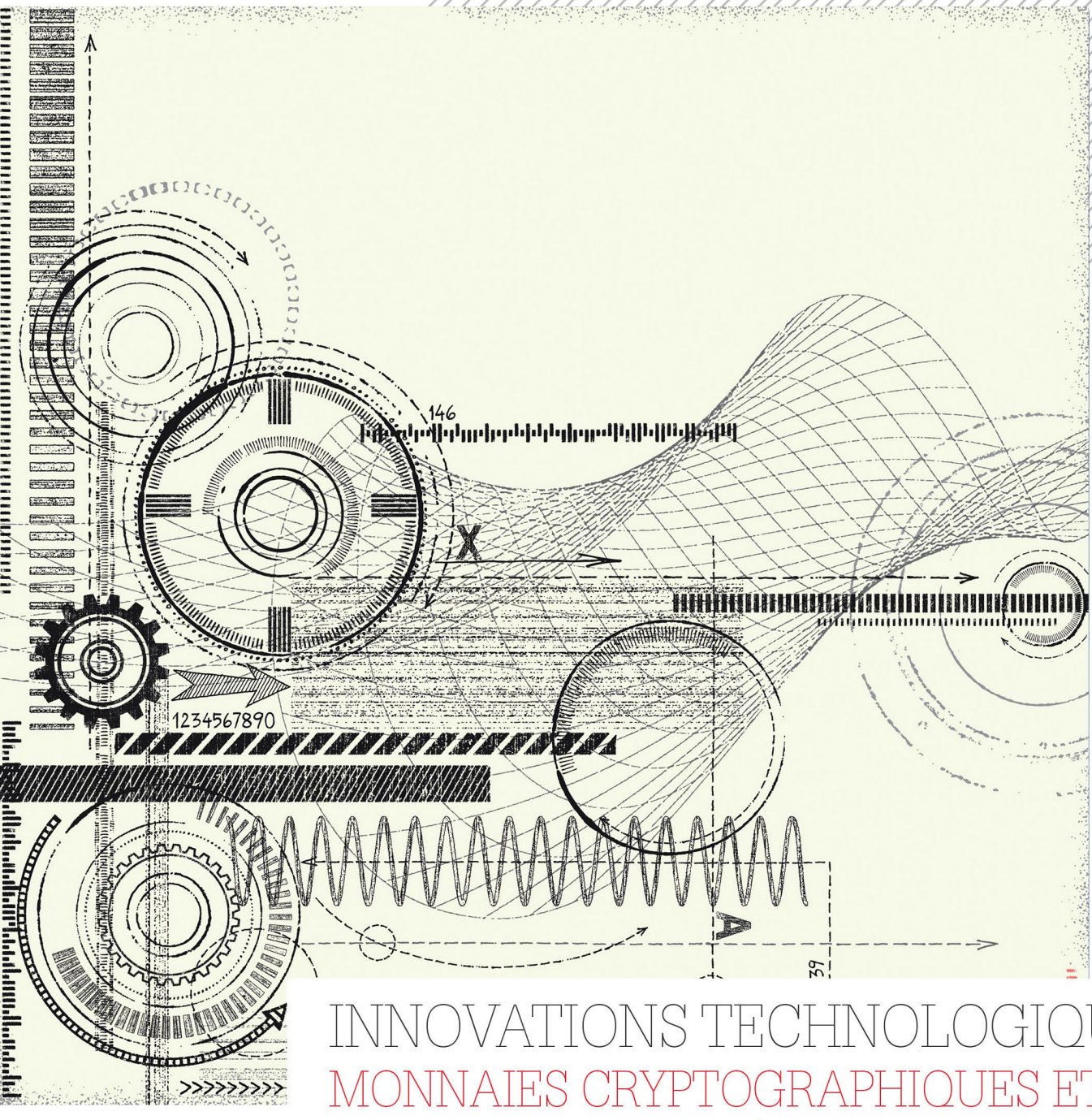
TECHNIQUES
DE L'INGÉNIEUR

LES FOCUS
TECHNIQUES DE L'INGÉNIEUR



INNOVATIONS TECHNOLOGIQUES

MONNAIES CRYPTOGRAPHIQUES ET BLOCKCHAINS - CRÉER DE LA CONFIANCE

février / 2021

TECHNIQUES
DE L'INGÉNIEUR

Réf. : **H5538 V2**

Date de publication :
10 décembre 2020

Monnaies cryptographiques et blockchains - Créer de la confiance

Cet article est issu de : **Innovation | Innovations technologiques**

par **Jean-Paul DELAHAYE**

Mots-clés
cryptographie | réseaux pair-à-pair | Bitcoin | confiance partagée | preuve de travail | blockchain

Résumé En 2008 Satoshi Nakamoto définissait un nouveau modèle de monnaies, dont l'émission et la gestion s'opèrent sur un réseau pair-à-pair sans contrôle centralisé. Le Bitcoin qui est la première monnaie cryptographique créée sur ce modèle existe depuis janvier 2009. Il tient très bien. Comme les 7000 autres monnaies du même type créées à sa suite, il fonctionne grâce à une blockchain. C'est un fichier partagé et collectivement contrôlé par un réseau pair-à-pair. Il peut servir à bien d'autres buts que la création de monnaie. Une multitude d'applications sont, grâce à cette technologie, étudiées et mises en place progressivement, en particulier dans le monde des banques et de la finance.

Keywords
cryptography | peer-to-peer networks | Bitcoin | shared trust | proof of work | blockchain

Abstract In 2008 Satoshi Nakamoto defined a new model of currencies. The issuance and management of such a currency take place on a peer-to-peer network without central control. Bitcoin is the first cryptographic currency created on this model. It exists since January 2009. As the 7000 other crypto-currencies of the same type created in its wake, it works through what is called a blockchain. This shared file and collectively controlled file by a peer-to-peer network can be used for many other purposes. Many applications are developed and implemented gradually, especially in the world of banking and finance.

Pour toute question :
Service Relation clientèle
Techniques de l'Ingénieur
Immeuble Pleyad 1
39, boulevard Ornano
93288 Saint-Denis Cedex

Par mail :
infos.clients@teching.com
Par téléphone :
00 33 (0)1 53 35 20 20

Document téléchargé le : **10/02/2021**
Pour le compte : **7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28**

© Techniques de l'Ingénieur | tous droits réservés

Monnaies cryptographiques et *blockchains*

Créer de la confiance

par **Jean-Paul DELAHAYE**

Professeur émerite à l'université de Lille, Centre de recherche en informatique, signal et automatique de Lille (CRISTAL), UMR CNRS 9189, France

Note de l'éditeur

Cet article est la mise à jour de l'article de même titre et du même auteur, publié par les Techniques de l'ingénieur en 2017.

*La **cryptographie** mathématique a acquis une maturité remarquable depuis la Seconde Guerre mondiale. En même temps, les progrès dans la conception et la réalisation matérielle des réseaux informatiques ont conduit à en concevoir fonctionnant sans centre principal de commande : les **réseaux pair à pair**. Ces deux éléments associés à la puissance de calcul et de mémorisation dont chaque machine dispose aujourd'hui ont rendu possible la conception de nouveaux moyens de paiement qui ne ressemblent à aucun autre et sont susceptibles de bouleverser l'économie et la finance, voire bien d'autres secteurs d'activité.*

Fin 2008, l'énigmatique Satoshi Nakamoto – c'est un pseudonyme – publie sur les réseaux un texte décrivant comment il est possible de mettre en place un système d'échange d'unités monétaires (qu'il nomme les **bitcoins***) qui n'a besoin d'**aucun contrôle centralisé pour fonctionner**, contrairement à toutes les monnaies usuelles émises par les banques centrales et à tous les systèmes de paiement en ligne. Le 3 janvier 2009, les programmes nécessaires au lancement de cette première « crypto-monnaie » sont prêts et elle est créée. Après des débuts confidentiels où seuls quelques experts en cryptologie connaissent son existence et s'y intéressent, elle se met à prospérer. Son cours, dérisoire en 2009, prend son envol, lui donnant une réalité concrète. Début 2013, un* bitcoin *vaut une dizaine d'euros. L'année 2013 est celle du décollage du* bitcoin *qui acquiert alors une notoriété mondiale. Il voit son cours multiplié par 50 en*

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

un an, pour atteindre 580 euros, le 1er janvier 2014. Après une période d'hésitations et de baisses qui dure deux ans, il repart à la hausse et le 1er janvier 2017, il s'échange contre 885 euros. L'année 2017 est une année folle qui le conduit le 17 décembre 2017 à 16 870 euros. Il est depuis redescendu et oscille autour de 11 000 euros (11 130 euros le 27 octobre 2020 par exemple). Contrairement à ce qui avait été annoncé par de nombreux analystes hostiles à cet étrange objet numérique souvent mal compris, le bitcoin *se maintient somme toute assez bien même si c'est avec des à-coups imprévisibles et inquiétants. Aujourd'hui, la capitalisation totale des 18,5 millions de* bitcoins *émis dépasse 206 milliards d'euros (le 27 octobre 2020).*

À partir de rien, la cryptologie mathématique et la technologie réseau ont donc créé des devises numériques qui s'échangent contre de l'argent sonnant et trébuchant, permettant par exemple à un étudiant norvégien – Kristoffer Koch – qui avait acquis pour 25 euros de bitcoins *en 2009, d'en revendre une partie pour s'acheter un appartement au centre d'Oslo. Plusieurs milliers de crypto-monnaies, copiant plus ou moins le* bitcoin *ont été introduites, mais le* bitcoin *reste très largement dominant : sa capitalisation représente 65 % environ de la capitalisation de toutes les crypto-monnaies.*

L'idée de cette monnaie est que, grâce à un subtil agencement de protocoles cryptographiques, on peut émettre une monnaie dont le contrôle se fait collectivement sur un réseau pair à pair, sans qu'aucune autorité ne dispose du pouvoir d'agir sur elle... et en particulier d'émettre de nouveaux bitcoins*. Le protocole de Nakamoto a été rendu possible grâce aux* ***fonctions de hachage cryptographique*** *(qui assurent l'intégrité d'un gros fichier de comptes), aux protocoles de* ***signatures à double clé*** *(qui certifient que seul le détenteur d'un compte l'utilise), au concept de* ***preuve de travail*** *(qui organise un système d'incitation pour que de nombreux utilisateurs participent à la gestion et à la surveillance du système).*

Ces primitives, convenablement assemblées, réalisent un dispositif numérique qu'on pensait impossible auparavant. La mise en place du protocole bitcoin *doit aussi son existence à la puissance informatique dont chacun dispose et qui fait qu'avec son ordinateur personnel il peut contribuer à la surveillance de la monnaie* bitcoin *au travers d'un réseau pair à pair. Ceux qui le souhaitent peuvent télécharger des logiciels* open source *et participer à la surveillance de la monnaie* bitcoin*, c'est-à-dire vérifier que personne ne crée des* bitcoins *non prévus par le protocole, et que toutes les transactions se déroulent conformément aux règles définies au départ par Nakamoto (ces règles peuvent évoluer, mais seulement lentement, et à la suite de sortes de votes où seuls participent ceux qui contribuent collectivement à sa gestion).*

Le registre des comptes qui détient une trace de chaque transaction entre comptes bitcoin *depuis 2009 se nomme la* **blockchain***. Chaque* ***nœud principal*** *(ou nœud validateur, ou «* full node *») du réseau (c'est-à-dire participant à sa gestion) en détient une copie et c'est cette information partagée, indestructible et infalsifiable qui assure la sécurité des comptes. Il y a aujourd'hui environ 10 000 nœuds principaux. Personne ne peut manipuler un compte, personne ne peut créer d'autres* bitcoins *que ceux prévus par le protocole qui, grâce à cette* blockchain*, engendre et maintient la confiance des utilisateurs. Ce succès a conduit à envisager d'autres applications de telles* blockchains*. On les utilise pour mémoriser et garantir les informations d'un cadastre, pour enregistrer les données sur la localisation d'œuvres d'art, pour détenir et garantir l'authenticité des listes des diplômes délivrés par des écoles et des universités et qu'on souhaite rendre consultables par tous, pour organiser toutes sortes de transactions, jeux, votes ou paris, etc. De tels fichiers partagés et collectivement surveillés semblent fournir plus de garanties et de fiabilité que les méthodes traditionnelles à base de tiers de confiance (un opérateur central qui détient le fichier doit le mettre à jour, le sécuriser et le rendre accessible, partiellement le plus souvent). C'est la raison d'un intérêt croissant depuis 2012 pour cette technologie des* blockchains *directement inspirée du* bitcoin*. Notons qu'elle n'en dépend pas et s'en éloigne souvent, tant les variantes sont nombreuses et s'ajustent à des applications variées et innovantes.*

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

Nota : Dans ce texte nous avons utilisé des extraits de textes publiés par nous précédemment au sujet du *bitcoin* et des *blockchains* (voir https://www.cristal.univ-lille.fr/profil/jdelahay#page4. Le texte ici proposé est cependant une synthèse nouvelle et originale d'informations et une mise à jour aussi précise que possible à la date du 27 octobre 2020 sur ce sujet en évolution rapide.

1. Obtention de *bitcoins*

Pour posséder des *bitcoins*, il faut disposer d'un compte, mais il n'est pas besoin de donner son identité pour en créer un. Cet anonymat des détenteurs de *bitcoins* est l'une des caractéristiques de cette monnaie. Il faut cependant savoir qu'il n'est que partiel, car le suivi des transactions opérées permet dans certains cas de remonter au détenteur d'un compte. On parle de **« pseudonymat »** plutôt que d'anonymat.

Chaque compte est associé à deux numéros. Il y a le numéro secret qu'il faut absolument garder pour soi, car quiconque en dispose peut dépenser le contenu du compte. Il y a aussi le numéro public que vous communiquerez et qui est comme une adresse ou un numéro de compte. Ce second numéro permet de recevoir des *bitcoins* : on l'indique à celui qui souhaite vous envoyer des *bitcoins*, ce qui lui permet de composer une transaction (qu'il signera) de son compte vers le vôtre.

Créer un compte est immédiat et gratuit : on télécharge un porte-monnaie (on dit aussi « portefeuille », ou *wallet* en anglais... et en français !) (voir par exemple [CHOI] du « *Pour en savoir plus* », rubrique « Sites Internet »).

Ces logiciels qui existent pour toutes les plateformes d'ordinateurs et de *smartphones* sont gratuits. Le plus souvent leur code est libre : vous pouvez contrôler que le programme ne fait que ce qui est prévu qu'il fasse. Quand on dispose d'un *wallet*, on peut créer autant de comptes qu'on le souhaite.

On obtient des *bitcoins* en en achetant contre de l'argent usuel sur les plateformes d'échange qui sont pour la plupart des entreprises tout à fait légales ayant reçu les accréditations et autorisations leur permettant ce type d'activité. Pour utiliser leur service, il faut décliner son identité (voir le « *Pour en savoir plus* », rubrique « Sites Internet » référence [PLA]).

On obtiendra aussi des *bitcoins* en faisant du commerce : vous échangez un bien contre des *bitcoins*.

Autre méthode encore pour avoir des *bitcoins* : participer à la surveillance de la monnaie. On peut pour cela soit détenir un nœud principal (nous avons dit qu'il y en a environ 10 000 aujourd'hui). Soit adhérer à un *pool* de minage qui est centré sur un nœud principal (le *leader* du *pool*), auquel on fournit une certaine puissance de calcul qui contribue à sa capacité de calcul et augmente donc sa capacité de gagner des *bitcoins*.

En effet, un nœud principal reçoit régulièrement une récompense en *bitcoins* dont la fréquence est fonction de la puissance dont il dispose : plus un nœud principal et ses associés (les mineurs) composant un *pool* de minage sont puissants, plus la probabilité de gain est forte. Aujourd'hui, cette récompense est de 6,25 *bitcoins* toutes les 10 minutes (de 2009 à 2013, elle était de 50 *bitcoins*, puis elle a été de 25 *bitcoins* jusqu'en juillet 2016, puis de 12,5 *bitcoins* jusqu'en mai 2020 avant de tomber à 6,25). La récompense n'est attribuée qu'à un seul nœud validateur, à la suite d'une sorte de tirage au sort, où la probabilité de gagner est proportionnelle à la capacité que possède le *pool* de calculer rapidement des valeurs de la fonction de hachage SHA256 (voir § 4). Un grand nombre de mineurs participent à ces *pools* de minage. On évalue qu'ils sont environ 100 000 regroupés autour des 10 000 nœuds validateurs. Participer à un *pool* de minage n'oblige pas à gérer directement la *blockchain* (dont la taille est de 357 gigaoctets en juin 2020). Seul le *leader* du *pool* détient une copie de la *blockchain*.

Plus il y a de *pools* de minage, plus la monnaie est solide. Créer un *pool* seul n'est plus raisonnable aujourd'hui car la probabilité que votre machine soit choisie pour recevoir les 6,25 *bitcoins* distribués toutes les 10 minutes serait trop faible. En se regroupant en *pool*, les mineurs augmentent la probabilité de gagner, même si à chaque fois que le *pool* gagne ils doivent se partager les 6,25 *bitcoins*. Aujourd'hui la grande majorité des mineurs utilisent des puces spécialisées ASIC conçues pour calculer rapidement SHA256 (nous y reviendrons).

Le cours du *bitcoin* et de toutes les monnaies cryptographiques est fixé, comme pour les actions boursières, par la rencontre de l'offre et de la demande : certains souhaitent vendre des *bitcoins* dont ils ne veulent plus, d'autres veulent en acheter ; un accord s'établit entre eux qui fixe la valeur d'échange des *bitcoins*. Les plateformes d'échange sont les lieux de ces rencontres comme le sont les Bourses pour les actions.

La figure **1** montre quelques courbes correspondant à la période du 29 avril 2013 au 26 juin 2020. Il y a le cours en dollars du *bitcoin*, la capitalisation des *bitcoins* émis, et le volume des transactions, qui est indiqué sans échelle mais permet de voir l'accroissement important de ce volume durant certaines périodes. Les courbes proviennent du site : Crypto-Currency Market Capitalizations (**http://coinmarketcap.com**).

La figure **2**, qui provient de la même source, indique le cours en dollars, la capitalisation en dollars et le nombre d'unités en circulation pour des 10 premières crypto-monnaies à la date du 26 juin 2020. On voit que le *bitcoin* est de loin la crypto-monnaie la plus valorisée (près de 7 fois plus que la seconde, l'Ether émis par le réseau Ethereum).

La figure **3** donne l'évolution de la taille de la *blockchain* du *bitcoin*. On observe qu'elle augmente régulièrement, en gros linéairement, et qu'elle a atteint la taille de 284 Go (gigaoctets) le 25 juin 2020. C'est beaucoup mais compatible avec la capacité d'un disque dur d'ordinateur de bureau actuel (source : **https://www.blockchain.com/charts/**).

2. Robustesse des *bitcoins*

Les *bitcoins* n'existent pas matériellement, ils n'existent que sur le réseau pair à pair. Ils sont le résultat d'un consensus entre utilisateurs qui, grâce aux informations présentes sur le réseau et que chacun peut consulter et contrôler, indiquent quelles sommes d'argent se trouvent sur les comptes. L'ensemble des comptes est stocké dans un fichier – la *blockchain* – accessible à tous. Plus précisément, la *blockchain* contient l'ensemble des transactions (validées par page ou « bloc ») depuis le début du *bitcoin*, dont on peut déduire le contenu en *bitcoins* de chaque compte.

Seul le *leader* d'un *pool* de mineurs contrôle la correction des transactions et leur inscription dans la *blockchain*. Il doit avoir téléchargé la *blockchain* (ce n'est pas rien !) dont il garde une copie. Il la met à jour toutes les dix minutes en lui ajoutant une nouvelle page (*block*). Les autres mineurs d'un *pool* travaillent juste à accroître sa puissance de calcul de *hash* (§ 4), pour augmenter la probabilité que le *pool* gagne toutes les 10 minutes.

Le protocole cryptographique de la monnaie assure que personne ne peut manipuler la *blockchain*, fausser les transactions, ou émettre d'autres *bitcoins* que ceux prévus (et qui apparaissent dans la *blockchain*). Il y avait 18,4 millions de *bitcoins* en circulation en juin 2020. Tous ont été émis pour récompenser les mineurs. Le rythme d'émission a été fixé dès le départ et ne peut pas changer :

– 50 *bitcoins* toutes les 10 minutes pendant les quatre premières années environ (en fait jusqu'au 29 novembre 2012) ;

– 25 *bitcoins* toutes les 10 minutes pendant les quatre années suivantes environ (en fait jusqu'au 10 juillet 2016) ;

– 12,5 *bitcoins*, toutes les 10 minutes pendant les quatre années suivantes environ (en fait jusqu'au 11 mai 2020)

– 6,25 *bitcoins* toutes les 10 minutes depuis le 11 mai 2020.

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

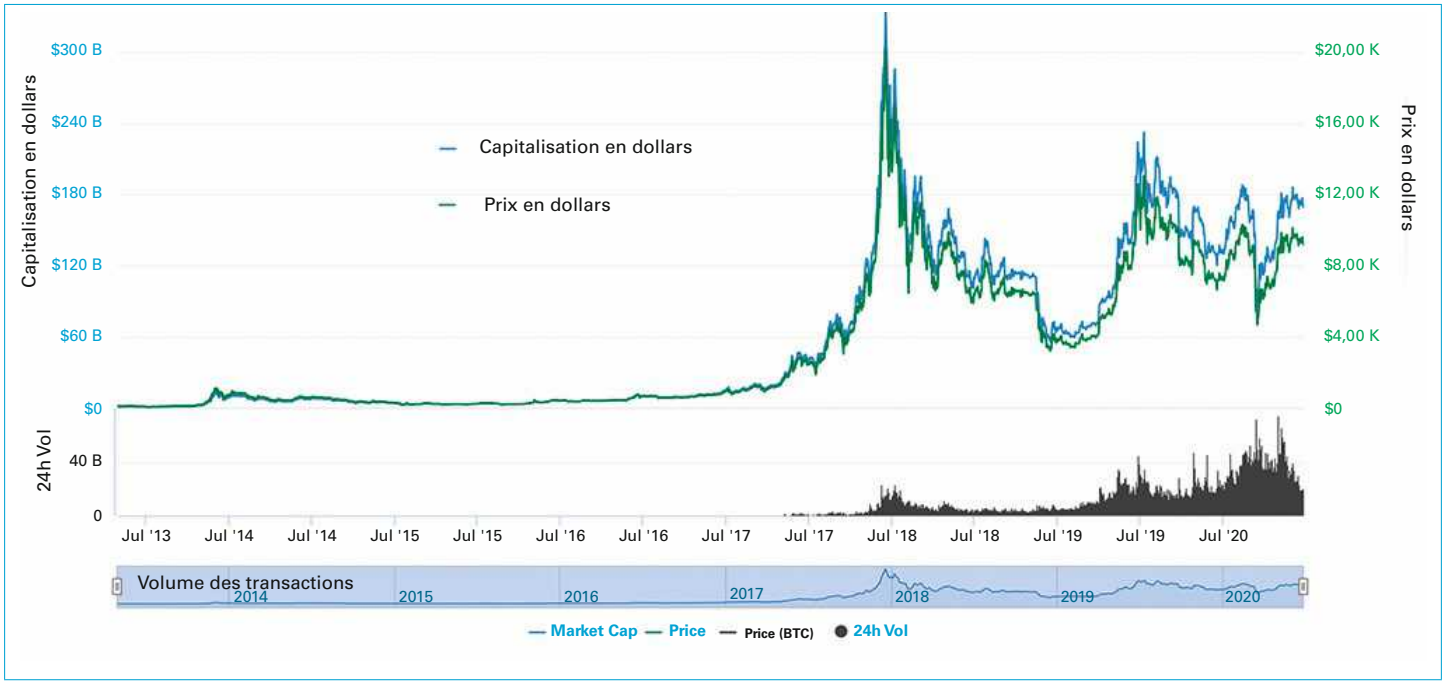


Figure 1 – Cours en dollars du *bitcoin* le 26 juin 2020, capitalisation des *bitcoins* émis et volume des transactions jusqu'au 26 juin 2020

	Nom	Capitalisation	Prix	Nombre d'unités
1	Bitcoin	$169 304 749 456	$9 193,79	18 415 125 BTC
2	Ethereum	$25 818 880 877	$231,54	111 508 568 ETH
3	Tether	$9 175 978 058	$0,998692	9 187 991 663 USDT
4	XRP	$8 168 176 275	$0,184559	44 257 803 618 XRP
5	Bitcoin Cash	$4 269 572 384	$231,47	18 445 544 BCH
6	Bitcoin SV	$3 128 299 674	$169,61	18 444 140 BSV
7	Litecoin	$2 804 851 321	$43,22	64 895 308 LTC
8	Binance Coin	$2 458 927 220	$15,81	155 536 713 BNB
9	EOS	$2 308 406 951	$2,47	933 814 123 EOS
10	Cardano	$2 110 634 208	$0,081407	25 927 070 538 ADA

Figure 2 – Cours en dollars, capitalisation en dollars et nombres d'unités en circulation pour les dix premières crypto-monnaies, le 26 juin 2020

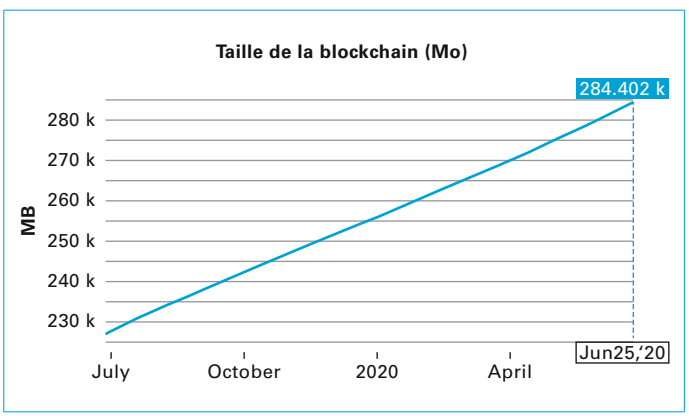


Figure 3 – Évolution de la taille de la *blockchain* du *bitcoin*

La division par deux de la récompense (appelée « *halving* ») se poursuivra jusqu'à ce que la somme distribuée devienne négligeable. Le nombre total de *bitcoins* émis ne dépassera jamais 21 millions de *bitcoins*. Ce nombre provient du calcul suivant. Le protocole *Bitcoin* fixe qu'il y a un *halving* précisément tous les 210 000 blocks ; le nombre total de *bitcoins* émis ne dépassera donc jamais :

$$50 \times 210\,000 \times \left[1 + 1/2 + 1/4 + \ldots + 1/2^n + \ldots\right] = 21\,000\,000$$

Précisément, l'émission de nouveaux *bitcoins* cessera quand, à force d'être divisée par 2, la somme émise sera devenue inférieure à 1/100 000 000 de *bitcoin* (car les programmes ne prévoient pas de divisions plus petites du *bitcoin*). Le total émis sera donc un peu inférieur à 21 millions et cela se produira environ en 2140.

La robustesse du protocole – confirmée par douze ans de fonctionnement – rend l'existence virtuelle et purement numérique des *bitcoins* aussi réelle et solide que celle des lingots d'or ou des billets de banque que vous avez en poche. À cause de l'anonymat (partiel) des comptes et des transactions, le *bitcoin* doit être considéré comme de « l'argent liquide numérique ». La **cryptographie** a réussi à créer des objets non matériels, infalsifiables, aussi résistants et persistants que s'ils étaient faits de métal, et qui circulent à la vitesse de la lumière (c'est un des avantages des *bitcoins* sur les autres monnaies) sans presque aucun coût, d'un endroit à l'autre du monde.

Comme toute monnaie, le *bitcoin* ne tient que par la confiance de ses utilisateurs qui en déterminent le cours par les échanges

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

opérés sur les plateformes d'achat et de vente de la monnaie. La confiance s'établit non pas parce qu'une banque centrale émettrice prétend se porter garant des devises qui circulent – on sait ce qu'il en est en cas de crise ! –, mais parce que le protocole cryptographique général qui organise le fonctionnement des opérations sur le réseau empêche quiconque de truquer les comptes et en particulier d'émettre sans retenue des masses de devises qui feraient s'effondrer son cours.

Les caractéristiques des *bitcoins* ont des conséquences positives dont – en théorie – une protection des détenteurs de *bitcoins* contre l'inflation. Celle-ci provient habituellement de l'émission plus ou moins massive par les banques centrales de devises créées à partir de rien : la fameuse « planche à billets ». Pour le *bitcoin*, aucune émission en dehors de celle inscrite dans le protocole n'est possible. Certains prétendent que, par nature, le *bitcoin* est déflationniste : il ne pourrait que prendre de la valeur. La réalité est évidemment plus complexe, comme l'histoire des variations de cours du *bitcoin* l'a montré.

On trouvera plus de détails sur ces questions en consultant la page [DEL] (rubrique « Sites Internet » du « *Pour en savoir plus* ») qui renvoie à divers documents.

3. Transactions

Entrons dans le détail du **fonctionnement du *bitcoin***. On s'intéresse à lui en particulier car c'est la monnaie cryptographique principale, largement plus importante que toutes les autres, et parce que c'est le meilleur moyen de comprendre ce qu'est une *blockchain*, les autres *blockchains* n'étant que des variantes de celle du *bitcoin* dont il faut donc avoir une compréhension précise.

Lorsqu'Alice veut faire un paiement en *bitcoins* à Bernard (par exemple en échange d'un livre), l'ordinateur d'Alice va opérer une série d'opérations. Ces opérations sont faites automatiquement par le logiciel (*wallet*) qu'elle a installé sur son ordinateur ou sur son *smartphone*, et qui gère les communications entre sa machine et le réseau pair à pair du *bitcoin*. Celui-ci acceptera ou refusera la transaction en contrôlant que la transaction est conforme au protocole et en particulier que le compte débité détient bien les *bitcoins* dépensés. Ce réseau pair à pair est au cœur du système. L'existence de tels réseaux est essentielle pour la monnaie *bitcoin* qui n'est gérée par aucun nœud central qui contrôlerait l'ensemble des communications.

La transaction qui résulte de l'ordre donné par Alice en faveur de Bernard est publique : elle circule sur le réseau et rapidement tous les ordinateurs présents sur le réseau en sont donc informés. Cela permet la mise à jour (toutes les 10 minutes), par tous les *leaders* de *pool*, de la *blockchain* qu'ils détiennent. Ils ajoutent à chaque fois une page (*bloc*) à ce fichier dont chacun détient une copie parfaitement identique à toutes les autres copies de la *blockchain*.

L'ordinateur de Bernard n'a pas besoin d'être connecté pour que la transaction s'opère : quand, plus tard, Bernard se connectera au réseau, celui-ci l'informera qu'une somme est arrivée sur son compte et lui dira quelle somme finalement s'y trouve.

Soyons plus précis (sans toutefois entrer dans toute la complexité technique de sa mise en œuvre) sur les opérations constituant une transaction signée :

– Alice souhaite envoyer N *bitcoins* à Bernard ;

– Bernard communique sa clé publique B_{pub} (c'est-à-dire son numéro de compte) à Alice ;

– Alice constitue un message M de transaction contenant la clé publique de Bernard B_{pub} et la somme N à transférer : $M = B_{pub}\ N$;

– Alice (dont les clés publique et privée sont A_{pub} et A_{pr}) signe la transaction M avec sa clé privée, c'est-à-dire calcule une suite de symboles $M' = f\left(A_{pr},\ M\right)$ qui avec sa clé publique redonne M :

$$g\left[A_{pub},\ f\left(A_{pr},\ M\right)\right] = g\left(A_{pub},\ M'\right) = M$$

(f et g sont les fonctions opérant signature et lecture des signatures).

Tout le monde peut donc contrôler que c'est Alice qui a signé, mais personne ne peut signer à sa place [H 5 210] ;

– Alice diffuse la transaction signée sur le réseau afin qu'elle soit vue par tout le monde. Cette diffusion constitue une validation de premier niveau de la transaction, mais c'est une validation faible et, par exemple, le compte qui reçoit l'argent ne peut pas le dépenser à cet instant : il faudra qu'il attende que la transaction ait été mise dans une page et que cette page ait été ajoutée à la *blockchain*.

En regardant cette transaction depuis l'extérieur, tout le monde voit qu'Alice a donné son accord pour transférer N *bitcoins* à Bernard. Ne disposant pas de la clé privée d'Alice, personne d'autre qu'elle ne peut envoyer une telle transaction sur le réseau. Son envoi est donc la preuve qu'Alice souhaitait ce transfert.

Un peu plus précisément, une transaction comporte dans l'ordre :

– un numéro de version ;

– le nombre d'entrées ;

– la liste des entrées, c'est-à-dire des transactions précédentes qui ont permis au compte émetteur de détenir une somme supérieure à celle dépensée ;

– le nombre de sorties ;

– la liste des sorties, c'est-à-dire des comptes où sera versée la dépense. Pour faciliter le calcul des soldes des comptes, tout l'argent d'un compte est dépensé à chaque transaction, quitte à ce que, parmi les comptes qui reçoivent les diverses parties de la dépense, il y ait le compte émetteur lui-même qui se reverse une partie de la dépense.

On trouvera d'autres précisions dans le « *Pour en savoir plus* », rubrique « Sites Internet » référence [TRAN1] ou encore [TRAN2]. Concernant les modes de fonctionnement plus classiques et les problèmes de sécurité des réseaux, on pourra étudier les articles [H 3 578] [H 3 580].

La *blockchain* évolue toutes les dix minutes (environ) car le *pool* de mineurs gagnant des 6,25 *bitcoins* ajoute une nouvelle page de transactions à la *blockchain*. Cette nouvelle page contient des transactions validées par le réseau mais pas encore présentes dans la *blockchain*. Parmi les transactions qui se trouvent validées par cet ajout de page, il y en a une qui crée 6,25 *bitcoins* attribués au *leader* du *pool* de minage qui ajoute la page. Le *leader* bien sûr redistribue ce gain aux membres du *pool*. C'est de cette façon que sont créés les nouveaux *bitcoins*. Répétons-le, tous les *bitcoins* en circulation ont été créés de cette façon. Cet ajout de page est une confirmation de second niveau de la validité de la transaction. Dépenser les *bitcoins* reçus par l'exécution des transactions présentes sur la page ajoutée est alors possible.

Donnons encore **trois précisions importantes**.

(a) Le *leader* du *pool* qui ajoute la page choisit (parmi les transactions en attente) les transactions qu'il met dans la page. Les transactions peuvent contenir une **commission** (facultative et souvent minime) qui s'ajoutera aux 6,25 *bitcoins* gagnés. Aujourd'hui les commissions associées à une page entière valent moins d'un *bitcoin* au total. Ce système de commissions assure que, lorsque la somme gagnée automatiquement par création de nouveaux *bitcoins* sera devenue trop faible (nous avons indiqué qu'elle est divisée par deux tous les quatre ans environ), il sera toujours intéressant de participer à la gestion et à la surveillance de la *blockchain*.

(b) La **page ajoutée**, dans certains cas exceptionnels – résultant par exemple de l'isolation d'une partie du réseau conduisant temporairement à la création de deux *blockchains* différentes –, peut être **annulée**. Cela signifie qu'on ne doit pas considérer comme définitivement réalisée une transaction présente sur une page de la *blockchain*.

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

Quand plusieurs *blockchains* différentes existent temporairement sur le réseau, celle qui est la plus « longue » est retenue par les mineurs. L'autre est oubliée, ce qui conduit à l'annulation des transactions qui y sont, si elles ne sont pas aussi sur la *blockchain* retenue (ce qui sera le cas le plus souvent). La « longueur » d'une *blockchain* est mesurée par sa **difficulté** et correspond à un contenu en calcul qui se compte en nombre de *hash* (§ 4). Ce choix uniforme opéré par tous les nœuds du réseau rétablit un état cohérent du réseau, avec une seule *blockchain* identique en chacun des nœuds. Dans le cas de transactions importantes en valeur, il faut donc attendre plusieurs fois 10 minutes pour considérer la transaction comme définitive et que les problèmes éventuels de duplication de *blockchain* aient été résolus. On évalue qu'une heure assure une certitude totale d'irréversibilité qui est une confirmation de troisième niveau. Ces duplications de la *blockchain* (appelées « *fork* ») sont inévitables à cause de l'imperfection des réseaux, et des délais de communication entre nœuds. Leur gestion et le rétablissement d'un état cohérent du réseau (reconstitution d'un consensus) constituent des éléments importants du protocole *bitcoin*, même si ce type d'événement est relativement rare.

(c) Le système de clés utilisé pour les signatures dans le protocole *bitcoin* est basé sur la **cryptographie à courbes elliptiques**, dite « ECDSA » (*Elliptic Curve Digital Signature Algorithm*). La courbe employée est secp256k1. C'est un système considéré comme sûr par les experts cryptologues.

La figure **4** montre la répartition de la puissance des principaux *pools* de minage, le 27 juin 2020. On remarquera que les quatre plus importants *pools* totalisent nettement plus de la moitié de la puissance de minage. Cela signifie que s'ils s'entendaient, ils pourraient facilement perturber le fonctionnement du réseau *bitcoin* et même faire perdre toute confiance en la monnaie *bitcoin*. Le schéma provient de :

https://www.blockchain.com/charts/pools

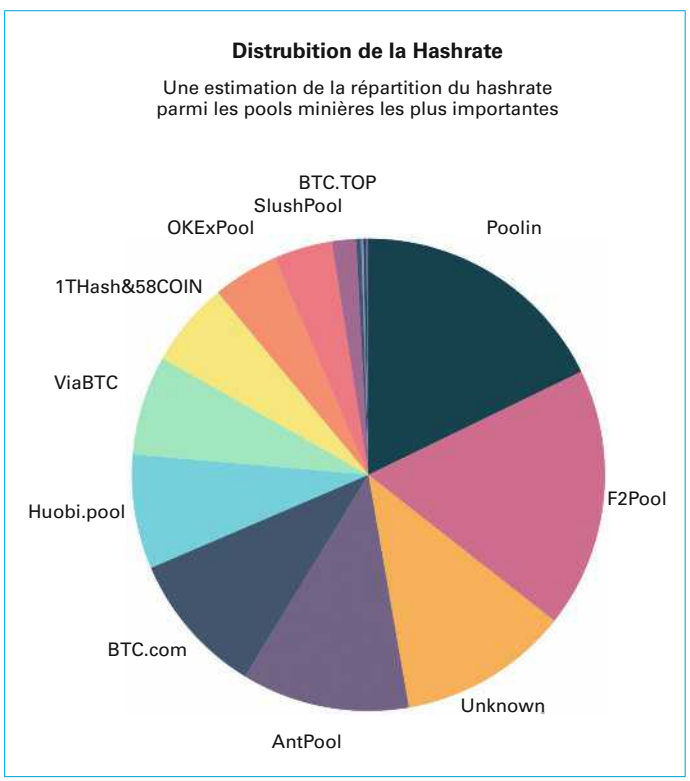


Figure 4 – Pools de minage du *bitcoin* les plus importants en juin 2020

4. Preuves de travail

Venons-en à cette compétition qui se déroule toutes les 10 minutes entre nœuds principaux pour être désigné gagnant de 6,25 *bitcoins*.

Une fonction de **hachage cryptographique** est une fonction h qui, à toute suite de symboles S (par exemple des chiffres et des lettres), associe une autre suite de symboles (plus courte) $h(S) = R$, et surtout, qui est telle qu'il est impossible en pratique pour une valeur possible R de la fonction h de trouver un S tel que $h(S) = R$ (impossibilité pratique de l'inversion). La valeur R est nommée « *hash* » du fichier S, ou « empreinte » du fichier S. Si h est une bonne fonction de hachage, les valeurs $h(S)$ produites par quelqu'un qui essaie diverses valeurs pour S sont aussi imprévisibles que si elles étaient tirées au hasard avec une roue de loterie. De plus, changer un seul symbole de S produit un résultat sans rapport apparent avec le résultat avant changement. La fonction utilisée pour le *bitcoin* est la fonction SHA256 : SHA = « *secure hash algorithm* » ; 256, car les valeurs produites ont comme longueur 256 bits = 32 octets.

Disposant d'une telle fonction h, on peut définir un « travail » qu'il sera impossible de faire rapidement :

Travail de niveau k : trouver S tel que $h(S)$ commence par k fois le symbole « 0 ».

Plus k est grand, plus il faut essayer de nombreux S avant de trouver un S convenable. En moyenne, ceux qui prétendent avoir trouvé un tel S ont fourni un travail de calcul qui est d'autant plus important que k est grand. C'est un peu comme si on demandait à quelqu'un de lancer deux dés (ou k dés) jusqu'à obtenir un double 6 (ou k fois le « 6 »). Il faudrait en moyenne qu'il les lance 36 fois (ou 6^k fois) pour réussir.

On vérifiera facilement que les S prétendument trouvés sont bons, en en demandant la communication, et en calculant $h(S)$ qui doit être un résultat avec k « 0 » en tête. Une fois effectué, vérifier que le long travail a bien été fait est donc une opération rapide. Trouver la solution est long et difficile, la vérifier est immédiat. L'idée de ces « **preuves de travail** » a été proposée en **cryptographie** dans le but, par exemple, de lutter contre le courrier électronique indésirable (spam). Si chaque ordinateur qui veut accéder à une boîte de messages doit prouver qu'il a effectué un certain travail dépendant de la boîte (par exemple trouver un S tel que $h(S)$ commence par 10 fois « 0 » pour une fonction h qui dépend de la boîte), il devient impossible à celui qui le voudrait d'envoyer des milliers de spams, car les preuves de travail nécessaires seraient trop lourdes au total. Cette barrière à l'entrée d'une boîte à lettres électronique n'est pas ennuyeuse pour celui qui ne veut envoyer que quelques messages, car les preuves de travail à fournir demandent un temps raisonnable de calcul quand le nombre d'envois est petit.

La technique des preuves de travail est au cœur du protocole *bitcoin*. C'est elle qui est utilisée pour la détermination de celui qui ajoute une page à la *blockchain*, et remporte toutes les dix minutes les 6,25 nouveaux *bitcoins*. Les mineurs d'un *pool* de minage calculent des *hash* pour résoudre le problème qui est posé au *leader* du *pool*. Bien sûr, un paramètre contextuel dans la définition de la fonction h n'est connu qu'au moment où un nouveau « tirage » est lancé, il empêche les participants de commencer à chercher le S en avance.

Ajustables en faisant varier l'entier k (ou un autre paramètre permettant un contrôle plus fin de la difficulté), les preuves de travail exigées pour emporter les 6,25 *bitcoins* créés toutes les 10 minutes sont devenues de plus en plus difficiles au cours des années. Le protocole prévoit un ajustement automatique de la difficulté des problèmes soumis : celle-ci s'ajuste automatiquement toutes les 2 016 pages pour qu'il y ait un gagnant environ toutes les 10 minutes. Quand la puissance globale de calcul du réseau augmente, l'intervalle moyen de temps entre deux pages diminue,

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

jusqu'à ce que le réajustement fait toutes les 2 016 pages le ramène à 10 minutes. La durée de 10 minutes, on le comprend, est une moyenne : un mineur peut avoir de la chance et résoudre le problème posé en 5 minutes, ou au contraire par malchance la résolution par le réseau du problème posé peut ne se faire qu'au bout de 15 minutes.

Depuis que des puces spécialisées ASIC (*Application Specific for Integrated Circuit*) ont été conçues pour calculer très vite les $h(S)$ (donc le SHA256), la difficulté du travail demandé est devenue considérable pour atteindre la valeur incroyable de 120×10^{18} calculs de *hash* par seconde pour l'ensemble du réseau *bitcoin* (en mars 2020).

Une telle quantité de calculs entraîne bien sûr une dépense considérable d'électricité qui s'ajoute à la dépense pour fabriquer les puces spécialisées dans le calcul du SHA256, et à celle pour entretenir et refroidir les installations où sont installés les dispositifs de minage. Cette situation semble d'autant plus absurde que cette dépense n'est pas consacrée à la surveillance même de la *blockchain* et à la gestion des transactions mais uniquement à la détermination du *pool* de minage qui doit recevoir les 6,25 *bitcoins* créés toutes les 10 minutes. Le calcul de la dépense électrique du réseau *bitcoin* est fait de manière assez rigoureuse par plusieurs observateurs dont https://digiconomist.net/bitcoin-energy-consumption.

En juin 2020, cette consommation correspond à un rythme de l'ordre de 60 TWh/an (Téra Watt heure par an) à comparer par exemple avec la consommation annuelle française qui pour l'année 2019 a été de 473 TWh. Nous reparlerons du problème du coût du minage à propos des *blockchains* privées pour expliquer que ce n'est pas une fatalité de la technologie *blockchain*.

Aujourd'hui plus de 60 % du minage est opéré en Chine ce qui est assez ennuyeux, puisque cela signifie que si le gouvernement chinois le souhaitait et exerçait son autorité sur l'ensemble des mineurs localisés en Chine, il disposerait du pouvoir de manipuler la *blockchain* du *bitcoin*.

5. Risques

Les transactions sont gratuites ou ont un faible coût (si on prend en compte la commission ajoutée aux transactions). La rapidité des transferts est très satisfaisante puisque envoyer n'importe quelle somme de manière irréversible d'un point du globe à un autre demandera (a) quelques secondes, (b) une dizaine de minutes ou (c) une heure, selon le niveau de confirmation qu'on souhaite.

Le nombre de transactions que le réseau *bitcoin* peut exécuter est cependant limité à environ 5 ou 10 transactions par seconde, ce qui est très faible comparé au réseau des cartes bancaires (2 000 transactions par seconde ou plus), et rend inconcevable pour l'instant qu'il puisse le concurrencer [H 5 860].

Plusieurs solutions sont envisagées et mises en place progressivement pour accroître la capacité du réseau. Il y a par exemple le protocole Lightning Network qui est une couche au-dessus du réseau *bitcoin*. Il n'intervient pas directement sur le fonctionnement du réseau, mais permet de réaliser des transactions sans les inscrire sur la *blockchain* du *bitcoin*, ce qui allège sa charge. C'est cependant un système complexe qui introduit donc de nouveaux risques et qui ne préserve pas toutes les bonnes propriétés d'un système à *blockchain* puisqu'il renonce à la redondance du stockage de l'information et de la vérification des opérations. Voir par exemple [BLN]

Malheureusement, les propriétés de la monnaie *bitcoin* ont des conséquences négatives. Citons-en quelques-unes :

– il faut être très attentif lors de la **manipulation de son compte** sur son ordinateur ou son *smartphone*. Si un *hacker* réussit à trouver votre clé secrète de compte en s'introduisant sur votre ordinateur, il pourra en dépenser entièrement le contenu. C'est déjà arrivé. N'effacez pas non plus votre porte-monnaie numérique par erreur, il serait définitivement perdu. C'est déjà arrivé ;

– l'**anonymat** (partiel, car on peut suivre les grosses sommes de compte en compte grâce à la *blockchain*) des comptes intéresse toutes sortes de gens peu recommandables qui utilisent le *bitcoin* pour échapper au fisc ou mener des trafics en tout genre. Cela nuit à la réputation du *bitcoin* !

– le fait qu'aucun contrôle centralisé ne soit opéré par une autorité centrale a pour conséquence que le cours des *bitcoins* n'est pas régulé, et est donc soumis à des **variations spéculatives**. Cela rend difficile son usage pour le commerce, sauf si le commerçant reconvertit immédiatement les *bitcoins* qu'il reçoit en monnaie usuelle. Cette pratique est assez systématiquement mise en œuvre aujourd'hui, ce qui explique qu'il existe un nombre assez grand de sites de commerce en ligne qui acceptent d'être payés en *bitcoins* ;

– le fait que la monnaie *bitcoin* soit concurrente des monnaies des banques centrales a pour conséquence que les **États lui sont parfois hostiles**, et que des réglementations existent limitant son usage, ou même l'interdisant (au Maroc par exemple). L'évolution de ces réglementations sera essentielle pour l'avenir du *bitcoin* ;

– puisque tous les programmes contribuant au fonctionnement de la monnaie *bitcoin* sont libres et publics, il est facile de concevoir et de faire fonctionner d'autres monnaies du même type (en recopiant totalement ou partiellement les programmes du *bitcoin*). C'est d'ailleurs ce qui se produit : il existe aujourd'hui **plus de 7 000 monnaies cryptographiques** basées, à peu de chose près, sur les mêmes principes que le *bitcoin* et tentant de lui faire concurrence. Répétons-le, leur capitalisation totale est deux fois inférieure à la capitalisation des seuls *bitcoins*. Cette domination forte du *bitcoin* sur toutes les autres monnaies cryptographiques explique pourquoi nous avons fait le choix de le décrire en détail.

6. Quelques points à ne pas oublier

Il faut énoncer quelques vérités bonnes à savoir sur le *bitcoin* et plus généralement sur toutes les monnaies cryptographiques du même type. Le *bitcoin* est parfois mal compris, sans doute parce qu'il est complexe ! On se trompe à son sujet et, qu'on y soit favorable ou opposé, on ignore fréquemment certaines choses élémentaires permettant de mieux en saisir la nature. Voici une liste partielle de ces vérités négligées qu'il serait pourtant utile d'avoir toujours en mémoire. Certaines semblent servir le *bitcoin*, d'autres suggèrent qu'il faut rester prudent.

Le risque mathématique d'un effondrement du *bitcoin* existe

Même « au froid » (dans votre porte-monnaie numérique sur le disque dur d'un ordinateur non relié au réseau et éteint) vos *bitcoins* peuvent disparaître instantanément. En effet, le système de signature à double clé du *bitcoin* (ECDSA avec la courbe secp256k1) n'a jamais été prouvé incassable. Cela signifie qu'il se peut qu'un mathématicien génial (... ou la NSA qui en emploie beaucoup) réussisse un jour à trouver un moyen de calculer les clés privées à partir des clés publiques. C'est peut-être déjà le cas. Cela lui permettrait alors de s'approprier le contenu de tous les comptes. Il le ferait probablement lentement pour ne pas attirer l'attention. Peut-être est-ce déjà en cours ? Il serait facile à ceux disposant de cette capacité de faire s'écrouler le *bitcoin* si c'est leur but. Le *bitcoin* reposera donc toujours sur un pari mathématique susceptible d'être perdu. Il faut en être conscient. Remarquons que ce n'est pas le cas de l'or, ou même du dollar ou de l'euro qui peuvent voir leurs cours évoluer rapidement (en cas de crise économique majeure) mais pas de manière instantanée comme le *bitcoin* qui reste en équilibre sur une conjecture mathématique. Quand vous détenez de l'or, on peut vous le voler, certes, mais s'il est enfermé dans un bon coffre, c'est difficile. Il n'existe

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

aucun bon coffre pour les *bitcoins*, même votre mémoire, du fait de l'incertitude mathématique qui concerne simultanément tous les *bitcoins* émis. Précisons que les cryptologues considèrent de manière unanime que cet effondrement mathématique est improbable... comme les cryptologues allemands pendant la seconde guère mondiale considéraient de manière unanime que la machine Enigma était sûre, alors que les équipes adverses britanniques réussissaient à en déchiffrer de nombreux messages.

L'effondrement informatique

À côté de l'effondrement mathématique, il y a aussi l'effondrement informatique dû à un bug dans les programmes faisant fonctionner le réseau *bitcoin*. Tous les bugs ne sont pas aussi graves que l'effondrement mathématique, mais certains le valent presque. L'histoire du *bitcoin* ne laisse guère de doute, voir [BBU] dans le « *Pour en savoir plus* », rubrique « Sites Internet ».

Le *bitcoin* ne jouera pas avant longtemps un rôle équivalent au dollar ou à l'euro

Le *bitcoin* ne sera pas avant longtemps, et peut-être jamais, un véritable concurrent international des grandes monnaies. Les rêves anarchistes ou libertariens de certains ne sont – aujourd'hui – pas sérieux. La raison est simple : il y a par exemple plus de 12 000 milliards de dollars en circulation (ce que les économistes appellent le M2 du dollars) et un peu moins pour l'euro. C'est nécessaire –semble-t-il – à la finance et à l'économie mondiale. Pour que le *bitcoin* puisse concurrencer le dollar ou l'euro, lui qui vaut aujourd'hui au total moins de 200 milliards de dollars, devrait voir son cours multiplié par plus de 60 (car la limitation à 21 millions de *bitcoins* a pour conséquence que seule l'augmentation du cours peut faire varier sensiblement la capitalisation totale).

Ce n'est pas impossible, mais qui peut croire que cela se fera rapidement et sans réaction des États concernés par l'émergence d'un concurrent nuisible à leurs monopoles. Un autre obstacle à cette variation rapide du cours du *bitcoin* est qu'elle entraînerait mécaniquement une augmentation de la consommation d'électricité dépensée par les mineurs pour sa preuve de travail, la conduisant à des niveaux inacceptables, bien supérieurs à ce qu'ils sont déjà et qu'on considère déjà comme une absurdité.

Ces remarques ne sont pas entièrement négatives, car elles n'excluent pas que si le *bitcoin* possède des propriétés intrinsèques très appréciées et préférées à celles du dollar ou de l'euro par un grand nombre d'acteurs économiques (rapidité, fluidité, faible coût des transactions), alors son cours montera inéluctablement, jusqu'à ce que la valeur totale des *bitcoins* atteigne des niveaux comparables à ceux du dollar ou de l'euro.

On peut aussi imaginer qu'une autre monnaie cryptographique pourrait mieux que le *bitcoin* devenir un concurrent des grandes monnaies usuelles. Il faudrait qu'elle ne s'appuie pas sur la preuve de travail (mais par exemple sur la *preuve d'enjeu* ou une de ses variantes, voir plus loin) car la preuve de travail est en définitive est un obstacle à la croissance du cours du *bitcoin* du fait la consommation d'électricité qu'elle provoque et qui est directement liée à son cours et qu'on ne peut imaginer être encore multipliée par 10 ou plus.

S'emparer du *bitcoin* par la force n'est pas aujourd'hui vraiment très cher

Réussir à mettre en place un ensemble de calculateurs qui domineraient le minage des *bitcoins* en produisant plus de 50 % de la puissance de minage (ce qui donne le pouvoir, on le sait, de perturber gravement le fonctionnement de la *blockchain*), n'est pas vraiment coûteux à l'échelle d'un État ou d'une grande entreprise. Le calcul sommaire suivant permet d'évaluer le coût de ce type d'attaques, appelées « attaques 51 % ».

– L'argent dépensé à chaque instant, en tout dans le monde, pour miner les *bitcoins* est en gros équivalent à ce que rapporte le minage. En effet :

- (a) si c'était sensiblement moins, les mineurs se multiplieraient car cela signifierait qu'il y a de l'argent facile à gagner ;
- (b) si c'était sensiblement plus, cela ne vaudrait plus la peine d'investir dans le minage et de le pratiquer, et donc des mineurs se retireraient jusqu'à ce que le rendement du minage redevienne intéressant (cela se produit parfois, et c'est ce qui se passe pour l'or où selon son cours, on ouvre ou ferme les mines aux plus faibles rendements).

– Les *bitcoins* rapportent aujourd'hui environ 6,25 × 6 × 24 × 10 000 × 365 = 3,285 milliards d'euros par an (en supposant un *bitcoin* à 10 000 euros). C'est, en ordre de grandeur, l'investissement maximal exigé pour dominer le minage.

D'autres calculs par exemple basés sur le coût des outils de minage confirment l'ordre de grandeur du prix au plus d'une attaque par la force brute de la *blockchain* du *bitcoin*.

De telles sommes permettraient donc de prendre suffisamment le contrôle de la *blockchain* pour en empêcher le bon fonctionnement et faire perdre toute confiance dans le *bitcoin* qui, n'étant pas régulé, verrait sa valeur s'écrouler en quelques heures. Si l'État américain, par exemple, en donnait l'ordre à l'un de ses services – la NSA à tout hasard – ce serait donc assez facile. À moins que le cours du *bitcoin* n'augmente très sensiblement, cette possibilité de s'emparer de la *blockchain* reste et restera largement à la portée de l'État américain (cela sans avoir à casser les protocoles cryptographiques de signature précédemment évoqués). D'autres États ou entreprises internationales (Apple dispose par exemple de plus de 200 milliards de dollars de cash en réserve) pourraient d'ailleurs aussi vouloir s'emparer de la *blockchain*, puisque ce n'est pas si cher ! Une telle attaque 51 % – avec pour objectif, non pas de s'enrichir, mais seulement de détruire le *bitcoin* ou de faire s'évanouir toute confiance en lui – a été nommée « *Goldfinger Attack* » par une équipe d'économistes de l'université de Princeton. Aujourd'hui nul ne peut faire l'impasse sur ce risque d'effondrement grave de tout le système *bitcoin*, résultant d'une attaque *Goldfinger*.

Le rôle des développeurs n'est pas clair, ni le pouvoir dont ils disposent

Le noyau de développeurs qui travaille à l'amélioration des programmes et protocoles *bitcoin* possède un certain pouvoir sur lui. N'oublions pas qu'en août 2010 un bug laissé dans les programmes avait permis à un petit malin de créer 194 milliards de *bitcoins*. Il fut décidé d'un commun accord par les mineurs de revenir en arrière à un état antérieur de la *blockchain* pour annuler cette création frauduleuse. Ce type de corrections à la suite de la découverte d'un bug est une bonne chose, et cette relative centralisation et réaction instantanée opérée par les mineurs permet d'éviter des catastrophes (toutes ?). Il se trouve que ces mécanismes d'intervention et leur existence sont contraires à l'image qu'on donne presque toujours du *bitcoin* qui serait une monnaie totalement décentralisée et sur laquelle personne n'a de pouvoir. De plus, les décisions de ce type (on parle de « *hardfork* ») consistant à annuler des transactions en annulant certaines pages de la *blockchain* sont devenues plus difficiles à prendre. Cela à cause de la multiplication des mineurs (ce sont eux qui opèrent une sorte de vote pour décider une telle opération) et peut-être aussi à cause de la domination des *pools* de minage chinois aujourd'hui qui rendent toute concertation assez délicate.

Sur ces questions, on lira [BNS] [CEV] dans le « *Pour en savoir plus* », rubrique « Sites Internet ».

Le minage a réellement quelque chose d'absurde

Même si logiquement il se justifie et constitue un élément important du protocole *bitcoin* qu'on ne peut pas éviter ou réformer facilement, le minage des *bitcoins* est de l'argent jeté par les fenêtres. Des milliards de dollars ont été dépensés en électricité et en matériels spécialisés pour résoudre des problèmes mathématiques sans le moindre intérêt : inverser partiellement la fonction de hachage SHA256 ! Il est peut-être possible d'éviter cela en faisant évoluer le protocole *bitcoin*, – d'autres protocoles de minage ont été proposés ou sont à l'étude –, mais ce ne sera pas facile.

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

La preuve d'enjeu fait aussi bien que la preuve de travail sans dépense électrique

En particulier le protocole dénommé « preuve d'enjeu » (« *proof of stake* ») peut se substituer à la preuve de travail pour choisir le nœud validateur (toutes les 10 minutes par exemple). Le réseau Ethereum qui pour l'instant fonctionne avec une preuve de travail, passera prochainement au protocole de preuve d'enjeu. L'idée du protocole qui possède de nombreuses variantes consiste à demander aux nœuds du réseau qui veulent valider les pages, d'engager de l'argent pour se déclarer. Le choix périodique du nœud validateur se fait de manière (quasi-probabiliste) en fonction des sommes engagées plutôt que de manière (quasi-probabiliste) en fonction de la puissance de calcul dans le cas des preuves de travail. On obtient des systèmes ayant à peu près la même sécurité que les systèmes à preuve de travail. De tels systèmes ont été mis en place et fonctionnent très bien (par exemple EOS, Cardano, voir figure **2**) détenant plusieurs milliards de dollars sur leur *blockchains*. Certains défenseurs de la preuve de travail soutiennent que les preuves d'enjeu sont moins résistantes aux attaques. Si c'était vrai, il y aurait eu des attaques pour s'emparer des milliards de dollars déposés sur les *blockchains* à preuve d'enjeu, or de telles attaques ne se sont pas produites.

D'autres méthodes où les nœuds validateurs sont limités en nombre (ce qui permet un grand nombre des transactions par seconde) et connus dispensent aussi de la consommation électrique des preuves de travail. C'est le cas pour XRP (figure **2**), et c'est ce qui était envisagé pour la monnaie cryptographique de LIBRA dont l'idée a été défendue par Facebook. Ces systèmes où on renonce à l'anonymat des validateurs (mais sans nécessairement renoncer à l'anonymat des détenteurs de comptes) sont certainement une voie pour résoudre à la fois le problème du trop petit nombre de transactions opérables par seconde par le réseau *Bitcoin* et le problème de la consommation d'électricité des preuves du travail.

Ce sont vers des systèmes de ce type que s'orienteront les banques centrales si elles se décident à émettre des jetons de type monnaies cryptographiques qui leur permettraient par exemple de faire circuler des dollars numériques ou des euros numériques.

Aujourd'hui, bien que le *bitcoin* reste la monnaie cryptographique dominante (c'est le fameux avantage au premier entrant), on dispose de méthodes qui en corrigent les défauts majeurs. Et les nouvelles crypto-monnaies ayant réellement l'objectif de jouer un rôle majeur dans l'économie mondiale (comme Libra, ou les monnaies cryptographiques de banques centrales) ne peuvent s'envisager qu'en corrigeant les défauts du protocole initial du *bitcoin*. Les fortes sommes d'argent détenues en *bitcoin* ont pour conséquence que ceux qui les contrôlent continuent de soutenir le *bitcoin* parfois contre toute logique (on parle de « maximaliste *bitcoin* ») ce qui freine l'évolution de la situation et même retarde le succès des monnaies cryptographiques.

L'anonymat de Satoshi est un problème ennuyeux

Le fait de ne pas savoir qui est Satoshi Nakamoto nuit au *bitcoin*. Comment faire confiance à un système dont on ne connaît pas l'inventeur (ou le groupe d'inventeurs) qui reste obstinément caché, ayant vraisemblablement réussi à capter une part importante de la richesse créée. On a en effet évalué à 5% au moins la part de *bitcoins* dont disposerait l'inventeur du système. Espérons qu'il finira de lui-même par faire connaître sa véritable identité. Il rendrait service à ceux qui travaillent au développement des monnaies cryptographiques et cherchent à établir la confiance autour d'elles.

Le *bitcoin* est très inégalitaire

Les premiers arrivants disposent d'une part vraiment importante des *bitcoins*. Notre monde économique est aujourd'hui très inégalitaire mais si le *bitcoin* s'imposait comme monnaie internationale (ce qui exige, nous l'avons dit, que sa valeur soit encore multipliée par 50) alors ce serait pire. On a en effet calculé que moins de mille personnes détiennent la moitié des *bitcoins*, ce qui signifie aussi qu'un petit nombre de détenteurs peuvent influer fortement sur les cours, ou même les manipuler (voir [PEO] du « *Pour en savoir plus* »).

Une telle répartition des *bitcoins* n'est pas nécessairement nuisible au bon fonctionnement général du protocole et à sa robustesse, car ceux qui disposent de grandes quantités de *bitcoins* entre leurs mains ont intérêt à ce que les *bitcoins* gardent leur valeur ou en prennent encore plus. On peut donc imaginer qu'ils vont – et peut-être que c'est le cas aujourd'hui – jouer le rôle de régulateurs, assurant le maintien et une meilleure stabilité des cours. Si c'est le cas, le contrôle sur les monnaies exercé aujourd'hui par les États sera, dans le cas du *bitcoin*, passé aux mains de quelques personnes privées !

Le potentiel le plus grand du *bitcoin* est peut-être dans les opérations nouvelles qu'il permet

Le protocole *bitcoin* autorise des opérations plus complexes que le simple transfert de valeurs. C'est peut-être son véritable avenir et sa force potentielle la plus grande. On peut l'utiliser pour organiser des **votes à distance** dont la confidentialité et l'honnêteté seraient garanties cryptographiquement. On peut utiliser la *blockchain* pour **gérer des titres de propriétés ou des contrats**. On peut opérer des transactions avec plusieurs acteurs signant et recevant les *bitcoins*, ou introduire des transactions dont la date de validité est décalée dans le temps, ou soumise à des conditions complexes, etc.

Si le *bitcoin* (ou d'autres crypto-monnaies aux possibilités encore plus étendues comme on travaille à en concevoir aujourd'hui) sait faire ce que les autres monnaies ou moyens de paiement ne savent pas faire, alors il aura en lui-même le pouvoir de développement qui lui assurera de persister et de s'imposer.

7. Devenir du bitcoin

On s'interroge sur ce que va devenir cette monnaie née des mathématiques et des **réseaux pair à pair**. Comme aucune monnaie de ce type n'a jamais existé auparavant, il est vraiment difficile de faire un pronostic et les avis sont partagés. Certains pensent que son cours élevé aujourd'hui est une bulle qui éclatera et ôtera toute valeur aux *bitcoins* : ceux qui en achètent finiront par perdre tout ce qu'ils y mettent.

D'autres soutiennent que le *bitcoin* possède des propriétés telles qu'il gardera toujours un certain intérêt pour mener des transactions rapides, presque sans coût et presque anonymes, ou pour conserver de l'argent à l'abri de l'inflation sous une forme discrète et facile à déplacer. En effet, il est possible de mémoriser votre numéro de compte secret et de tout effacer de votre ordinateur ; ce numéro en tête vous permettra de passer tranquillement toutes les frontières, puis en le réintroduisant à l'aide d'un autre *wallet* sur un autre ordinateur de retrouver vos *bitcoins* où vous le souhaiterez ailleurs dans le monde.

Les monnaies cryptographiques sont utiles pour de multiples raisons. Pour envoyer de l'argent d'un pays à un autre, ce qui intéresse les travailleurs étrangers souhaitant régulièrement faire parvenir de l'argent à leur famille et qu'on exploite aujourd'hui. Pour organiser des plateformes de jeux où on risque de l'argent sans décliner son identité et sans avoir à créer de compte local. Pour disposer de sommes importantes sous un petit volume, voire réduit à rien. Pour spéculer. Pour payer sans avoir de compte bancaire et sans avoir à laisser son identité au vendeur, etc.

Ces propriétés particulières que le *bitcoin* possède pourraient faire persister et croître l'intérêt qu'il suscite et avoir pour effet que son cours s'élèvera au fur et à mesure que les utilisateurs seront plus nombreux.

D'autres encore pensent que l'essentiel est l'idée d'un fonctionnement pair à pair fondé sur un fichier analogue à la *blockchain*,

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

car de tels fichiers permettent de traiter de manière décentralisée un grand nombre de problèmes et d'applications (contrats, votes, certificats, preuves, etc.) et qu'avec le *bitcoin* ou sans lui (s'il ne tient pas), cette idée recèle un énorme potentiel. C'est l'idée des ***blockchains* non basées sur le *bitcoin*** et dont la fonction principale n'est pas la création d'une monnaie.

Mais avant d'envisager ces autres usages possibles de l'idée de *blockchain*, il faut évoquer une catégorie particulière de monnaies cryptographiques qui est devenue importante depuis 3 ans : les « *stablecoins* ».

Les *stablecoins*

L'un des problèmes du *bitcoin*, mais aussi de l'ether (du réseau Ethereum) du ripple (ou XRP), de bitcoinCash et finalement des dix plus importantes monnaies cryptographiques mentionnées à la figure **2** sauf une, est la volatilité de leurs cours. Il n'est pas rare d'observer des variations de cours de 10 % en quelques heures dans un sens ou un autre, et de beaucoup plus si on considère une période de 3 ou 6 mois (entre le 1er octobre 2017 et le 17 décembre 2017 le cours du *bitcoin* a progressé de 351 %). Cela rend attrayantes ces monnaies pour ceux qui veulent spéculer et acceptent de prendre des risques, mais cela décourage ceux qui veulent utiliser ces monnaies numériques pour opérer des échanges de biens ou de marchandises ou qui veulent détenir ces monnaies pour conserver de la valeur. La solution existe et prend de plus en plus d'importance dans le monde des monnaies cryptographiques. Ce sont les ***stablecoins*** dont le Tether est la principale, classée troisième par ordre de capitalisation (figure **2**), et qui aujourd'hui est plus utilisée que le *bitcoin* lui-même pour des opérations par exemple entre plateformes d'échange ou dans le monde de la finance décentralisée. Le Tether est émis par la société Tether-Limited qui assure qu'elle est prête à racheter chaque Tether émis contre 1 dollar, et qui en même temps propose de vendre des Tether à 1 dollar l'unité. La société affirme détenir une réserve de dollars lui permettant de faire face à toute demande d'échange Tether contre dollars. Noter que le cours du Tether indiqué sur la figure **2** est 0,998692 dollar, proche à 0,14 % de 1 dollar. Plus de neuf milliards de Tethers circulent aujourd'hui. La contrepartie (ou collatéral) que prétend détenir Tether-Limited qui jusqu'à maintenant s'est révélée fiable a pour conséquence que le cours du Tether ne peut varier sensiblement (sauf en de rares moments par exemple si des doutes surgissent au sujet de la société Tether-Limited). Vous ne gagnerez pas d'argent en détenant des Tethers, mais vous serez assuré aussi de ne pas en perdre. De ce fait, pour détenir et protéger de la valeur, ou pour faire des affaires en utilisant les facilités qu'offrent les crypto-monnaies, c'est un outil idéal : il est aussi stable que le dollar qui est régulé et peut circuler avec une fluidité bien supérieure.

Concernant l'idéal de décentralisation, le Tether est en recul sensible comparé au *bitcoin* qui lui ne s'appuie sur aucune société. Cependant, sauf pour l'achat et la vente contre des dollars à un contre un où la société Tether-Limited joue un rôle, la circulation des Tethers entre détenteurs fonctionne indépendamment de Tether-Limited grâce au principe des *blockchain*s et donc de manière décentralisée, non censurable (personne ne peut refuser une transaction dès l'instant où votre compte est correctement approvisionné) et en assurant un assez bon anonymat.

La monnaie Libra que Facebook a tenté de créer avec d'autres firmes auquel il s'est associé en 2019 aurait fonctionné comme un *stablecoin*. Aujourd'hui le projet Libra a évolué vers un système multi-devises de *stablecoins* dont on attend prochainement la mise en fonctionnement. Il est certain que ces monnaies cryptographiques non spéculatives et préservant plusieurs propriétés importantes du *bitcoin* joueront un rôle croissant dans l'économie mondiale qui a besoin de la souplesse et de la rapidité de circulation des monnaies fondées sur des *blockchains* même si elles renoncent à certaines propriétés de décentralisation... sans renoncer à toutes.

Les monnaies qu'envisagent de créer les banques centrales et qu'elles étudient activement aujourd'hui seront toutes des sortes de *stablecoins*.

8. Autres *blockchains* possibles

La définition générale d'une *blockchain* pourrait être : une ***blockchain*** est un fichier (a) partagé sur un réseau pair à pair (c'est-à-dire reproduit et conservé en chaque nœud), (b) sécurisé par de bonnes primitives cryptographiques, (c) qui n'évolue que sous le contrôle d'une communauté ayant un intérêt à son existence, (d) où rien ne s'efface et (e) qui accroît son contenu par ajout périodique de pages chaînées les unes aux autres. En disposer est un moyen sûr de partager de l'information et de créer de la confiance entre des acteurs éloignés, qui éventuellement ne se connaissent même pas.

Satoshi Nakamoto a inventé et astucieusement mis en forme cette idée en lui donnant une implémentation particulière et ouverte : de nouveaux acteurs peuvent intervenir à chaque instant, d'autres peuvent se retirer, tout y est public, rien n'y est chiffré. Cependant, créer des monnaies numériques décentralisées n'est pas le seul usage qu'on peut faire de ce type de constructions logicielles à base de réseaux pair à pair, et de nombreux traits particuliers de la *blockchain bitcoin* peuvent être discutés et modifiés.

C'est ce qu'on a compris progressivement depuis que le *bitcoin* existe et qu'il tient solidement, quels qu'en soient les usages qu'on en fait et les trafics qui l'utilisent. Le *bitcoin* est de l'argent liquide numérique ; doit-on s'étonner alors que des malfrats s'en servent ? Il ne faut cependant pas confondre les trafics dans lesquels il joue un rôle (comme l'argent liquide en euros ou en dollars dans toutes sortes de trafics du même genre) avec des défauts ou des faiblesses du protocole *bitcoin* [H 5 340]. Les risques et incertitudes portant sur le protocole ont été évoqués, il faut en avoir conscience, mais il faut noter aussi que pour l'instant il n'y a jamais eu de dysfonctionnements graves de cette machine *bitcoin* qui tourne, répartie en environ 10 000 points depuis plus de 10 ans et a créé plus de cent cinquante milliards d'euros en valeur. Le *bitcoin* tient bien, prouvant que le concept de *blockchain* est robuste et que, même dans le cas le plus difficile des *blockchains* publiques, on peut l'utiliser.

Les banques et le monde de la finance en particulier sont intéressés par l'idée de la *blockchain* qui est devenue une technologie nouvelle de développement logiciel. Aujourd'hui, des études sont menées partout dans le monde pour tester et expérimenter des *blockchains* diverses.

En particulier, l'idée des ***blockchains* privées** (ou *blockchain* de consortium) a vu le jour. Un ensemble réduit d'acteurs, par exemple 50 banques voulant faciliter entre elles les échanges sécurisés (d'informations, de titres ou de valeurs) peuvent juger intéressant de créer un fichier partagé détenant des informations sur les échanges qu'elles effectuent d'heure en heure. Un réseau des 50 nœuds dans un tel cas leur permet de mettre à jour en continu ou périodiquement les données sur leurs échanges et d'en calculer le bilan instantané. La gestion d'une telle *blockchain* privée, à laquelle personne en dehors des 50 banques ne pourrait accéder, établirait une confiance solide entre elles, puisque tout y sera enregistré et calculé 50 fois, et serait l'objet d'un consensus permanent, renouvelé et consolidé entre tous. Pour une telle *blockchain*, pas besoin de minage et donc de la terrible compétition qui pousse à dépenser des sommes importantes en électricité et en dispositifs spécialisés de calcul. En effet, pas besoin de système d'incitation à surveiller et gérer la *blockchain* : c'est l'intérêt de chacun des 50 acteurs de mener cette surveillance et ils le feront volontiers. Déterminer qui ajoute la page nouvelle (si on adopte un système d'ajout périodique de pages) peut se faire par

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

un système de tirage aléatoire équitable **cryptographiquement sûr** (dont l'équité est garantie par des primitives cryptographiques), ou même plus simplement à tour de rôle.

Énumérons, sans prétendre à l'exhaustivité, les applications possibles de la technologie *blockchain* vue sous sa forme souple et pouvant s'éloigner sensiblement de celle du *bitcoin* :

– **dépôt d'informations datées** permettant d'attester qu'une information était bien détenue par une certaine personne ou entreprise à un instant donné. De tels dépôts pourraient se substituer aux enveloppes Soleau de l'INPI. L'information déposée peut être chiffrée ; quand on voudra rendre public le contenu, on dévoilera la clé. Elle peut aussi être signée. On peut ne déposer sur la *blockchain* que l'empreinte du fichier. On perd alors l'indestructibilité, mais on a une parfaite méthode d'horodatage ;

– **courrier électronique**. On écrit les messages sur la *blockchain* avec des informations sur celui qui envoie et le destinataire. Les messages peuvent être chiffrés ou non, signés ou non. Les messages seront infalsifiables et indestructibles, ce qui dans certaines situations sera utile. On peut, pour les courriers trop volumineux, ne déposer que l'empreinte de ce qu'on envoie (comme précédemment, on perd l'indestructibilité) ;

– **dépôt de diplômes**. La *blockchain* serait gérée par toutes les universités et écoles. Elles seules pourraient y écrire, mais tout le monde pourrait lire les informations. Les informations déposées devraient être signées (par un système à double clé comme pour les transactions *bitcoin*) pour en assurer l'authenticité ;

– ***smart contract***. Des opérations plus complexes que de simples transactions sont possibles avec *bitcoin* : signatures multiples, déclenchement retardé, ou conditionnels, etc. La *blockchain* Ethereum permet cela et bien plus, puisqu'on peut y déposer des programmes (appelés « *smart contacts* ») écrits dans un langage Turing-complet. Aujourd'hui il s'agit d'une technologie un peu fragile et sans doute risquée comme les problèmes graves qui se sont manifestés en 2016 l'ont montré. Une fois bien mis au point, ce type de *blockchains* très générales et puissantes jouera certainement un rôle important. Les *Ethers* créés par Ethereum valent, en juin 2020, plus de 20 milliards d'euros ; cette *blockchain* avant-gardiste réussit à être la seconde en valeur derrière *bitcoin* ! Les *smart contracts* qu'elle fait fonctionner peuvent être le support d'autres monnaies cryptographiques ;

– **certificats de propriété, cadastres, engagements, assurances, opérations financières**. Toutes sortes de documents liants des acteurs humains ou économiques les uns aux autres peuvent être gérés par une *blockchain* qui crée la confiance entre les utilisateurs, autant que les systèmes usuels d'aujourd'hui fonctionnant à l'aide de tiers de confiance (notaires, huissiers, administrations, banques, etc.) dont le rôle est probablement appelé à se réformer ;

– **votes**. Des systèmes de votes électroniques ont été conçus pour fonctionner avec des *blockchains*. Une grande variété de solutions existe selon ce qu'on demande au système de votes ;

– **brevets, certificats d'antériorité, informations certifiées** concernant le suivi d'objets (œuvres d'art par exemple). Le fait de déposer ce type d'informations sur un fichier infalsifiable et indestructible est un moyen d'assurer la pérennité des informations en même temps qu'on les date ;

– **jeux** prouvablement équitables, **paris, plateforme de prédiction** ;

– **fonds d'investissement automatiques et décentralisés** : ils reçoivent de l'argent, ils organisent des votes, ils investissent dans les projets sélectionnés par les votes. C'est un tel fonds, nommé THE DAO, qui a connu des ennuis graves en juin 2016. Il fonctionnait sur *Ethereum* (dont le cœur n'était pas concerné).

Insistons pour terminer sur un point : concevoir une application *blockchain* exige de faire un grand nombre de choix :

– on peut soit utiliser les *blockchains* existantes et y écrire des informations qui seront datées et qu'on sera certain d'y retrouver. De nombreuses applications utilisent ainsi la *blockchain* du *bitcoin* (souvent en y écrivant seulement l'empreinte des informations qu'on veut certifier et dater) ;

– on peut créer des *blockchains* publiques comme celle du *bitcoin* mais différentes en prévoyant un système d'incitation pour que certains utilisateurs prennent en charge la surveillance et la gestion de la *blockchain*, système qui peut être différent des preuves de travail du *bitcoin*.

Si on opte pour une *blockchain* simplifiée (par exemple parce que le problème de l'incitation à gérer les nœuds du réseau est résolu par l'intérêt même des acteurs utilisant la *blockchain*, voir l'exemple du réseau des 50 banques évoqué plus haut) alors reste encore à fixer plusieurs paramètres :

– la *blockchain* sera-t-elle totalement publique ? Ou seulement publique en lecture, et privée en écriture ? Ou d'usage réservé à une collectivité réduite ? Cette collectivité pourra-t-elle évoluer ? Comment ?

– écrira-t-on en clair ou en chiffrant ce qu'on dépose (ou avec les deux méthodes, selon les opérations) ?

– signera-t-on ce qu'on y écrit ?

– sera-t-elle associée à une monnaie cryptographique ? Quelles en seront alors les caractéristiques ?

– quel système d'incitation sera prévu pour encourager la création de nœuds détenteurs de la *blockchain* et s'occupant du contrôle de ses mises à jour ? Comment éviter la concentration du pouvoir sur la *blockchain* aux mains de quelques acteurs ?

– envisage-t-on qu'il n'y ait aucun contrôle centralisé (comme pour *bitcoin*), ou fixe-t-on un nombre limité d'administrateurs de la *blockchain* ?

– souhaite-t-on limiter (en taille, en format) ce qui est écrit sur la *blockchain* :

- on peut envisager de n'écrire que les empreintes des fichiers qui seraient ailleurs,
- on peut envisager que la *blockchain* soit découpée et que chaque nœud principal n'en garde qu'un partie ;

– quelles sont précisément les primitives cryptographiques utilisées ? Que prévoit-on pour les changer si cela se révèle nécessaire ?

– la programmation des actions sur la *blockchain* est-elle limitée (*bitcoin*) ou Turing-complète (*Ethereum*), ou autres ?

– comment se font les évolutions (mises à jour, gestion de crise, nettoyage de la *blockchain* pour en limiter la taille, etc.) ?

9. Conclusion

La technologie *blockchain* est née avec le *bitcoin* qui reste aujourd'hui l'application majeure et l'exemple le plus remarquable de sa mise en œuvre. Il est cependant apparu qu'à côté de la réussite de cette *blockchain* particulière, bien des variantes sont possibles, certaines plus complexes, plus puissantes (*Ethereum*), certaines plus simples (les *blockchains* privées), certaines évitant la consommation électrique de la preuve de travail grâce aux preuves d'enjeu, certaines moins spéculatives (*stablecoins*). C'est un volumineux ensemble de méthodes et d'applications qui est en train de naître et qu'on est en train de perfectionner en s'inspirant de près ou de loin de la construction inattendue de Satoshi Nakamoto. Il ne fait aucun doute que le rôle de cette technologie nouvelle sera déterminant dans le monde de réseaux qui est le nôtre, où les outils permettant de créer des échanges sécurisés d'informations, de valeurs et de confiance seront des clés du progrès. À moyen terme on verra naître des crypto-monnaies de banques centrales dont les propriétés sont à l'étude et qui reprendront en partie seulement celles du *bitcoin*.

10. Glossaire

Bitcoin

Désigne à la fois le protocole général permettant l'émission et la gestion de la monnaie numérique décentralisée créé par Satoshi Nakamoto en 2009, et les unités de compte de cette monnaie qui, en 2020, valaient entre 800 et 1 200 euros chacune.

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

Blockchain (on dit parfois *chaîne de blocs*)

Fichier partagé reproduit en chaque nœud du réseau pair à pair *bitcoin* (qui comporte environ 10 000 nœuds). Plus généralement une *blockchain* est un fichier partagé sur un réseau pair à pair qui évolue par ajout de pages (appelés « bloc ») liées les unes aux autres (on dit aussi « chaînées ») et qui est surveillé par tous les nœuds du réseau. Les pages sont liées les unes aux autres parce que par exemple chaque page nouvelle commence par l'empreinte (le *hash*) de l'état précédent de la *blockchain*. Ces liens interdisent toute modification d'une *blockchain* en la rendant immédiatement apparente.

DAO (organisation autonome décentralisée) ; *Decentralised Autonomous Organisation*

Programme fonctionnant à l'identique sur une multitude de machines d'un réseau pair à pair et effectuant un travail autonome sans contrôle centralisé. Le *bitcoin* est une DAO, *Ethereum* aussi, mais surtout, *Ethereum* permet facilement la création de nouvelles DAO.

Ethereum

Désigne un protocole imitant le *bitcoin*, mais autorisant la programmation d'opérations plus complexes que des transactions d'*Ethers* (la monnaie cryptographique engendrée par *Ethereum*).

Hachage ; *hash*

Algorithme transformant un fichier A en un autre fichier B, en général d'un format court fixé (par exemple de 256 bits). Le résultat produit se nomme « l'empreinte » du fichier A ou le *hash* du fichier A. Les fonctions de hachage sont conçues pour qu'il soit impossible en pratique de les inverser : connaissant une image possible B choisie au hasard (par exemple 256 bits tirés au hasard) on ne peut pas trouver en temps raisonnable un A dont l'empreinte soit B.

Mineur de *bitcoins*

Machine sur le réseau *bitcoin* (ou plus généralement d'une monnaie cryptographique) ou propriétaire de la machine qui participe au fonctionnement du réseau, soit seul, soit associé à d'autres en un *pool* de minage. Le *leader* du *pool* détient une copie de la *blockchain*. Il y a environ 100 000 mineurs de *bitcoins* organisés en environ 10 000 *pools* de minage.

***Pool* de minage**

Association de mineurs de *bitcoins* qui préfèrent travailler à plusieurs plutôt que seul dans le but de gagner plus souvent, même s'ils doivent partager les gains.

Porte-monnaie ou **portefeuille** ou **wallet** ; *wallet*

Programme qu'un utilisateur du *bitcoin* ou d'une monnaie cryptographique installe sur sa machine ou son *smartphone* et qui lui permet de créer et de gérer un compte détenant des *bitcoins* ou des unités de comptes de la monnaie cryptographique considérée.

Preuve de travail

Question posée à un programme qu'il peut résoudre, mais qu'il ne peut pas résoudre rapidement. On utilise les preuves de travail pour forcer un programme à attendre où dans le cas du *bitcoin* pour opérer un choix entre divers programmes mis en concurrence : le premier qui résout la question gagne.

Preuve d'enjeu

Protocole permettant de rémunérer les nœuds validateurs d'une *blockchain* basée sur un engagement d'unités monétaires plutôt que sur une compétition de calcul, ce qui évite la grave consommation électrique des monnaies à base de Preuve de travail.

Stablecoin

Monnaie cryptographique qu'on peut acheter à un prix fixé (par exemple 1 dollar pour une unité) et dont un acteur particulier assure garder en réserve la contrepartie (ou collatéral) pour garantir les échanges en retour d'une unité contre un dollar. Le Tether est la plus importante des *stablecoins*.

11. Infographie

Cette infographie, synthèse graphique d'une partie du présent article, reprend en images les points essentiels et les informations à retenir sur les *blockchains* : les principes, les avantages, la cryptomonnaie ***Bitcoin*** et les applications potentielles de cette technologie.

Elle est accessible en suivant le lien : http://cdn.techniques-ingenieur.fr/natifs/h5538/ih5538.pdf.

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

Monnaies cryptographiques et *blockchains*

Créer de la confiance

par **Jean-Paul DELAHAYE**

Professeur émerite à l'université de Lille, Centre de recherche en informatique, signal et automatique de Lille (CRISTAL), UMR CNRS 9189, France

POUR EN SAVOIR PLUS

Sources bibliographiques

[1] ANTONOPOULOS (A.). – *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc. (2014 et 2018).

[2] ANTONOPOULOS (A.). – *Mastering ethereum: building smart contracts and dapps*. O'reilly Media (2018).

[3] DELAHAYE (J.-P.). – *Comment déjouer les points faibles du* Bitcoin, The Conversation, Décembre 2019. https://theconversation.com/comment-dejouer-les-points-faibles-du-bitcoin-126875.

[4] DELAHAYE (J.-P.). – *Mathématiques et mystère*. Éditions Belin, [Trois chapitres consacrés respectivement au *bitcoin*, aux *blockchains*, aux preuves de travail (2016).

[5] DELAHAYE (J.-P.). – *Du* bitcoin *à Ethereum : l'ordinateur-monde*, Pour la science, pages 104-109, novembre 2016.

[6] DELAHAYE (J.-P.). – *Les preuves de travail*. Pour la science, p. 86-91, avril 2014.

[7] DELAHAYE (J.-P.). – Bitcoin, *la crypto-monnaie*. Pour la science, p. 76-81, déc. 2013.

[8] FAVIER (J.) et al. – Bitcoin, *Métamorphoses. De l'or des fous à l'or numérique ?* Dunod (2018).

[9] HERLIN (P.). – *Apple,* Bitcoin*, Paypal, Google : la fin des banques*, Eyrolles (2015).

[10] KROLL (J.) et al. – *The economics of* bitcoin *mining, or* bitcoins *in the presence of adversaries*, 12th Workshop on the economics of information security (2013).

[11] LANDAU (J.-P.) et al. – *Les crypto-monnaies, rapport au ministre de l'Économie et des Finances*, 4 juillet 2018 : https://bit.ly/2UXAZqn

[12] MOUGAYAR (W.). – *The business* blockchain*, promise, practice, and applications of the next internet technology*, Wiley (2016).

[13] NAKAMOTO (S.). – Bitcoin *: a peer-to-peer electronic cash system* (2008).

[14] NARAYANAN (A.) et al. – Bitcoin *and cryptocurrency technologies*, Princeton University Press (2016).

[15] OPECST (Office parlementaire d'évaluation des choix scientifiques et technologiques). – *Les enjeux technologiques des* blockchains, (2018) : http://www.senat.fr/rap/r17-584/r17-5841.pdf.

[16] SWAN (M.). – Blockchain*, blueprint for a new economy*, O'Reilly (2016).

[17] WATTENHOFER (R.). – *The science of the* blockchain, Inverted Forest Publishing (2016).

À lire également dans nos bases

FOUQUE (P.A.). – *Cryptographie appliquée*. [H 5 210] Sécurité des systèmes d'information (2003).

MAGNIN (N.). – *Internet et cybercriminalité*. [H 5 340] Sécurité des systèmes d'information (2016).

RAYNAL (F.). – *Canaux cachés*. [H 5 860] Sécurité des systèmes d'information (2003).

RIBIERE (G.). – *Paiement sécurisé sur internet avec le protocole SET*. [H 3 578] Sécurité des systèmes d'information (1998). Article archivé.

PLADEAU (B.) et SAIF (A.). – *Sécurité du paiement mobile NFC*. [H 3 580] Internet des objets (2013).

CHABRIDON (S.), MAISONEUVE (J.) et SIMON (F). – *Sûreté de fonctionnement des applications en réseau*. [H 5 850] Sécurité des systèmes d'information (2004).

Sites internet

[BBU] The 184 Billion BTC Bug : https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/ (page consultée le 27 juin 2020)

[BLN] Lightning-Network : https://bitconseil.fr/bitcoin-lightning-network-histoire-fonctionnement/ (page consultée le 27 juin 2020)

[BNS] *Bitcoin* Network Shaken by *Blockchain* Fork : http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/ (page consultée le 27 juin 2020)

[CEV] Vulnerabilities : CVE-2010-5139 https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures#CVE-2010-5139 (page consultée le 27 juin 2020)

[CHOI] Choisir votre portefeuille *bitcoin* : https://bitcoin.org/fr/choisir-votre-porte-monnaie (page consultée le 27 juin 2020)

[DEL] *Bitcoin*, *Blockchains*, Cryptomonnaies : https://www.cristal.univ-lille.fr/profil/jdelahay#page4 (page consultée le 26 juin 2020)

[PEO] 927 People Own Half Of All *Bitcoins* : http://www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12 (page consultée le 27 juin 2020)

[PLA] Plateforme d'échange *bitcoin* : https://bitcoin.fr/acheter-bitcoin/ (page consultée le 27 juin 2020)

[STA] Stablecoins : https://www.bilan.ch/opinions/yves-bennaïm/stablecoins-cryptomonnaies-stables (page consultée le 27 juin 2020).

[TRAN1] Transaction : https://en.bitcoin.it/wiki/Transaction (page consultée le 27 juin 2020)

[TRAN2] Transactions : https://bitcoin.org/en/developer-guide#transactions (page consultée le 27 juin 2020)

Parution : décembre 2020 - Ce document a ete delivre pour le compte de 7200055771 - techniques de l'ingenieur // romain LELOUP // 2.59.188.28

Copyright © – Techniques de l'Ingénieur – Tous droits réservés

TECHNIQUES DE L'INGÉNIEUR

GAGNEZ DU TEMPS ET SÉCURISEZ VOS PROJETS EN UTILISANT UNE SOURCE ACTUALISÉE ET FIABLE

Techniques de l'Ingénieur propose la plus importante collection documentaire technique et scientifique en français !

Grâce à vos droits d'accès, retrouvez l'ensemble des **articles et fiches pratiques de votre offre, leurs compléments et mises à jour,** et bénéficiez des **services inclus.**

RÉDIGÉE ET VALIDÉE PAR DES EXPERTS	MISE À JOUR PERMANENTE	100 % COMPATIBLE SUR TOUS SUPPORTS NUMÉRIQUES	SERVICES INCLUS DANS CHAQUE OFFRE

- **+ de 350 000 utilisateurs**
- **+ de 10 000 articles de référence**
- **+ de 80 offres**
- **15 domaines d'expertise**

- **Automatique - Robotique**
- **Biomédical - Pharma**
- **Construction et travaux publics**
- **Électronique - Photonique**
- **Énergies**
- **Environnement - Sécurité**
- **Génie industriel**
- **Ingénierie des transports**
- **Innovation**
- **Matériaux**
- **Mécanique**
- **Mesures - Analyses**
- **Procédés chimie - Bio - Agro**
- **Sciences fondamentales**
- **Technologies de l'information**

Pour des offres toujours plus adaptées à votre métier, découvrez les offres dédiées à votre secteur d'activité

Depuis plus de 70 ans, Techniques de l'Ingénieur est la source d'informations de référence des bureaux d'études, de la R&D et de l'innovation.

www.techniques-ingenieur.fr

CONTACT : Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com

TECHNIQUES DE L'INGÉNIEUR

LES AVANTAGES ET SERVICES compris dans les offres Techniques de l'Ingénieur

ACCÈS

Accès illimité aux articles en HTML
Enrichis et mis à jour pendant toute la durée de la souscription

Téléchargement des articles au format PDF
Pour un usage en toute liberté

Consultation sur tous les supports numériques
Des contenus optimisés pour ordinateurs, tablettes et mobiles

SERVICES ET OUTILS PRATIQUES

Questions aux experts*
Les meilleurs experts techniques et scientifiques vous répondent

Articles Découverte
La possibilité de consulter des articles en dehors de votre offre

Dictionnaire technique multilingue
45 000 termes en français, anglais, espagnol et allemand

Archives
Technologies anciennes et versions antérieures des articles

Impression à la demande
Commandez les éditions papier de vos ressources documentaires

Alertes actualisations
Recevez par email toutes les nouveautés de vos ressources documentaires

*Questions aux experts est un service réservé aux entreprises, non proposé dans les offres écoles, universités ou pour tout autre organisme de formation.

ILS NOUS FONT CONFIANCE

AgroParisTech · AIRBUS · cea · CESI Enseignement Supérieur et Formation Professionnelle · cnes Centre National d'Études Spatiales · CSTB le futur en construction · ENGIE · GE · L'ORÉAL · Leroy-Somer · École Polytechnique Université Paris-Saclay · SAFRAN Aerospace Defence Security · Sagemcom · SAINT-GOBAIN · Schneider Electric · THALES · TOTAL · Valeo · VEOLIA · Wallonie · SPW Service public de Wallonie

www.techniques-ingenieur.fr

CONTACT : Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com

TECHNIQUES DE L'INGÉNIEUR

GAGNEZ DU TEMPS ET SÉCURISEZ VOS PROJETS EN UTILISANT UNE SOURCE ACTUALISÉE ET FIABLE

Techniques de l'Ingénieur propose la plus importante collection documentaire technique et scientifique en français !

Grâce à vos droits d'accès, retrouvez l'ensemble des **articles et fiches pratiques de votre offre, leurs compléments et mises à jour,** et bénéficiez des **services inclus.**

RÉDIGÉE ET VALIDÉE PAR DES EXPERTS	MISE À JOUR PERMANENTE	100 % COMPATIBLE SUR TOUS SUPPORTS NUMÉRIQUES	SERVICES INCLUS DANS CHAQUE OFFRE

- **+ de 350 000 utilisateurs**
- **+ de 10 000 articles de référence**
- **+ de 80 offres**
- **15 domaines d'expertise**

- **Automatique - Robotique**
- **Biomédical - Pharma**
- **Construction et travaux publics**
- **Électronique - Photonique**
- **Énergies**
- **Environnement - Sécurité**
- **Génie industriel**
- **Ingénierie des transports**
- **Innovation**
- **Matériaux**
- **Mécanique**
- **Mesures - Analyses**
- **Procédés chimie - Bio - Agro**
- **Sciences fondamentales**
- **Technologies de l'information**

Pour des offres toujours plus adaptées à votre métier, découvrez les offres dédiées à votre secteur d'activité

Depuis plus de 70 ans, Techniques de l'Ingénieur est la source d'informations de référence des bureaux d'études, de la R&D et de l'innovation.

www.techniques-ingenieur.fr

CONTACT : Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com

TECHNIQUES DE L'INGÉNIEUR

LES AVANTAGES ET SERVICES compris dans les offres Techniques de l'Ingénieur

ACCÈS

Accès illimité aux articles en HTML
Enrichis et mis à jour pendant toute la durée de la souscription

Téléchargement des articles au format PDF
Pour un usage en toute liberté

Consultation sur tous les supports numériques
Des contenus optimisés pour ordinateurs, tablettes et mobiles

SERVICES ET OUTILS PRATIQUES

Questions aux experts*
Les meilleurs experts techniques et scientifiques vous répondent

Articles Découverte
La possibilité de consulter des articles en dehors de votre offre

Dictionnaire technique multilingue
45 000 termes en français, anglais, espagnol et allemand

Archives
Technologies anciennes et versions antérieures des articles

Impression à la demande
Commandez les éditions papier de vos ressources documentaires

Alertes actualisations
Recevez par email toutes les nouveautés de vos ressources documentaires

*Questions aux experts est un service réservé aux entreprises, non proposé dans les offres écoles, universités ou pour tout autre organisme de formation.

ILS NOUS FONT CONFIANCE

AgroParisTech · AIRBUS · cea · CESI Enseignement Supérieur et Formation Professionnelle · cnes Centre National d'Études Spatiales · CSTB le futur en construction · ENGIE · GE · L'ORÉAL · Leroy-Somer · École Polytechnique Université Paris-Saclay · SAFRAN Aerospace Defence Security · Sagemcom · SAINT-GOBAIN · Schneider Electric · THALES · TOTAL · Valeo · VEOLIA · Wallonie · SPW Service public de Wallonie

www.techniques-ingenieur.fr

CONTACT : Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com