Christian Fauré

Hypomnemata : supports de mémoire

La Blockchain et l’émergence des « distributed consensus engines »

by Christian on 13 septembre, 2015

La blockchain à la hache

Je vais y aller *à la hache*. Mon propos ne sera pas chirurgical, précis ; il sera assez grossier.

Grossier d’abord parce que je vais vous parler de choses qui sont **émergentes** et qui n’ont **pas encore de formes précises** mais produisent beaucoup de **protentions**, c’est à dire beaucoup **d’attente.**

Tout le monde a entendu parler du **Bitcoin**, ce système de transfert d’argent, mais probablement peu a entendu parler de la **blockchain,** qui est la technologie sous-jacente au Bitcoin.

Le Bitcoin est à la croisée de différentes technologies parmi lesquelles : les protocoles Peer-to-peer, les mécanismes de cryptographie, les systèmes de gestion de version de code, les bases de données distribuées , etc.

Même si, en apparence, il n’y a rien de nouveau, **la blockchain est une réelle innovation** dont les conséquences ont encore du mal à être appréhendées. Ceux qui se sont intéressés à la blockchain **la comparent volontiers au web** de part l’ampleur des conséquences qu’elle pourrait avoir.

De fait, il y a beaucoup de **discours prophétiques** à son sujet ; c’est le temps des *prophéties* et des *prophètes* de la blockchain.

Salim Ismail, qui est l’ambassadeur de l’*Université de la Singularité* – et qui passe son temps à cataloguer et à qualifier toutes les innovations technologiques – a déclaré, en Juillet 2015 à Paris, lors de la conférence USI : *« The blockchain is THE most disruptive technology I have EVER seen »*. Cela donne le ton.

In the beginning was Satoshi Nakamoto

Le principe du bitcoin a été publié en 2008 et mise en oeuvre en 2009 par le mystérieux Satoshi Nakamoto.

Il permet de surmonter un problème de taille qui est celui **du double paiement** dans les transactions financières (*double spend problem*) : comment s'assurer qu'un montant ne sera pas dépensé deux fois ? Comment ne pas se faire remettre un chèque en bois ? etc.

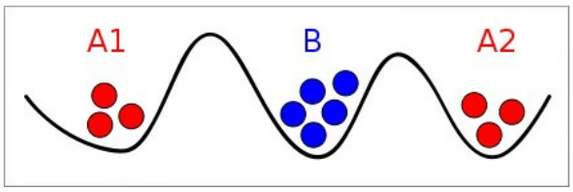
Traditionnellement il faut faire appel **à des tiers de confiance** que sont typiquement **les banques**. Mais, même avec un tiers, le risque de fraude est toujours présent, les systèmes bancaires centralisés facturent ce risque (et bien d'autres services encore), ce qui conduit à rendre très difficile des micros-paiements qui ne supportent pas les frais induits par les structures centralisées.

Satoshi Nakamoto précise, dans son papier fondateur sur le BitCoin, sont intention avec la création du Bitcoin :

> « Un système de monnaie électronique entièrement en pair-à-pair permettrait d'effectuer des paiements en ligne directement d'un tiers à un autre **sans passer par une institution financière** »

Avec la blockchain, le fait qu'une transaction soit acceptée ou rejetée est le fruit d'un **consensus distribué** et non d'une **institution centralisée**.

La manière dont ce consensus distribué peut être réalisé renvoi aux travaux sur les systèmes informatiques distribués où l'on parle de « problème des généraux byzantins ».



Ce problème classique de l'informatique distribué dans un environnement non sécurisé peut s'expliquer par la métaphore des généraux byzantins suivante : dans le schéma ci-dessus l'armée A fait le siège de l'armée B, A1 et A2 doivent attaquer ensemble pour gagner contre B. Pour cela ils doivent s'envoyer des messages : d'abord de A1 vers A2 pour proposer le moment et l'heure de l'attaque, mais A2 peut douter du message qu'il recevra de A1 (B en a eu connaissance, et peut-être l'a-t-il modifié, etc). De même A1 attend le message de confirmation de A2 pour ne pas se retrouver à attaquer seul. Mais quand il reçoit ce message il peut lui aussi douter de son origine et de son contenu.

Résoudre ce genre de problème, c'est ce qu'on l'on fait quand on fait de la conception de logiciels distribués, tolérants aux pannes et aux erreurs (avec une logique que l'on qualifie de *Design for Failure*), et capables de se coordonner dans un environnement non fiable et asynchrone.

Satoshi Nakamoto (cf. Bitcoin expliqué par son fondateur) donne les principes de sa solution pour opérer le bitcoin et résoudre les problèmes du double paiement et des généraux byzantins :

> « nous proposons une solution au problème de double-dépense en utilisant un **serveur horodaté distribué en pair-à-pair** pour **générer des preuves informatiques** de **l'ordre chronologique des transactions**. Le système est sécurisé tant que des nœuds honnêtes contrôlent ensemble plus de puissance de calcul qu'un groupe de nœuds qui coopéreraient pour réaliser une attaque. »

Au coeur du Bitcoin, ce « serveur horodaté distribué en pair à pair » qui à la fois **est** *la blockchain* (en tant que technologie de stockage distribuée) et **produit** *la blockchain* (en tant que **livre de compte** ouvert, public et distribué où l'on peut lire l'**enchainement des transactions horodatées**, et ce depuis la toute première transaction).

Les *miners* de la blockchain

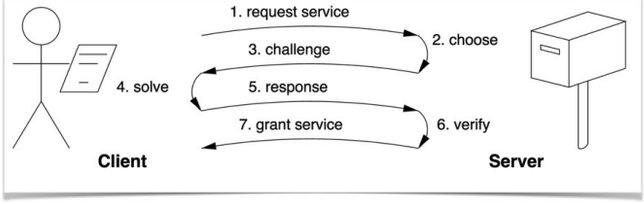
Dans le réseau de pair à pair de la blockchain, les *miners* sont des noeuds du réseau qui, en « travaillant », produisent des **preuves de travail.** Preuves qui les autorisent à ajouter une transaction dans la chaîne (un block est créé toutes les dix minutes)

Après les dockers, voici les *miners.*

L'aspect novateur de la résolution proposé par Satoshi Nakamoto c'est donc de faire **travailler les machines**, c'est à dire les CPUs, pour pouvoir ajouter un block à la blockchain. Chaque block est **le fruit d'un consensus machinique et algorithmique**.

La puissance de calcul est au coeur du protocole et de l'économie du bitcoin : **l'intégrité** de la blockchain est garantie par le fait que la puissance de calcul nécessaire pour **falsifier** le réseau couterait plus cher qu'elle ne rapporterait et aussi parce que tout *miner* qui souhaiterait falsifier la blockchain se retrouverait **en compétition avec l'ensemble des autres miners.**

La **preuve de travail** qui est demandée au *miners* est donc une **preuve de calcul via les technologies ce cryptage** (des message cryptés – des énigmes – sont proposés aux serveur en maîtrisant la complexité du cryptage pour que cela prenne environ 10 min) ; c'est la clé de voute du Bitcoin.



Les nouvelles protentions de la Blockchain

La Blockchain créée de nouvelles attentes (c'est à dire des protentions qui polarisent les attentions).

Ce qu'apporte la blockchain, c'est l'avènement d'un réseau décentralisé non plus seulement de **transport** ou de **transfert**, mais de **transaction**. En ce sens, c'est un **système transactionnel sécurisé à très bas coût**. Ce que la blockchain peut apporter, c'est une **automatisation distribuée des transactions** qui peut rendre caduque toutes les formes d'organisations et d'institutions qui se posent en tiers de confiance ou de certification dans un **contexte transactionnel (propriété, bien, argent).**

Du coup, cela place toute **l'économie traditionnelle de la transaction** en porte à faux. Et pas seulement les industries qui se font « ubériser » , puisque cela peut aussi *ubériser* Uber ; tout comme booking.com, Airbnb, Twitter, Paypal, c'est à dire que tous ceux qui ont **court-circuité les industries traditionnelles** se retrouvent eux-mêmes potentiellement sur la sellette.

Ce qui me fait dire que si le Web a permis **l'automatisation de la relation** (et de la mise en relation), la Blockchain permet **l'automatisation de la transaction** en supprimant les tiers.

La blockchain apporte également un élément très important : on parle souvent de **transparence**, puisque l'ensemble des transactions sont publiques. Mais je préfère souligner le fait qu'il n'y a **pas d'asymétrie de l'information** (asymétrie illustré par le tableau de De la Tour) **;** il n'y a pas un point de vue panoptique qui soit privilégié.

Ainsi, avec la blockchain, **tout le monde voit la même chose**, là où avec les géants du web plus personne ne voyait la même chose, à force de *profiling* : par exemple, plus aucun d'entre nous n'a la même page de résultat sur Google pour une recherche donnée.

La blockchain sans le Bitcoin

De même que la blockchain du bitcoin a montré sa puissance en appliquant des protocoles de transaction distribués à la monnaie, de même **cette technologie peut être utilisée dans d'autres champs d'activité** que la transaction monétaire.

Exemples : systèmes de vote, gestion décentralisées des DNS (cf. le projet Namecoin).

Désormais la technologie blockchain peut être utilisée pour des transactions qui vont **au delà d'une simple transaction de paiement** et qui contiennent des instructions beaucoup plus complexes (des instructions conditionnelles et programmables), on parle alors de **contrats.** Contrats qui peuvent être publiés sur la blockchain pour qu'ils s'exécutent automatiquement sous certaines conditions, raison pour laquelle on utilise l'expression de **« Smart Contracts »**.

On est donc au **coeur des technologies de transfert**, surtout si l'on se réfère au Littré qui nous rappelle que « transfert » est un terme d'origine financière et juridique ; **on transfère des droits, des actions, des biens et des propriétés.**

La blockchain n'est pas le web

Par ailleurs, la blockchain est une nouvelle forme d'espace public, différente du Web. Si le web est un système de **publication décentralisé**, la blockchain est **un système de consensus distribué**. Du *web* à la *blockchain*, on passe d'une **infrastructure de publication** à une **infrastructure de certification.**

La blockchain peut ainsi jouer un rôle similaire à un protocole de transfert et remplacer le Web, surtout quand ces transferts doivent donner lieu à des **transactions certifiantes et sécurisés**, ce que **ne sait pas faire le web** sans faire intervenir des organisations certifiantes centralisées.

Ainsi, la blockchain apporte une **infrastructure de confiance algorithmique distribuée.** En plus court : *consensus-as-a-service (consensus à la demande).*

Consensus et dissensus

Ici, il ne faut pas confondre deux choses : d'une part la **topologie distribuée de la technologie blockchain** et, d'autre part, le *produit* de cette technologie qui est la **chaîne linéaire** des transactions (celle que l'on télécharge quand on se connecte la première fois – fichier d'environ 30 Go).

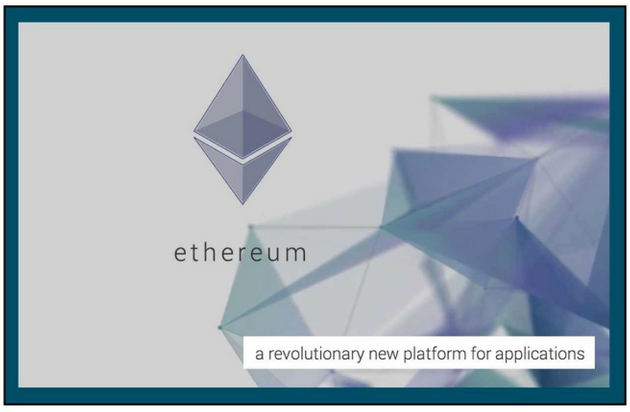
Or la **topologie linéaire d'une chaine** n'est précisément pas celle d'une **arborescence**. La blockchain n'est donc pas une technologie de **dissensus** mais de **consensus**, et tout ce qu'on appelle les *forks de la chaîne* – les **bifurcations** – sont ici **systématiquement élaguées**.

Je dis çà pour bien préciser que **la blockchain** n'est pas un système herméneutique qui enregistrerait l'ensemble des interprétations et arguments pour retracer un débat par exemple.

Ce n'est pas le GitHub des forks **et des dissensus** mais un système de **« consensus distribué ».** Mais il est possible que la Blockchain puisse, **en retour** (parce que tout çà, c'est systémique), permettre de poser la différemment question d'un système herméneutique (qui outille le dissensus)..

L'explosion cambrienne de la Blockchain

La blockchain se présente donc comme une **infrastructure de certification** dont toute application pourrait bénéficier nativement si elle s'appuie dessus.



Des projets comme **Ethereum** ou **Eris** cherchent à proposer un environnement, un *framework*, capable de faire tourner n'importe quelle application sur la base d'une blockchain. Là où çà se complique, c'est que Ethereum et Eris s'appuient sur **des blockchains différentes**. En effet Etherum repose sur une **blockchain publique** là où Eris repose sur une **blockchain privée.** Mais il y a aussi d'autres solutions alternatives comme Tendermint (merci Nicolas Sauret).

Aussi, si j'ai parlé de **LA** blockchain depuis le début de cette note, sachez pourtant qu'**il n'y a pas UNE blockchain mais de nombreuses**, et toutes avec des variantes. Il faut donc souligner qu'il y a une **explosion des blockchains**, ce qui contribue à la difficulté de cerner le sujet et ses enjeux.

Sachez que l'on parle aujourd'hui d'**explosion cambrienne de la blockchain.**

Le fait que la technologie blockchain puisse **servir d'infrastructure a de nouvelles applications** amène à parler de DApps, pour « Distributed Applications » . Des premières initiatives existent, tels que :

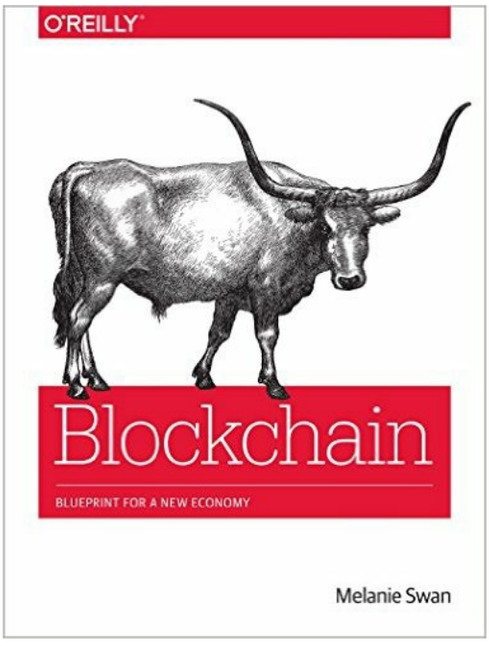
- **OpenBazaar** dont l'équivalent centralisé est **Craiglist**
- **lazoozorg** dont l'équivalent centralisé est **Uber**
- **Twister** dont les équivalent centralisés sont **Twitter** ou Facebook
- **Storj** dont l'équivalent centralisé est **Dropbox**
- **...**

Dans une **logique prophétique,** nous pourrions rajouter la possibilité d'avoir des agents intelligents (au sens de l'intelligence artificielle) qui pourrait exécuter des tâches pré-spécifiées selon certains conditions ou évènements ajoutés à la blockchain.

Rajoutons à ce tableau que la blockchain pourrait jouer un rôle décisif dans l'interconnexion des objets : **l'internet des objets (IoT)** pourrait bien se révéler être la **Blockchain des Objets (BoT)**.

D'ailleurs pour Mélanie Swan, auteur de Blockchain, Blueprint for a new economy :

> « The blockchain could be an Occam's razor, the most efficient, direct and natural means of **coordinating all human and machine activity** ; it is a natural efficiency process. »



Print PDF
Signaler sur Twitter

Autres notes similaires :

- **REST en image**

On a beau dire, parler de « Representational State Transfert » reste souvent un terme auquel il est difficile d'associer une représentation imagée. Pourquoi parle-t-on d'état ? De représentation ? Et de transfert ? Cette image peut aider : Signaler sur Twitter.....

- **Le propre du transfert et le tranfert du propre (infrastructure studies)**

Transport et Transfert Parler d'infrastructure du numérique c'est toujours prendre le risque d'ennuyer son auditoire et de faire peur : On va encore nous parler des « autoroute de l'information », d'accès internet à très haut débit, de la taille des tuyaux, etc. Or je ne parlerai pas de tuyaux, ni d'accès internet à très haut débit, […].....

- **Services Web ou API ?**

Web service & APIs On ne parle plus beaucoup de « services web » pour désigner les communications de machines à machines sur le web. On préfère mettre en avant le terme d'API : par exemple on ne dit plus « Restful web services » mais « Restful API« . Qu'est ce qui a changé ? A part que cela permet […].....

Tagged as: Architecture, blockchain, transaction, transfert

{ 12 comments… read them below or add one }

Hugues septembre 13, 2015 à 2:12

Merci pour cette synthèse autour de la blockchain, tres claire, même à la hâche 😉

Je ne suis pas du tout spécialiste du sujet, mais il y a un question de fond que je n'arrive pas comprendre.
C'est la soi-disant « absence » du besoin « du tiers », du troisième nécessaire a toute relation contractuelle, à tout échange. Pour qu'il y ai contrat entre 2 personnes, il y a necessairement un troisieme entre les deux pour que ce contrat tienne (meme si les valeurs du cadre contractuel semble absentes, elles sont interioriées par les individus).

Je renvois a l'excellent travail d'Alain Supiot sur « la gouvernance par les nombres »
http://www.iea-nantes.fr/cn/conferences/actualite_553

Il me semble que ce troisième, ce tiers de confiance, bien plus qu'absent est en fait « inclus » dans la construction même de la blockchain, est-ce bien cela ?
Si c'est le cas, cela veut dire que l'ideologie politique sous-jacente est en fait tout à fait explicite dans le code de la blockchain, mais qu'elle est retiré de tout processus politique de délibération, de toute processus démocratique.
Si cette intuition s'avere juste, on retombe ce qu'explique et dénonce Supiot, « une gouvernance par les nombres »…ce qui repose sur une idéologie: l'anarcho-capitalisme .
La blockchain serait donc le parfait outil pour instaurer l'échange, les transactions suivant cette idéologie anarcho-capitaliste.

Et il me semble que le recul sur le bitcoin, et ces critiques, donne un exemple concret sur cela. Par exemple la critique de Jorion sur le bitcoin
http://www.pauljorion.com/blog/2013/10/03/bitcoin-la-monnaie-du-futur/
« L'idée est intrigante : peut-on transformer une « monnaie-on-joue » en une « monnaie-on-ne-rigole-pas », sans police, seulement par la méthode Coué ? Pendant un certain temps peut-être, mais tout cela reste fondamentalement une pyramide, une « cavalerie », une « machine de Ponzi » comme on dit aujourd'hui, qui fera un jour ou l'autre des malins qui auront gagné et des gogos qui auront perdu. À moins bien sûr que le Bitcoin ne devienne une monnaie réglementée, c'est-à-dire protégée par un système légal et judiciaire. »

la generalisation de la blockchain a bien « tout » processus de transactions, de contrat, comme évoqué dans votre article, soulève beaucoup de questions.
En tout cas pour moi, cela soulève une question de fond, sur la nature de l'échange, et l'idéologie politique sous-jacente a l'œuvre dans ces technologies….qui me semble bien être l'anarcho-capitalisme, enfin de ce que j'en comprends.

Hugues

Répondre

Stéphane Traumat septembre 13, 2015 à 5:18

Si cela peut aider, j'ai écrit quelques articles sur le bitcoin :
Qu'est-ce que Bitcoin, comment ça marche et pourquoi c'est une révolution ? (https://medium.com/@straumat/quest-ce-que-bitcoin-comment-ca-marche-et-pourquoi-cest-une-revolution-63720070c5cd?source=featured———1)
Que répondre quand on vous dit que Bitcoin n'est pas une vraie monnaie ? (https://medium.com/@straumat/que-r%C3%A9pondre-quand-on-vous-dit-que-bitcoin-n-est-pas-une-vraie-monnaie-140d2d58d9f9)
et un article devenu un peu inutile : Tutorial : Miner des bitcoins à la maison avec un Raspberry Pi (https://medium.com/@straumat/tutorial-miner-des-bitcoins-a-la-maison-avec-un-raspberry-pi-c1631bb11a06)

Répondre

Emmanuel Lécharny septembre 14, 2015 à 9:10

Intéressant.
Cela dit, il serait bon d'évoquer deux problèmes majeurs du mécanisme de blockchain :
– la taille du backlog des transactions qui ne peut que grossir avec le temps
– le coût du calcul du challenge mathématique, qui se traduit en consommation d'énergie.

A moyen et surtout long terme, ce coût peut être un vrai problème pour ce type de système, par rapport à un méchanisme de validation centralisé.
Pas sûr que ce soit économiquement viable à grande échelle…

Répondre

Emmanuel Lécharny septembre 14, 2015 à 9:12

Par ailleurs, les commentaires ne sont pas visibles… En attente de modération ?

Répondre

hugobiwan septembre 14, 2015 à 10:36

Très beau billet de vulgarisation. Les implications du blockchain sont éminemment politiques !! Il faudrait lui trouver un autre nom afin de pouvoir débattre sans faire fuire les « non geeks » !

Répondre

frth septembre 14, 2015 à 11:43

Très intéressant, grâce à vous j'ai enfin pris le temps de comprendre ce qu'était le bitcoin et la blockchain. Merci.
À la lecture ici et ailleurs pour compléter, je me suis demandé ce qui arrivera quand tous les bitcoins auront été minés, et qu'il n'y aura donc plus de récompenses pour les miners ? J'ai alors appris que les miners étaient aussi rétribués par les frais de transaction, et que par ailleurs, le système était pensé en partant du principe qu'à cette échéance, la masse de miners serait suffisante pour s'autoréguler (s'il y a moins de miners, les rétributions sont plus importantes). Cela pose quand même le problème de cette « masse critique » indispensable à la robustesse de la blockchain, qui n'est jamais complètement acquise, mais qui est surtout un prérequis indispensable au bon fonctionnement de tout système qui se base sur ce mécanisme, et donc un frein important au départ (il me semble).
En furetant vers les noms de la fin de votre article, et notamment en découvrant Tendermint, il apparaît que chacun est tend à développer sa propre blockchain singulière, avec ses propres Tokens, son système non-relié aux autres. Est-ce qu'il n'y a pas à craindre un morcellement infini, une multitudes de mécanismes parallèles non-connectés, aux évolutions autonomes et aux interconnexions de ce fait difficilement maîtrisables dans le temps? Comment faire fonctionner une société quand les règles des interactions sont sans cesse changeantes? Tendermint prétend déjà avoir résolu les problèmes de consensus de Bitcoin. Mais si Bitcoin est déjà « périmé » dans son mécanisme, comment pourrait-on avoir confiance dans la monnaie qu'il représente, puisque d'autres plus « optimisées » sont amenées à venir le supplanter? Cela rejoint je crois les interrogations d'Hugues plus haut.

Répondre

Christian septembre 19, 2015 à 2:19

@Hugues Bien d'accord avec toutes ces questions, et merci pour les références. Pour ma part j'essaye d'articuler la blockchain avec les conceptions politiques des techno-libetariens (qui est derrière ce quu appelles les « anarcho capitalistes »).
Je publierai bientôt une note là-dessus.

Répondre

Christian septembre 19, 2015 à 2:32

@frth Merci pour ton message.
La tendance serait de faire des blockchains privées qui inscriraient des hashs dans la blockchain publique (celle du Bitcoin). La blockchain publique serait un méta-annuaire des blockchains privées.

Répondre

Antoine octobre 2, 2015 à 10:32

Excellent article! En tout cas clair, complet et précis, c'est un bel exploit sur un sujet aussi touffu. Pour ceux que ça intéresseraient, nous tenons un blog sur l'actualité du sujet Blockchain (https://blockchainfrance.wordpress.com/). Je crois que nous allons essayer de nous inspirer de votre travail pour être aussi efficace dans la pédagogie, il y aura du travail ^^

Répondre

Houssais Gwenola janvier 31, 2016 à 6:34

Excellent article clair.
Je comprends que la Blockchain est un réseau de transaction, voir une infrastructure de certification, régulée par des mineurs (noeuds de réseaux) et que l'intégrité du système repose sur la puissance de calcul. Je comprends également que les Bitcoins miners se font rémunérer en bitcoins pour leur travail. Qui sont les miners, quel est leur mode de recrutement, quel est le business model ? Lorsqu'on parle de Blockchain publique (Ethereum) ou de Blockchain privé (Eris) en tant qu'infrastructure pour développer des applications, qui sont les mineurs, comment sont-ils rétribués, sélectionnés ?
Je vous remercie si vous pouvez m'éclairer.

Répondre

Laurent Leloup février 2, 2016 à 2:49

Christian bonjour,

Bravo pour cet article très bien ficelé et documenté : un vrai travail de synthèse !

Merci à vous

Laurent
Finyear.com

Répondre

Saxoprane juin 22, 2016 à 2:54

Il faut surtout éviter de parler de Bitcoin quand on parle de Blockchain, trop facile pour un non initié de faire l'amalgame.

Répondre

Leave a Comment

Name *

E-mail *

Website

Submit

{ 1 trackback }

- ★ ENMI 2015 Actualités

Previous post: La conteneurisation du monde

Next post: Conférence : La blockchain au delà du Bitcoin

-
-
- **Newsletter**

  Saisissez votre mail

  Envoyer

- **Nuages de mots-clefs**

  algorithme API Architecture Ars-Industrialis business_model cinéma Cloud Computing consulting contribution Dataware Derrida Digital Studies Elections-Présidentielles enregistrement entreprise Entreprise-2.0 google grammatisation humeur hypomnemata lecture management_des_connaissances milieu_associé Moteur-de-recherche mémoire ontologie participation Politique Probabilité programmation projet prolétarisation REST simondon Social-Network stiegler support_numérique système_d'information technique technologies relationnelles travail Web-2.0 Web-Sémantique économie écriture

- **Archives**

  Archives Sélectionner un mois

Get smart with the Thesis WordPress Theme from DIYthemes.

WordPress Admin