Les blockchainsÂ : une invention qui nâ€™aÂ pas dix ans

Description

Si en chimie,Â *Â« rien ne se perd, rien ne se crÃ©eÂ : tout se transforme Â»*Â [1], en informatique, tout se copie. Tout du moins jusquâ€™en 2008. Quâ€™une suite de 0 et de 1 puisse Ãªtre copiÃ©e est dâ€™ailleurs le fondement mÃªme des technologies de l'information et de la communication. Or, comme lâ€™Ã©crivent Adli Takkal Bataille et Jacques Favier dansÂ *Bitcoin, la monnaie acÃ©phale*Â [2], pour la premiÃ¨re fois depuis lâ€™invention de lâ€™informatique,Â *Â« le protocole Bitcoin a rÃ©ussi Ã crÃ©er un bien numÃ©rique non reproductible Â»*.

> Le protocole Bitcoin a rÃ©ussi Ã crÃ©er un bien numÃ©rique non reproductible
> Adli Takkal Bataille et Jacques Favier

Lorsque Satoshi Nakamoto, pseudonyme dâ€™une personne ou dâ€™un groupe, publie en novembre 2008 lâ€™articleÂ fondateurÂ *Â« BitcoinÂ : un systÃ¨me de paiement Ã©lectronique pair-Ã -pair Â»*, il proposeÂ *Â« une solution au problÃ¨me de la double dÃ©pense Â»*. En effet, le problÃ¨me majeur dâ€™une monnaie Ã©lectronique, qui par dÃ©finition peut-Ãªtre recopiÃ©e, consiste Ã sâ€™assurer quâ€™une personne ne dÃ©pensera pas deux fois la mÃªme somme dâ€™argent. Avec lâ€™invention du Bitcoin, pour la premiÃ¨re fois, la propriÃ©tÃ© dâ€™un bien numÃ©rique peut Ãªtre transfÃ©rÃ©e sans Ãªtre dupliquÃ©e ni passer par un registre centralisÃ©.

Ce que dÃ©crit exactement Satoshi Nakamoto estÂ *Â« un rÃ©seauÂ* [qui]*Â horodate les transactions en les hachant en une chaÃ®ne continue de Â«Â preuves-de-travailÂ Â», formant un enregistrement de donnÃ©es qui ne peut pas Ãªtre changÃ© sans avoir Ã refaire la Â«Â preuve-de-travailÂ Â» Â»*. Ce que lâ€™on appelle communÃ©ment aujourdâ€™huiÂ *blockchain*Â correspond en rÃ©alitÃ© Ã la combinaison de plusieurs technologiesÂ : un protocole de rÃ©seau pair-Ã -pair, le minage par la preuve de travail, la cryptographie asymÃ©trique et, enfin, uneÂ *blockchain*Â ou plus prÃ©cisÃ©ment uneÂ Â« base de donnÃ©es distribuÃ©e de typeÂ *blockchain*Â Â».

ExplicationsÂ : avoir un compte Bitcoin requiert au prÃ©alable de tÃ©lÃ©charger sur un ordinateur ou sur un smartphone unÂ Â« porte-monnaie Â»Â appelÃ© aussiÂ *wallet*. Ce porte-monnaie permet Ã un utilisateur de gÃ©nÃ©rer des adressesÂ *bitcoin*. Chaque adresse, par exemple 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa, est en rÃ©alitÃ© une paire de clÃ©s cryptographiques composÃ©e dâ€™une clÃ© privÃ©e et dâ€™une clÃ© publique. Pour recevoir desÂ *bitcoins*, un utilisateur fournira une adresse, gÃ©nÃ©rÃ©e Ã partir de sa clÃ© publique, et quâ€™il renouvellera, idÃ©alement, Ã chaque transaction. Tandis que pour envoyer desÂ *bitcoins*Â Ã lâ€™adresse du destinataire, il signera la transaction avec sa clÃ© privÃ©e.

> Pour la premiÃ¨re fois, la propriÃ©tÃ© dâ€™un bien numÃ©rique peut Ãªtre transfÃ©rÃ©e sans Ãªtre dupliquÃ©e ni passer par un registre centralisÃ©

La signature et la vÃ©rification des transactions enÂ *bitcoins*Â reposent sur la cryptographie asymÃ©trique, câ€™est-Ã -dire que la clÃ© privÃ©e permet de vÃ©rifier lâ€™authenticitÃ© dâ€™une signature Ã partir de la clÃ© publique, lâ€™inverse Ã©tant bien Ã©videmment impossible. Lâ€™ensemble des transactions enÂ *bitcoins*Â consiste ainsi Ã dÃ©biter certains comptes pour en crÃ©diter dâ€™autres. Ces transactions sont enregistrÃ©es dans des fichiers que lâ€™on appelle des blocs. Un bloc reprÃ©sente lâ€™Ã©quivalent de dix minutes de transactions, et comporte leÂ Â« rÃ©sumÃ© Â» du bloc prÃ©cÃ©dent. Pour garantir lâ€™intÃ©gritÃ© des blocs, enchaÃ®nÃ©s chronologiquement les uns aprÃ¨s les autres, depuis la premiÃ¨re transaction enÂ *bitcoin*, effectuÃ©e en 2009, le systÃ¨me utilise desÂ Â« fonctions deÂ *hash*Â Â». Une fonction deÂ *hash*Â est une fonction mathÃ©matique qui transforme nâ€™importe quel contenu sous la forme dâ€™un nombre hexadÃ©cimal.

Par exemple, le titreÂ Â« La revue europÃ©enne des mÃ©dias et du numÃ©rique Â»Â *hashÃ©*Â donneÂ Â« EDD559832CFB3B135BFAD11A0EB68D34F1C77D252140EAE01D8D3FE8EE0FBEDEÂ Â». MaisÂ Â« la revue europÃ©enne des mÃ©dias et du numÃ©rique Â», sans majuscule au dÃ©but, donneÂ Â« C39398ED08D75CC4CAA03D7FA223B3193E6212F1026021D0B1328760E5E8403C Â». Ã€ la moindre modification du contenu, le nombreÂ *hashÃ©*Â devient totalement diffÃ©rent. Il est possible deÂ *hasher*Â une phrase ou un mot de passe, tout commeÂ *Lâ€™Iliade et lâ€™OdyssÃ©e*Â *in extenso*. Lâ€™intÃ©grÃªt dâ€™une fonction deÂ *hashage*Â est quâ€™elle ne sâ€™applique que dans un sensÂ : leÂ *hash*Â obtenu ne permet ainsi pas de remonter au contenu dâ€™origine, en revanche il suffit deÂ *hasher*Â Ã nouveau ce contenu pour vÃ©rifier que leÂ *hash*Â en rÃ©sultant est identique, preuve quâ€™aucune modification nâ€™est intervenue. Les blocs du Bitcoin sont ainsiÂ *hashÃ©s*Â et permettent d’avoir la garantie quâ€™ils nâ€™ont jamais Ã©tÃ© modifiÃ©s depuis la premiÃ¨re transaction.

Comme son nom lâ€™indique, laÂ *blockchain*Â est un enchaÃ®nement de blocs, chacun contenant leÂ *hash*Â des blocs prÃ©cÃ©dents, qui regroupe des transactions. CetteÂ *blockchain*Â est synchronisÃ©e et stockÃ©e dans tous les ordinateurs de ceux qui lâ€™utilisent. Câ€™est une monnaie Ã©lectronique dÃ©centralisÃ©e. Chaque ordinateur possÃ©dant une copie de laÂ *blockchain*Â est appelÃ© unÂ Â«

nÅ“ud Â»Â du rÃ©seau et vÃ©rifie en permanence lâ€™intÃ©gritÃ© de celle-ci.

Les nouveaux blocs sont crÃ©Ã©s par certains nÅ“uds du rÃ©seau appelÃ©s les mineurs. Ils mettent Ã la disposition du systÃ¨me leur puissance de calcul pour rÃ©soudre un problÃ¨me mathÃ©matique complexe dont le principe est de trouver un nombreÂ *hashÃ©*. Comme il est impossible de retrouver le contenu original Ã partir duÂ *hash*, lâ€™ensemble des ordinateurs quiÂ Â« minent Â»Â calcule toutes les possibilitÃ©s pour arriver au rÃ©sultat. Cette opÃ©ration, appelÃ©e validation parÂ Â« preuve de travail Â»Â (*proof-of-work*), ne peut Ãªtre obtenue que par la rÃ©alisation dâ€™une tÃ¢che fortement consommatrice en Ã©nergie et en puissance de calcul.

Le systÃ¨me est conÃ§u de telle sorte quâ€™il faudrait contrÃ´ler plus de 50 %Â de la puissance de calcul de tous les ordinateurs qui minent dans le monde pour arriver Ã modifier un bloc Ã lâ€™insu de tous. Câ€™est pour cette raison que, Ã ce jour, le Bitcoin et lesÂ *blockchains*Â nâ€™ont jamais Ã©tÃ© piratÃ©es. La difficultÃ© du minage est automatiquement ajustÃ©e en fonction du nombre d’ordinateurs en train deÂ *hasher*, afin qu’un nouveau bloc soit gÃ©nÃ©rÃ© en moyenne toutes les dix minutes. Ã€ chaque fois quâ€™un ordinateur trouve la bonne rÃ©ponse, le bloc est crÃ©Ã© et le mineur est rÃ©munÃ©rÃ© 12,5Â *bitcoins*. Câ€™est de cette faÃ§on quâ€™est programmÃ©e la crÃ©ation dâ€™unitÃ©s de compteÂ *bitcoins*. Le protocole a Ã©tÃ© conÃ§u pour que lesÂ *bitcoins*Â soient crÃ©Ã©s graduellement sans quâ€™une instance centrale sâ€™en charge.

Il est Ã©galement prÃ©vu dans le code informatique que plus la chaÃ®ne croÃ®t, plus il est difficile deÂ minerÂ desÂ *bitcoins*, et plus la rÃ©munÃ©ration baisse. Câ€™est pourquoi si, aux dÃ©buts du Bitcoin, des particuliersÂ minaientÂ sur leur ordinateur, la puissance de calcul nÃ©cessaire est aujourdâ€™hui telle quâ€™ils sont supplantÃ©s par des entreprises qui font travailler des milliers de serveurs dans des entrepÃ´ts, notamment en Chine. Depuis janvier 2009, environ 16 millions deÂ *bitcoins* Â ont Ã©tÃ© Ã©mis et seuls 21 millions seront gÃ©nÃ©rÃ©s en tout et pour tout, le dernier devant Ãªtre produit en 2140.

LesÂ bases de donnÃ©es distribuÃ©es de typeÂ *blockchain*
sont Ã la transaction ce que les protocoles
TCP et IP sont Ã la transmission dâ€™information
viaÂ lâ€™internet

Par extension, laÂ Â« chaÃ®ne de blocs Â»Â peut Ãªtre assimilÃ©e Ã un grand livre des comptes, public, anonyme et infalsifiable (voirÂ *La rem*Â nÂ°37, p.67). Il est dâ€™ailleurs intÃ©ressant de noter que, pas une seule fois, le motÂ *blockchain*Â nâ€™est citÃ© dans le texte fondateur de Satoshi Nakamoto.

LesÂ bases de donnÃ©es distribuÃ©es de typeÂ *blockchain*Â sont Ã la transaction ce que les protocoles TCP et IP sont Ã la transmission dâ€™informationÂ *viaÂ* lâ€™internet. Le code informatique de la plupart desÂ *blockchains*Â publiques Ã©tantÂ *open source*, quiconque possÃ©dant les compÃ©tences

informatiques requises peut mettre en place uneÂ *blockchain*. Au-delÃ du Bitcoin, il existe aujourdâ€™hui prÃ¨s deÂ 1 150 registres distribuÃ©s de typeÂ *blockchain*Â publique, dont la convertibilitÃ© en monnaie lÃ©gale est assurÃ©e par des milliers de plates-formes de change Ã travers le monde. Lorsque lesÂ *blockchains*Â sont publiques, comme Bitcoin, Ether ou Monero, tout le monde, avec une connexion internet et un ordinateur, peut accÃ©der Ã leurs services. Lorsquâ€™elles sont privÃ©es, leur utilisation est limitÃ©e Ã certains acteurs.

> Lâ€™avÃ¨nement du pair-Ã -pair pour certifier et enclencher automatiquement des transactions ouvre des perspectives inÃ©dites

Ã€ partir du protocole Bitcoin crÃ©Ã© pour produire une base de donnÃ©es enregistrant lâ€™ensemble des transactions opÃ©rÃ©es par ses utilisateurs, une dÃ©clinaison de laÂ *blockchain*Â a Ã©tÃ© inventÃ©e en dÃ©cembre 2013 par Vitalik Buterin. BaptisÃ© Ethereum, ce protocole d'Ã©changes dÃ©centralisÃ©s permet la crÃ©ation deÂ Â« contrats intelligents Â». Il utilise Solidity, un langage de programmation dit Turing-complet, parce quâ€™il permet de programmer lâ€™ensemble des fonctions calculables au sens de Turing, Ã savoir quasiment toutes les fonctions que lâ€™on connaÃ®t des langages de programmation modernes. Ces contrats intelligents permettent de vÃ©rifier et de mettre en application des accords mutuels qui sont enregistrÃ©s et consultables publiquement dans laÂ *blockchain* Â dâ€™Ethereum. Lâ€™intÃ©rÃªt de ces contrats est quâ€™ils sont autonomes, rÃ©pliquÃ©s dans tous les nÅ“uds de laÂ *blockchain*, et que leur exÃ©cution ne passe pas par un tiers de confiance pour en garantir la validitÃ©.

Lâ€™avÃ¨nement du pair-Ã -pair, non plus simplement pour transmettre et recevoir des informations mais Ã©galement pour certifier et enclencher automatiquement des transactions, ouvre des perspectives inÃ©dites aux utilisateurs dâ€™internetÂ : particuliers, entreprises et Ã‰tats.

Les usages des bases de donnÃ©es distribuÃ©es de typeÂ *blockchain*

Il nâ€™aura fallu que quelques annÃ©es pour que de nombreuses entreprises sâ€™emparent de cette invention et appliquent Ã divers domaines, outre la banque, ce que le Bitcoin rÃ©invente pour la monnaieÂ : passer dâ€™un fonctionnement centralisÃ© Ã une organisation dÃ©centralisÃ©e. Chacune de ces entreprises dÃ©ploie des services basÃ©s sur un registre distribuÃ© dont la promesse, Ã lâ€™instar de la cryptomonnaie, repose sur lâ€™Ã©limination des tiers de confiance historiques (notaire, administration, sociÃ©tÃ© de gestion de droit dâ€™auteurâ€¦). Lâ€™utopie dont est porteur ce modÃ¨le de base de donnÃ©es peut sâ€™Ã©tendre Ã tous les domaines nÃ©cessitant un organe central ou un tiers de confiance, mais Ã©galement Ã toute activitÃ© pour laquelle des Ã©changes entre de multiples acteurs induisent de nombreux contrÃ´les, des problÃ¨mes de logistique, de lourdeur administrative et parfois de corruption.

Comme aux dÃ©buts de lâ€™automobile, lorsque la France comptait 155 constructeurs en 1914, de

nombreuses expÃ©rimentations en cours dans le monde tÃ©moignent de cet engouement pour lesÂ *blockchains*, dont lâ€™intÃ©rÃªt et lâ€™utilitÃ© des services proposÃ©s sont parfois relatifs. Selon le siteÂ blockchainfrance.net, les applications se classent en trois catÃ©goriesÂ :

- le transfert dâ€™actifs, comme des monnaies Ã©lectroniques, des titres, des actions ou des obligations ;
- la tenue dâ€™un registre, garantissant son intÃ©gritÃ© comme l'Ã©tablissement dâ€™un cadastre ou la certification de diplÃ´mes ;
- lâ€™exÃ©cution automatique de programmes autonomes, appelÃ©sÂ *smart contracts*.

Transfert dâ€™actifs

Rappelons que lâ€™article de Satoshi Nakamoto a Ã©tÃ© publiÃ© en pleine dÃ©bÃ¢cle financiÃ¨re, deux ans aprÃ¨s la crise desÂ *subprimes*Â aux Ã‰tats-Unis et au moment oÃ¹, en septembre 2008, plusieurs Ã©tablissements financiers amÃ©ricains entraient en cessation de paiement.

Câ€™est dans ce contexte que leÂ BitcoinÂ a Ã©tÃ© conÃ§u comme un systÃ¨me permettant le transfert dâ€™actifs Ã travers une monnaie Ã©lectronique entiÃ¨rement dÃ©centralisÃ©e dont les transactions sont validÃ©es et sÃ©curisÃ©es par les utilisateurs eux-mÃªmes. Dâ€™abord confidentiel, il faudra attendre 2013 pour que la spÃ©culation donne un coup de projecteur au Bitcoin, dont le cours, passÃ© de 100 Ã Â 1 000 dollars en quelques semaines, attire les foudres et les critiques des professionnels de la banque et des experts de la finance qui furent, et sont encore nombreux, Ã prÃ©dire sa mort imminente. Au-delÃ de lâ€™aspect sulfureux du Bitcoin souvent associÃ© auÂ *darknet*Â (voirÂ *La rem*Â nÂ°33, p.63), force est de constater que le transfert dâ€™actif sans passer par un organe central trouve des applications de bon sens.

Le marchÃ© du transfert dâ€™argent en est un bon exemple. Selon la Banque mondiale, ce marchÃ© va reprÃ©senter 636 milliards de dollars en 2017. Les opÃ©rateurs de transfert, comme Western Union, prennent quelque 10 %Â de commission sur chaque transaction, et encore plus lorsque les transferts concernent lâ€™Afrique, qui perd ainsi, selon lâ€™ONG Overseas Development Institute, prÃ¨s de deux milliards de dollars par an. Le transfert dâ€™argent entre particuliersÂ *viaÂ* uneÂ *blockchain*Â ferait disparaÃ®tre les commissions exorbitantes de ces intermÃ©diaires. Par exemple, la fondation Stellar, organisme sans but lucratif crÃ©Ã© en 2014 par Jed McCaled, a pour but de dÃ©velopper un rÃ©seau de paiement transfrontalier Ã faible frais, accessible Ã tous et rapide. La cryptomonnaie Ã©mise par Stellar, appelÃ©e Lumen, est directement convertie en monnaie fiduciaire locale par des banques partenaires, la compensation ainsi que le rÃ¨glement des transactions transitant par un rÃ©seau unique opÃ©rÃ© par IBM. Alors quâ€™un transfert dâ€™argent, assujetti Ã une commission calculÃ©e en pourcentage, passe par de nombreux intermÃ©diaires et prend aujourdâ€™hui plusieurs jours, une transaction entre particuliers *Â viaÂ* cetteÂ *blockchain*Â ne coÃ»te que quelques centimes et est validÃ©e en quelques minutes. La plate-forme est actuellement limitÃ©e aux paiements transfrontaliers en livres britanniques et en dollars fidjiens, mais devrait Ã lâ€™avenir concerner sept autres devises dâ€™Ã‰tats du Pacifique Sud, notamment le

dollar australien, le dollar nÃ©o-zÃ©landais et le pa'anga des Tonga.

Les transactions sont validÃ©es et sÃ©curisÃ©es par les utilisateurs eux-mÃªmes

Le transfert dâ€™actifs ne concerne pas uniquement les particuliers. Depuis lâ€™automne 2015, les banques et les institutions financiÃ¨res considÃ¨rent lesÂ *blockchains*Â comme une opportunitÃ© pour Ã©conomiser dâ€™importants frais liÃ©s au transfert dâ€™argent. R3 est Ã la fois une start-up amÃ©ricaine crÃ©Ã©e en septembre 2015 et un consortium regroupant neuf banques Ã son lancement, parmi lesquelles Barclays, CrÃ©dit Suisse, Goldman Sachs, JP Morgan (qui a depuis quittÃ© le consortium) ou encore la Royal Bank of Scotland. Rejointes sans plus attendre par dâ€™autres institutions financiÃ¨res dont la SociÃ©tÃ© GÃ©nÃ©rale, BNP Paribas ou encore Natixis, ce sont aujourdâ€™hui quelque 80 Ã©tablissements financiers du monde entier qui mÃ¨nent de concert des travaux portant sur lesÂ *blockchains*. Il sâ€™agit, non plus deÂ *blockchains*Â publiques et ouvertes Ã tous, mais deÂ *blockchains*Â privÃ©es, oÃ¹ les nÅ“uds du rÃ©seau sont prÃ©dÃ©terminÃ©s. Si la perspective de rÃ©duction des coÃ»ts pour le secteur bancaire, jusquâ€™Ã 20 milliards de dollars par an, a fait rÃªver plus dâ€™un directeur dâ€™institution financiÃ¨re, des tensions liÃ©es Ã la gouvernance, la concurrence entre les acteurs et lâ€™absence de rÃ©sultat immÃ©diatement opÃ©rationnel ont dÃ©jÃ provoquÃ© le dÃ©part de certains. Dâ€™autres initiatives existent, par exemple celle dâ€™UBS, Deutsche Bank, BNY Mellon et Santander, qui souhaitent lancer lâ€™Utility Settlement Coin en 2018, dont le fonctionnement sâ€™inspirerait de laÂ *blockchain*Â Bitcoin. MaisÂ *Â« il s'agit plutÃ´t d'une nouvelle architecture IT permettant de faire de la compensation et du rÃ¨glement plus rapidement Â»*, explique Gonzague Grandval, cofondateur de Paymium.

La tenue dâ€™un registre

Les bases de donnÃ©es distribuÃ©es de typeÂ *blockchain*Â trouvent Ã©galement, comme domaine de prÃ©dilection, la tenue dâ€™un registre infalsifiable et transparent, par exemple, pour lâ€™Ã©tablissement dâ€™un cadastre ou pour la certification des diplÃ´mes.

Au Honduras, le gouvernement a inscrit dans uneÂ *blockchain*Â publique lâ€™intÃ©gralitÃ© des titres fonciers du territoire afin dâ€™Ã©viter lâ€™appropriation unilatÃ©rale des terres par certains, et garantir aux yeux de tous que le cadastre ne soit pas modifiÃ© ou altÃ©rÃ©. Au Ghana, une initiative similaire, menÃ©e par lâ€™ONG Bitland, permet dâ€™enregistrer les actes fonciers associÃ©s Ã des coordonnÃ©es GPS qui, une fois inscrits dans uneÂ *blockchain*Â appelÃ©e Bitshare, sont immuables sans un transfert de propriÃ©tÃ© en bonne et due forme. Depuis 2016 en GÃ©orgie, lâ€™initiative est directement portÃ©e par le gouvernement, avec le concours de lâ€™entreprise Bitfury. Loin dâ€™Â« uberiser Â»Â les notaires, ces initiatives prennent forme dans des pays oÃ¹ lâ€™absence de cadastre et de services notariÃ©s, ainsi quâ€™un haut niveau de corruption, incitent des start-up Ã proposer ce genre de services ou les Ã‰tats eux-mÃªmes Ã mettre en place un cadastre inviolable.

RÃ©guliÃ¨rement dÃ©noncÃ©e par les Ã©coles et par les entreprises, la fraude au diplÃ´me serait un flÃ©au en constante progression. Pour ne citer quâ€™un seul cas tristement cÃ©lÃ¨bre, Gilles Bernheim, grand rabbin de France, a reconnu avoir menti sur son CV, en 2015, en usurpant le titre dâ€™agrÃ©gÃ© de philosophie, mentionnÃ© dans toutes ses biographies. Des entreprises, comme Verifdiploma fondÃ©e en 2000, se sont lancÃ©es sur ce crÃ©neau dâ€™authentification des diplÃ´mes et autres certificats dâ€™un candidat. Une des solutions mises en Å“uvre par lâ€™ESILV (Ã‰cole supÃ©rieure dâ€™ingÃ©nieurs LÃ©onard de Vinci) en partenariat avec la sociÃ©tÃ© Paymium en France, ou par lâ€™Ã‰cole dâ€™ingÃ©nieurs Holberton Ã San Francisco, aux Ã‰tats-Unis, avec la sociÃ©tÃ© Bitproof, a Ã©tÃ© dâ€™enregistrer la signature de chaque diplÃ´me dans laÂ *blockchain*Â Bitcoin et de tenir ainsi Ã jour le registre de leurs diplÃ´mÃ©s.

> Lâ€™exÃ©cution automatique de programmes autonomes, appelÃ©sÂ *smart contracts*, est lâ€™un des domaines les plus prometteurs

Il est, Ã la fois, extrÃªmement difficile de falsifier un tel registre, qui horodate par ordre chronologique lâ€™ensemble des diplÃ´mes Ã©mis par lâ€™Ã©cole et trÃ¨s simple pour une entreprise de vÃ©rifier dans ce mÃªme registre si un candidat est bel et bien diplÃ´mÃ© de ladite Ã©cole. En France, le ministÃ¨re de lâ€™Ã©ducation nationale et le rectorat devraient sâ€™emparer du sujet au plus vite afin de moderniser le RÃ©pertoire national des certifications professionnelles (RNCP), registre des diplÃ´mes reconnus par lâ€™Ã‰tat, ce qui permettrait de les distinguer facilement de ceux qui ne le sont pas. Serait en mÃªme temps crÃ©Ã©e uneÂ *blockchain*Â publique dans laquelle les Ã©coles et les universitÃ©s inscriraient leurs diplÃ´mÃ©s, cette base de donnÃ©es pouvant Ãªtre consultÃ©e par tous les employeurs de France ou de lâ€™Ã©tranger.

LesÂ *smart contracts*

Lâ€™exÃ©cution automatique de programmes autonomes, appelÃ©sÂ *smart contracts*, est lâ€™un des domaines les plus prometteurs des bases de donnÃ©es distribuÃ©es de typeÂ *blockchain*. Il ne sâ€™agit

plus simplement de transfert dâ€™actifs ou de la tenue dâ€™un registre mais de rendre possible le dÃ©veloppement dâ€™organisations autonomes dÃ©centralisÃ©es. Dans chaque nÅ“ud du rÃ©seau Ethereum est installÃ©e une EVM (Ethereum Virtual Machine), dont lâ€™objet est dâ€™exÃ©cuter automatiquement les conditions et les termes de contrat, sans nÃ©cessiter dâ€™intervention humaine, une fois lancÃ©s. Pour ne citer quâ€™un seul exemple, la mise en Å“uvre dâ€™une organisation autonome dÃ©centralisÃ©e de transport entre particuliers permettrait Ã leurs utilisateurs â€“ conducteurs et personnes souhaitant se dÃ©placer â€“ dâ€™Ã©tablir un contrat, sans passer par un tiers de confiance, et de garantir le paiement. De fait, Ã tous les services leaders du web, nouveaux intermÃ©diaires des temps modernes, correspondent un ou plusieurs projets concurrents dâ€™organisation autonome dÃ©centralisÃ©e. Ainsi, LaZooz ou Arcade City, services de transport entre particuliers, concurrenceraient Uber ou Blablacar. Storj rivaliserait dans les services deÂ *cloudÂ computing*Â avec DropBox. OpenBazaar deviendrait un site de petites annonces comme Craigslist. Slockit relie des objets physiques au rÃ©seau Ethereum afin dâ€™interagir avec eux Ã travers desÂ *smart contracts*Â : une serrure dâ€™appartement connectÃ©e lui permettrait de concurrencer AirBnB.

Au-delÃ Â Â« dâ€™uberiser Â»Â Ã leur tour les nouveaux intermÃ©diaires du web, la diversitÃ© des applications mises en Å“uvre Ã travers ces organisations autonomes dÃ©centralisÃ©es semble sans limite. Dans le domaine de la logistique et de la traÃ§abilitÃ© par exemple, la start-up Everledger utilise uneÂ *blockchain*Â pour combattre la fraude dans l’industrie du diamant. Des start-up ont dÃ©jÃ mis en place un systÃ¨me de vote, inviolable et infalsifiable. En France, laprimaire.org, initiative citoyenne organisÃ©e en dehors de tout parti politique traditionnel, a utilisÃ© la plate-forme Ethereum pour organiser le vote de son candidat Ã lâ€™Ã©lection prÃ©sidentielle 2017. Ainsi a peut-Ãªtre Ã©tÃ© inventÃ© lâ€™un des futurs outils politiques au service de la dÃ©mocratie.

Dans les domaines de la production dâ€™Ã©nergie solaire, de lâ€™assurance ou de la gestion des droits dâ€™auteur, lâ€™utilisation deÂ *smart contracts*Â apporterait une transparence et une confiance, qui font parfois dÃ©faut, tout en inventant des services dâ€™un genre inÃ©dit.

La production dâ€™Ã©nergie solaireÂ â€“ LeÂ *Solarcoin*Â est une monnaie Ã©lectronique adossÃ©e Ã la production dâ€™Ã©nergie solaire, crÃ©Ã©e par la Fondation SolarCoin en 2014. Câ€™est un programme de rÃ©compense, Ã lâ€™instar desÂ *miles*Â des compagnies aÃ©riennes ou ferroviaires, qui vise Ã encourager la production dâ€™Ã©nergie solaire photovoltaÃ¯que Ã travers le monde. Les dÃ©tenteurs dâ€™installations photovoltaÃ¯ques peuvent Ãªtre rÃ©munÃ©rÃ©s en monnaie Ã©lectronique sur la base dâ€™unÂ *Solarcoin*Â pour un mÃ©gawattheure produit. Cette monnaie peut ensuite Ãªtre utilisÃ©e entre les partenaires du projet, comme le franÃ§ais ekWateur (prononcer Ã©quateur), premier fournisseur dâ€™Ã©nergie franÃ§ais Ã accepter le paiement de sa consommation dâ€™Ã©nergie enÂ *Solarcoins*. Lâ€™utilisation dâ€™uneÂ *blockchain*Â permet de certifier lâ€™origine de la production dâ€™Ã©nergie solaire.Â *Â« Les panneaux photovoltaÃ¯ques des participants sont munis de capteurs qui envoient dans laÂ* blockchain*Â les informations sur les quantitÃ©s d’Ã©lectrons produitesÂ : quand, par quel panneau photovoltaÃ¯que de quel membre du rÃ©seau, et ce dernier reÃ§oit lesÂ* SolarCoins*Â correspondants. Le tout est consultable par tous les participants. Il n’y a pas de serveur central ni d’autoritÃ© rÃ©gulatrice, car dÃ¨s lors qu’une personne intÃ¨gre ce rÃ©seau, laÂ*

blockchain*Â se tÃ©lÃ©charge sur son ordinateur Â»*. Autre partenaire de la Fondation SolarCoin, Lumo est une plate-forme d'Ã©pargne participative consacrÃ©e aux Ã©nergies renouvelables, dont lâ€™objectif est de populariser lesÂ *SolarCoins*Â et dâ€™en multiplier le nombre de dÃ©tenteursÂ :Â *Â« tous ceux qui auront participÃ© au financement d'une centrale solaire recevront desÂ* SolarCoins*Â Â»*, explique Alex Raguet, cofondateur de Lumo.

Les assurancesÂ â€“ Les assureurs sâ€™intÃ©ressent Ã©galement auxÂ *smart contracts*, notamment dans le domaine de lâ€™assurance dite paramÃ©trique ou indicielle. EncouragÃ© par la Banque mondiale pour couvrir les agriculteurs des pays en voie de dÃ©veloppement, ce type de contrats dâ€™assuranceÂ intelligents, Ã©galement disponible sur les marchÃ©s matures, consiste Ã enclencher une indemnisation dÃ¨s lors quâ€™une anomalie mÃ©tÃ©orologique est constatÃ©e. Par exemple, un agriculteur souscrit une assurance stipulant quâ€™une indemnisation sera versÃ©e aprÃ¨s 30 jours de sÃ©cheresse. Lorsque lâ€™Ã©vÃ©nement se produit, lâ€™agriculteur est automatiquement indemnisÃ©, sans avoir Ã faire de dÃ©claration auprÃ¨s de son assureur.

Axa Assurances a rÃ©cemment lancÃ© une offre deÂ *smart contract*Â sur laÂ *blockchain* Â dâ€™Ethereum, visant Ã indemniser les retards dâ€™avion de plus de deux heures. La souscription de lâ€™offre sâ€™effectue en ligne quinze jours avant le dÃ©part. Le contrat est reliÃ© aux bases de donnÃ©es de Flightstats, recensant le trafic aÃ©rien mondial. DÃ¨s quâ€™un vol a deux heures de retard, lâ€™indemnisation de lâ€™assurÃ© est dÃ©clenchÃ©e automatiquement, sans que lâ€™assureur ait de dÃ©claration de sinistre Ã traiter. Actuellement testÃ©e sur les vols transatlantiques directs entre lâ€™aÃ©roport Paris Charles-de-Gaulle et les Ã‰tats-Unis, lâ€™offre a vocation Ã sâ€™Ã©tendre au reste du monde dÃ¨s 2018.

En avril 2017, Spotify a annoncÃ© avoir rachetÃ© la start-up Mediachain Labs, qui dÃ©ploie une solution deÂ *smart contracts*

Les droits dâ€™auteurÂ â€“ La gestion des droits dâ€™auteur est un casse-tÃªte pour lâ€™industrie musicale, tout particuliÃ¨rement aux Ã‰tats-Unis oÃ¹ les services deÂ *streaming*Â rencontrent de plus en plus de succÃ¨s. Le suÃ©dois Spotify, leader mondial, est frÃ©quemment attaquÃ© pour non-respect du versement des droits dâ€™auteur. Au terme dâ€™une longue bataille judiciaire aux Ã‰tats-Unis, lâ€™entreprise a finalement dÃ» reverser en mars 2016 plus de vingt millions de dollars Ã la National Music Publishersâ€™Association (NMPA), selon laquelle plus de 25 %Â des Ã©coutes sur Spotify Ã©taientÂ Â« sans licence Â». En avril 2017, Spotify a annoncÃ© avoir rachetÃ© la start-up Mediachain Labs, qui dÃ©ploie une solution deÂ *smart contracts*Â sur laÂ *blockchain*Â dâ€™Ethereum, afin de gÃ©rer finement les droits dâ€™auteur attachÃ©s Ã un artiste. Le service rendrait transparente lâ€™attribution dâ€™une Å“uvre Ã©coutÃ©e sur la plate-forme Ã tel ou tel artiste et dÃ©clencherait automatiquement le paiement des droits dâ€™auteur.

Ã‰galement en avril 2017, trois des plus importantes sociÃ©tÃ©s de gestion de droits dâ€™auteur au

monde, la Sacem (SociÃ©tÃ© des auteurs compositeurs et Ã©diteurs de musique), lâ€™Ascap (American Society for Composers Authors and Publishers) et PRS for Music (Performing Right Society for Music) ont annoncÃ© travailler ensemble Ã la mise en Å“uvre dâ€™un prototype deÂ *Â« gestion partagÃ©e des informations relatives aux droits dâ€™auteur Â»*. Ce prototype sâ€™appuie sur laÂ *blockchain*Â *open source* Â du consortium privÃ© Hyperledger, chapeautÃ© par la Fondation Linux, qui rÃ©unit vingt-sept entreprises, notamment IBM, SAP, Fujitsu, GE, Hitachi et Huawei. Le prototype de gestion des droits dâ€™auteur reposera sur le projet Hyperledger Fabric, auquel IBM a grandement contribuÃ©, et qui est un concurrent desÂ *smart contracts*Â proposÃ©s par Ethereum. CetteÂ *blockchain*Â privÃ©e permettra dâ€™associer Ã chaque morceau une signature contenant les informations liÃ©es aux droits dâ€™auteur et, Ã terme, de crÃ©er unÂ *Â« registre mondial des droits dâ€™auteur Â»*.

> Le 5 octobre 2009, date Ã laquelle est publiÃ© le premier taux de change *bitcoin*/dollar, unÂ *bitcoin*Â vaut 0,001 dollar.
> Le 21 octobre 2017, il vaut 6 100Â dollars.

Dâ€™abord utilisÃ©e comme registre, laÂ *blockchain*Â pourrait Ã terme Ãªtre assortie deÂ *smart contracts*Â utiles pour affecter trÃ¨s prÃ©cisÃ©ment les droits dâ€™auteur Ã chaque Å“uvre.Â *Â« Un artiste pourra demander une rÃ©munÃ©ration pour une diffusion de sa musique Ã la radio, ne pas en demander aux boÃ®tes de nuit et demander un prix moins Ã©levÃ© aux particuliers. Il pourrait aussi ne pas faire payer des sites deÂ* streaming*Â qui ont une approche Ã©thique. Enfin, laÂ* blockchain*Â et lesÂ* smart contracts*Â permettent de diffÃ©rencier la rÃ©partition des droitsÂ :Â 5 %Â Ã tel musicien,Â 2 %Â Ã tel autre Â»*Â explique ClÃ©ment Jeanneau, cofondateur de Blockchain France.

Lâ€™univers desÂ *blockchains*Â laisse prÃ©sager autant de perspectives quâ€™il relÃ¨ve dÃ©jÃ dâ€™innombrables dÃ©fis. La spÃ©culation dont les cryptomonnaies font lâ€™objet impressionne. Le 5 octobre 2009, date Ã laquelle est publiÃ© le premier taux de changeÂ *bitcoin*/dollar, unÂ *bitcoin*Â vaut 0,001 dollar. Le 21 octobre 2017, il vautÂ 6 100Â dollars. Inexistante en 2008, la capitalisation totale des cryptomonnaies avoisine, Ã lâ€™heure oÃ¹ cet article est Ã©crit, 173 milliards de dollars, et 4 milliards de dollars en valeur sont Ã©changÃ©s quotidiennement sur les places de marchÃ©. Ã€ lui seul, leÂ *bitcoin* Â reprÃ©sente la moitiÃ© de la valorisation totale des cryptomonnaies.

Breveter lâ€™*open source*

Le fonctionnement de lâ€™internet repose sur des logiciels et protocolesÂ *open source*, comme TCP et IP. Le protocole Bitcoin est Ã©galementÂ *open source*. Cela nâ€™empÃªche pas certains acteurs de dÃ©poser des demandes de brevets. Aux Ã‰tats-Unis, lâ€™US Patent and Trademark Office (USPTO) a dÃ©jÃ enregistrÃ© 220 brevets entre 2013 et 2016. Les banques et les Ã©tablissements financiers, comme Morgan Stanley, Accenture, Bank of America ou encore Goldman Sachs, comptent parmi les dÃ©posants les plus actifs. En 2016, lâ€™Australien Craig Wright sâ€™est prÃ©sentÃ© comme Ã©tant

le crÃ©ateur du Bitcoin, sans toutefois en apporter la preuve irrÃ©futable. Il a depuis constituÃ© un portefeuille de demandes dâ€™une centaine de brevets auprÃ¨s de lâ€™Office britannique de la propriÃ©tÃ© intellectuelle. Il semblerait que Craig Wright tente de breveter chaque Ã©lÃ©ment de toute base de donnÃ©es distribuÃ©e. Il faudra attendre plusieurs annÃ©es avant que ces brevets soient enregistrÃ©s ou rejetÃ©s.

LesÂ *ICO*

Par nature accessibles Ã quiconque installe le logiciel Bitcoin sur son ordinateur ou son smartphone, les cryptomonnaies sont actuellement utilisÃ©es par des start-up pour lever des fonds, concurrenÃ§ant les professionnels du capital-risque, au point de dÃ©passer en valeur leur fonds dâ€™amorÃ§age. Si les introductions en Bourse, en anglaisÂ *Initial Public Offering*Â (*IPO*), sont extrÃªmement rÃ©glementÃ©es et dÃ©terminent la cotation de titres de capital dâ€™une entreprise sur un marchÃ© boursier, leur Ã©quivalent dans lâ€™univers des cryptomonnaies, lesÂ *ICO*Â *(Initial Coin Offering)Â* ne le sont pas du tout. UneÂ *ICO*Â correspond Ã une levÃ©e de fonds directement auprÃ¨s des internautes qui Ã©changent desÂ *tokens*, actif numÃ©rique correspondant Ã un droit liÃ© au service lancÃ©, contre des cryptomonnaies, principalement desÂ *bitcoins*Â et desÂ *ethers*, soit lâ€™Ã©quivalent de 14 millions de dollars en 2015, 222 millions en 2016 et plus de 1,2 milliard sur les six premiers mois de 2017, dont la moitiÃ© sur les 30 derniers jours de ce semestre, selon le bureau de recherche indÃ©pendant Autonomous. Ã€ lui seul, le projet Tezos, qui se place en concurrent de laÂ *blockchain*Â dâ€™Ethereum, a levÃ© lâ€™Ã©quivalent de 232 millions de dollars.

Piratage et arnaques

LesÂ *smart contracts*Â dÃ©veloppÃ©s sur Ethereum et lesÂ *ICO*Â ont fait lâ€™objet dâ€™importants dÃ©tournements sans pour autant quâ€™une seuleÂ *blockchain*Â se soit dÃ©jÃ fait piratÃ©e. En juin 2016, une faille de sÃ©curitÃ© dans une application construite sur Ethereum a provoquÃ© le dÃ©tournement de 50 millions de dollars (voirÂ *La rem*Â nÂ°40, p.29). PlusieursÂ *ICO*Â ont Ã©galement fait lâ€™objet de dÃ©tournements, toujours spectaculaires, comme celle de CoinDash, le 17 juillet 2017. Un individu a piratÃ© le site web de la sociÃ©tÃ©, le jour du lancement de lâ€™*ICO*Â en remplaÃ§ant lâ€™adresse Ethereum de CoinDash, Ã laquelle les intÃ©ressÃ©s Ã©taient censÃ©s envoyer leur cryptomonnaie, par sa propre adresse Ethereum. Durant les trois premiÃ¨res minutes, le temps que les organisateurs se rendent compte du problÃ¨me, 8 millions de dollars avaient Ã©tÃ© dÃ©tournÃ©s.

De tels flux monÃ©taires nâ€™ont pas manquÃ© dâ€™alerter les institutions financiÃ¨res chargÃ©es de la rÃ©gulation des monnaies lÃ©gales. En effet, lâ€™absence de cadre rÃ©glementaire a laissÃ© foisonner bon nombre dâ€™arnaques, mais aussi des levÃ©es de fonds phÃ©nomÃ©nales au profit de sociÃ©tÃ©s nâ€™ayant parfois rien proposÃ© dâ€™autre quâ€™une prÃ©sentation Powerpoint et une vidÃ©o dâ€™autopromotion. Pour ne citer quâ€™un exemple, le projet Eros.Vision, qui se prÃ©sentait comme lâ€™Â« Uber de la prostitution Â», a pu bÃ©nÃ©ficier dâ€™une importante mÃ©diatisation, y compris en FranceÂ *via*Â le trimestrielÂ *Usbek & Rica*Â et la radio BFM, et lever lâ€™Ã©quivalent de 19

millions de dollars avant de disparaÃ®tre quelques jours plus tard.

Des rÃ©gulations tÃ¢tonnantes

Les cryptomonnaies sont par nature transfrontaliÃ¨res. Si des pays se sont emparÃ©s de la question, comme la Chine, les Ã‰tats-Unis, le Japon, la CorÃ©e du Sud, ainsi que certains pays europÃ©ens, il nâ€™en reste pas moins quâ€™ils alternent entre, dâ€™un cÃ´tÃ©, une interdiction pure et simple desÂ *ICO*Â et des places de marchÃ© ouvertes au public, et de lâ€™autre, une absence totale de rÃ©gulation. Le 1er Â avril 2017, le Japon a reconnu leÂ *bitcoin*Â comme instrument de paiement, tout en rÃ©gulant,*Â viaÂ* la Department and Financial Services Agency (FSA), les places de marchÃ© ouvertes au public sur lesquelles sâ€™effectue le change de ces monnaies Ã©lectroniques en monnaies nationales.

La dÃ©valuation du yuan ayant provoquÃ© dâ€™importants transferts dâ€™argent vers les cryptomonnaies, la Chine a purement et simplement interdit lesÂ *ICO*Â et les places de marchÃ© le 1er Â octobre 2017, sÃ»rement pour pouvoir mettre en Å“uvre une rÃ©gulation Ã lâ€™Ã©chelle du pays. La CorÃ©e du Sud a fait la mÃªme annonce. En mars 2017, aux Ã‰tats-Unis, la SEC (Securities and Exchange Commission) a refusÃ© Ã lâ€™agence Winklevoss Bitcoin Trust, Ã©tablie Ã Wilmington en Californie, lâ€™autorisation de crÃ©er un fonds indiciel cotÃ© en Bourse en expliquant queÂ *Â« le marchÃ© duÂ* bitcoin*Â nâ€™est pas suffisamment rÃ©gulÃ© pour faire face aux fraudes et aux cyberattaques, dont il a dÃ©jÃ Ã©tÃ© victime plusieurs fois depuis sa crÃ©ation, et lâ€™absence dâ€™une Banque centrale ou dâ€™institution de rÃ©fÃ©rence en fait une proie idÃ©ale pour les spÃ©culateurs et la formation de bulles Â»*. En rÃ©ponse Ã une question posÃ©e par la Commission des affaires Ã©conomiques et monÃ©taires du Parlement europÃ©en, le prÃ©sident de la Banque centrale europÃ©enne, Mario Draghi, a dÃ©clarÃ© en septembre 2017Â *Â« quâ€™il nâ€™Ã©tait pas dans son pouvoir dâ€™interdire ou rÃ©guler leÂ* bitcoin*Â Â»*.

> Il est intÃ©ressant de voir combien lâ€™invention de lâ€™internet et celle du Bitcoin se ressemblent Ã bien des Ã©gards

En France, le TrÃ©sor public va proposer Ã lâ€™automne 2017 un projet dâ€™ordonnance pour faciliter la transmission de certains titres financiersÂ *Â« au moyen de la technologieÂ* blockchain*Â Â»*, afin de leur garantir un cadre rÃ©glementaire. Les minibons (anciennement appelÃ©sÂ Â« bons de caisse Â», instrument financier entre le prÃªt et lâ€™obligation) associÃ©s Ã uneÂ *blockchain*Â bÃ©nÃ©ficient dÃ©jÃ dâ€™une assise lÃ©gale en droit franÃ§ais, Ã la suite de lâ€™ordonnance du 28 avril 2016 prise en application de la loi Macron du 6 aoÃ»t 2015. Chaque Ã‰tat va ainsi sâ€™assurer dâ€™apporter ou non, selon le type deÂ *blockchain*, un cadre rÃ©glementaire ou, Ã lâ€™inverse, mettre en place un dispositif dâ€™interdiction de ces registres distribuÃ©s.

De mÃªme quâ€™il Ã©tait impossible dâ€™imaginer le dÃ©veloppement des services offerts par lâ€™internet Ã la naissance du rÃ©seau, il serait vain de parier sur les usages et services Ã naÃ®tre desÂ *blockchains*

. Il est cependant intÃ©ressant de voir combien lâ€™invention de lâ€™internet et celle du Bitcoin se ressemblent Ã bien des Ã©gards. Tous deux sont indissociables dâ€™un contexte politique et social sous tension et dâ€™une effervescence idÃ©ologique qui se rÃ©clame d'une doctrine de libertÃ© absolue. Ã€ la naissance de lâ€™internet dans les annÃ©es 1960 et 1970 correspond le contexte politique de la guerre du Vietnam, de lâ€™assassinat de John Fitzgerald Kennedy et du dÃ©veloppement des mouvements pacifistes amÃ©ricains, au cours desquels de nombreux universitaires et chercheurs vont contribuer Ã rÃ©flÃ©chir Ã de nouvelles utopies dans un climat de plus en plus libertaire. Quant au Bitcoin, son contexte gÃ©opolitique est celui de la plus grande crise financiÃ¨re que le monde ait connu depuis 1929, marquÃ© par une perte de confiance envers les banques, les institutions et les Ã‰tats, dont les plans de sauvetage puis de relance et enfin dâ€™austÃ©ritÃ© ont fait exploser les dettes publiques et aggravÃ© encore davantage la progression du chÃ´mage comme l'accroissement des inÃ©galitÃ©s dans les pays matures.

Lâ€™internet et le Bitcoin nâ€™ont pas Ã©tÃ© crÃ©Ã©sÂ *ex nihilo*, ils sont au contraire lâ€™aboutissement de recherches et de tÃ¢tonnements aux filiations diverses. Pour lâ€™internet, ce sont des intÃ©rÃªts parfois trÃ¨s Ã©loignÃ©s entre lâ€™ArmÃ©e, les Ã‰tats, les entrepreneurs et les chercheurs. Le rÃ©seau de rÃ©seaux est le fruit dâ€™un assemblage dâ€™innovations disparates, comme celle du FranÃ§ais Louis Pouzin qui, en inventant en France Clyclade, premier rÃ©seau Ã commutation de paquets, va permettre quelques annÃ©es plus tard Ã Vinton Cerf de mettre au point les protocoles TCP/IP, au cÅ“ur du fonctionnement de lâ€™internet. De la mÃªme maniÃ¨re, le Bitcoin sâ€™inspire des travaux de cryptographie proposÃ©s dans les annÃ©es 1990 par Haber et Stornetta, ou encore de Nick Szabo, informaticien, juriste et cryptographe, qui a proposÃ© dÃ¨s 2005 un systÃ¨me dâ€™Ã©change monÃ©taire basÃ© sur la validation par la preuve de travail, dont sâ€™est probablement inspirÃ© le [ou les] dÃ©nommÃ©(s) Satoshi Nakamoto.

> Il nâ€™aura fallu que trente ans pour transformer profondÃ©ment la pensÃ©e libertarienne de lâ€™internet

Enfin, un autre dÃ©nominateur commun entre lâ€™internet et les registres distribuÃ©s de typeÂ *blockchain*Â repose sur leur architecture, tous deux ayant des protocolesÂ *open source*Â et fonctionnant en pair-Ã -pair. Qui aurait pu imaginer le dÃ©veloppement du rÃ©seau internet et de ses services comme le web, leÂ *mail*Â ou le pair-Ã -pair, puis des plates-formes comme Facebook, Google ou Amazon. Il nâ€™aura fallu que trente ans pour transformer profondÃ©ment la pensÃ©e libertarienne de lâ€™internet, et pour que le rÃªve initial de Norbert Wiener, J.C.R. Licklider, Robert Taylor et bien dâ€™autres â€“ crÃ©er un outil citoyen de participation active et de crÃ©ativitÃ© dÃ©cuplÃ©e par lâ€™interaction â€“ engendre dans le mÃªme temps une surveillance de masse oÃ¹ les donnÃ©es personnelles sont devenues le pÃ©trole du XXI[e]Â siÃ¨cle. Et gare Ã ceux qui, vingt ans plus tard, tenteront de sâ€™en rÃ©clamer encore, comme Aaron Swartz qui lutta pourÂ *Â« la libertÃ© dâ€™internet et pour faire de la connaissance une donnÃ©e aussi largement et gratuitement accessibleÂ [3]Â Â»*. Il nâ€™aura mÃªme pas fallu dix ans pour que cette mÃªme idÃ©ologie, au fondement du Bitcoin, soit reprise par le secteur financier, quâ€™une

avalanche de dÃ©pÃ´ts de brevets prÃ©voit dâ€™en parasiter le dÃ©veloppement Ã moyen terme, et que de nombreux Ã‰tats tentent de rÃ©guler les places de marchÃ© grand public. Pour autant, lâ€™idÃ©ologie de rupture, dont sont porteuses les bases de donnÃ©es distribuÃ©es de typeÂ *blockchain*, sâ€™inscrit dans des initiatives bien au-delÃ du secteur financier et du transfert dâ€™actifs, par exemple dans les domaines de la traÃ§abilitÃ© alimentaire, de lâ€™industrie pharmaceutique, de la distribution dâ€™Ã©nergie, de la certification dâ€™identitÃ© et potentiellement, dans tous les domaines susceptibles de passer dâ€™une autoritÃ© de confiance institutionnelle Ã une confiance distribuÃ©e Ã travers un rÃ©seau de pairs.

> Il nâ€™aura mÃªme pas fallu dix ans pour que cette mÃªme idÃ©ologie, au fondement du Bitcoin, soit reprise par le secteur financier

LesÂ *blockchains*Â vont-ellesÂ Â« uberiser Â»Â Uber ? Permettront-elles au contraire de corriger les excÃ¨s de lâ€™uberisation ? Se substitueront-elles Ã lâ€™organisation Ã la fois centralisÃ©e et pyramidale qui rÃ©git nos institutions ? Insuffleront-elles la volontÃ© politique dâ€™introduire deÂ Â« lâ€™horizontalitÃ© Â»Â comme instrument pourÂ *Â« faire appliquer les rÃ¨gles de droit lÃ oÃ¹ la loi nâ€™arrive pas, Ã elle seule, Ã protÃ©ger les droits fondamentaux des citoyens Â»*Â [3], mais Ã©galement, pour assurer une transparence dans des chaÃ®nes de valeur complexes et souvent opaques parce quâ€™humaines et motivÃ©es par des intÃ©rÃªts parfois divergents ? Ã€ nâ€™en pas douter, des mÃ©ta-organisations inÃ©dites, dÃ©centralisÃ©es et autonomes, sont probablement en gestation parmi le millier dâ€™initiatives dans le monde sâ€™appuyant sur les bases de donnÃ©es distribuÃ©es de typeÂ *blockchain*. Et nul ne sait ce quâ€™il adviendra si ce nâ€™est que, dorÃ©navant, la boÃ®te de Pandore est ouverte.

[1] Antoine-Laurent de Lavoisier.

[2] *Bitcoin, la monnaie acÃ©phale*, Adli Takkal Bataille et Jacques Favier, CNRS Ã‰ditions, 2017.

[3] *AbÃ©cÃ©daire des architectures distribuÃ©es*, CÃ©cile MÃ©adel, Francesca Musiani (coord.), Presses des Mines, 2015.

SourcesÂ :

- *Les tÃ©lÃ©communications entre bien public et marchandises*, Laurent Chemla, Ã‰ditions Charles LÃ©opoldMayer, 2005.
- Â« La Blockchain, au-delÃ du Bitcoin Â», Goofy, framablog.org, 30 janvier 2016.
- Â« Introduction (non technique) Ã la Â«Â blockchainÂ Â» Â», LinkedIn.com, Romain Rouphael, 1er Â avril 2016.
- Â« Lumo intÃ¨gre le projet blockchain ElectriCChain, distributeur de la monnaie Â«Â SolarCoinÂ Â» Â», Delphine Sibony, Lumo-france.com, 2 juin 2016.
- Â« La Blockchain dÃ©cryptÃ©e, les clefs dâ€™une rÃ©volution Â», Blockchain France, Netexplo

Obervatory, mai 2016.
- Â« Quand le crowdfunding sâ€™allie Ã lâ€™Ã©nergie solaire et Ã la blockchain Â», Dominique Pialot, Latribune.fr, 9 juin 2016.
- Â« La Blockchain, ou la confiance distribuÃ©e Â», Yves Caseau, Serge Soudoplatoff, Fondation pour l'innovation politique, juin 2016.
- Â« Vote Ã©lectroniqueÂ : la blockchain Ã la rescousse ? Â», Louis Adam, ZDNet.fr, 22 mars 2017.
- Â« Pourquoi lâ€™industrie musicale a besoin de la blockchain Â», Paul LoubiÃ¨re, Challenges.fr, 14 avril 2017.
- Â« La Blockchain au secours des droits musicaux Â», T.B.,Â *Ecran total*, nÂ° 1144, 8 mai 2017.
- Â« #Token Mania Â», Lex Sokolin, Autonomous Next, juillet 2017.
- Â« AssuranceÂ : les premiÃ¨res offres fondÃ©es sur la Â«Â blockchain Â Â» font leur apparition Â», Laurent Thevenin,Â *Les Echos*, 19 septembre 2017.
- Â« Comprendre le Bitcoin et la Blockchain Â», Mathieu Nebra, Openclassrooms.com, consultÃ© le 21 octobre 2017.
- Â« Comprendre Bitcoin Â», bitcoin.fr/faq/, consultÃ© le 23 octobre 2017.

Categorie

1. Articles & chroniques

date crÃ©Ã©e
3 janvier 2018
Auteur
jacquesandrefines