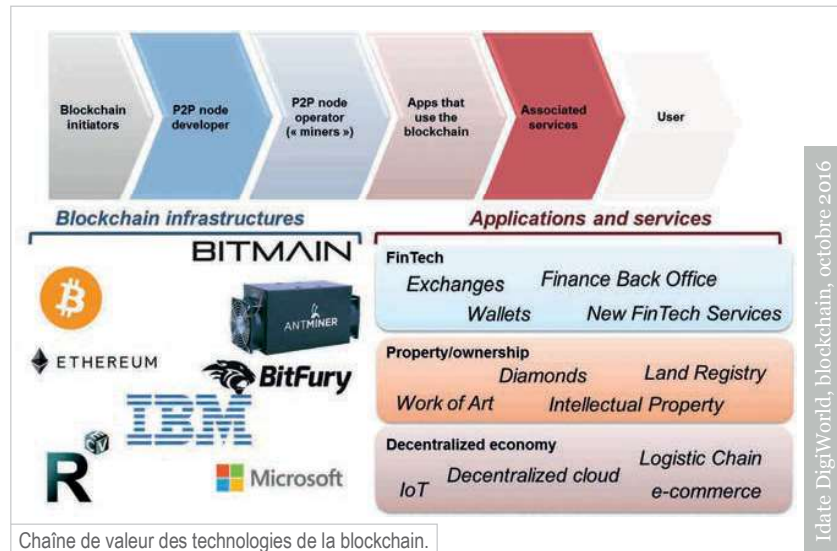
Quel est le poids économique présent ou pressenti de la blockchain ? Un nouveau marché se dessine-t-il ? Réponse avec l'Idate DigiWorld, think tank travaillant sur les grandes évolutions du numérique et produisant notamment des analyses économiques.

La blockchain est une rupture technologique en matière d'infrastructure sécurisée. Elle s'appuie sur la combinaison d'algorithmes cryptographiques avec un stockage dupliqué d'informations sur un réseau informatique pair-à-pair. En tant qu'infrastructure sécurisée, elle peut apporter des réponses aux industries ayant de forts besoins de sécurité. Mais sa spécificité tient surtout aux possibilités d'établir une infrastructure dédiée à l'échange d'informations entre des tiers ayant des intérêts divergents sans qu'aucun d'entre eux n'ait un contrôle complet de l'infrastructure. Issue de la cryptomonnaie bitcoin, la blockchain émerge aujourd'hui comme une nouvelle infrastructure IT décentralisée, avec des usages allant au-delà des cryptomonnaies et des applications financières.

1. l'écosystème de la blockchain

■ la chaîne de valeur

La mise en œuvre de la blockchain demande un ensemble d'activités nécessaires à son utilisation, de l'initiation de la chaîne au développement des logiciels nécessaires ou à l'opération des nœuds du réseau pair-à-pair. L'écosystème offre des opportunités aussi bien pour des acteurs établis que pour des nouveaux entrants, avec deux



positionnements principaux : sur les infrastructures ou sur les applications et services utilisant une infrastructure blockchain.

■ les infrastructures de la blockchain

■ les initiateurs

Les initiateurs d'une blockchain définissent les règles et algorithmes de la chaîne. C'est dans la majorité des cas (blockchain publique ou hybride) un ensemble d'acteurs qui décident de s'unir pour lancer une blockchain répondant à un objectif commun. Par exemple : Bitcoin, Ethereum, Everledger...

■ les développeurs

Les développeurs de nœuds du réseau pair-à-pair créent le logiciel qui est utilisé pour former des nœuds du réseau de la blockchain. Ce logiciel, déployé ensuite par les opérateurs de nœuds pair-à-pair sera chargé de valider les transactions et de les inscrire dans la blockchain. Par exemple : BitMain, BitFury, IBM...

■ les opérateurs ou mineurs

Les opérateurs de nœud du réseau pair-à-pair (aussi appelés « mineurs ») utilisent leurs ordinateurs reliés au réseau internet

pour faire s'exécuter le logiciel des nœuds du réseau pair-à-pair. Dans le cas d'une blockchain publique, ils sont rémunérés pour ce rôle clef (mineurs). Par exemple : BitMain, BitFury, Microsoft...

■ les applications de la blockchain

■ les cryptomonnaies et applications financières

C'est l'utilisation initiale de la blockchain et aujourd'hui encore la plus développée. La blockchain se substitue au système bancaire pour permettre aux utilisateurs d'effectuer des transactions financières et d'en archiver l'historique.

Les principaux avantages de cette substitution sont une réduction des frais de transaction, une décorrélation des systèmes bancaires et étatiques et une réduction du temps de validation des transactions (étant donné qu'une fois validée et enfouie dans la blockchain, une transaction est impossible à invalider).

Autour de cette utilisation initiale comme cryptomonnaie, d'autres applications financières se sont greffées, offrant des

blockchain : une machine à preuves

Que des paiements en ligne soient détournés vers des poches frauduleuses, qu'un parti politique conteste le résultat d'une élection ou que deux auteurs se crêpent le chignon pour la paternité d'une oeuvre, tous ces dilemmes pourraient être évités si la blockchain parvenait à trouver sa voie.

La blockchain prend la forme d'un registre numérique qui consigne tous les échanges effectués entre les utilisateurs depuis sa création. À tout moment, le système sait qui possède quoi et est capable d'en fournir la preuve. Plusieurs offres ont déjà vu le jour dans ce domaine.

AuCoffre.com

France

Aucoffre.com, plateforme d'intermédiation spécialisée dans les métaux précieux, a implémenté la blockchain sur son système afin de simplifier le travail de traçabilité demandé par les autorités de contrôle et par ses propres membres utilisateurs. Auditeurs, commissaires aux comptes et douanes peuvent désormais utiliser la blockchain comme support et outil de contrôle. Ce qui améliore la transparence des transactions, et apporte aussi des garanties supplémentaires aux e-consommateurs.

→ www.aucoffre.com

InnovSanté

France

Chain For Health

InnovSanté a créé un passeport santé numérique baptisé « *Passeport vital* ».

Il s'agit d'un système sécurisé permettant d'accéder au dossier médical numérique du patient, quel que soit l'hôpital où il se trouve. Dans un second temps, InnovSanté compte développer une chaîne de sécurité sociale numérique mondiale pour les pays qui n'ont pas de système de santé souverain ou qui souhaitent faire évoluer leur système de soins vers une organisation numérique intelligente et économique.

→ www.innovsante.com

Keeex

France

Keeex est une start-up française qui propose plusieurs services basés sur la blockchain : un service de transfert de propriété virtuelle blockchain, de signature électronique et de documents certifiés. Mais ce qui l'a fait connaître, c'est

des lieux (automobile, immobilier, mobilier...), des déclarations de sinistres, des constats, des preuves de présence à une date et dans un lieu donnés, des preuves de patrimoine (bijoux, objets de valeur), de colis détériorés à sa réception, etc.

→ keeex.me/fr/

Virtual Notary

États-Unis

Virtual Notary utilise la blockchain pour authentifier, par le biais d'un certificat électronique crypté, tout type de contenus (documents électroniques, images, enregistrements, code source, contenus web, contenus des réseaux sociaux, lettre de créances personnelles, enregistrements DNS et Whois, etc.).

→ virtual-notary.org



La blockchain peut prendre la forme d'un registre numérique qui consigne tous les échanges effectués entre les utilisateurs depuis sa création.

son application Photo Proof by Keeex qui prend, authentifie, géolocalise et horodate les photos prises avec son smartphone sur la blockchain. Photo Proof peut par exemple servir pour des états

Microsoft

États-Unis

Pour Microsoft, les applications de la blockchain sont presque sans limites : prêts, obligations, paiements, chaînes