paiement de la location, le transfert vers votre compte de l'argent reçu, la détermination du code pour l'ouverture de la porte, sa mise en fonctionnement pendant un mois, tout cela sera géré automatiquement par le programme déposé sur la blockchain de l'ordinateur-monde. Personne ne pourra tricher avec ses engagements, ni le propriétaire ni le locataire. (Pour d'autres applications, voir http://dapps.ethercasts.com.)

Si l'utilisation des programmes sur la blockchain n'exigeait aucune contrepartie, on pourrait y faire fonctionner un programme qui tourne indéfiniment et consomme la puissance des ordinateurs du réseau. Sans moyen de freiner cette consommation de puissance, on arriverait à saturation et il serait facile de mettre en panne le réseau tout entier par l'introduction délibérée de programmes exécutant des calculs excessivement gourmands en puissance qu'on ferait fonctionner sans retenue – une attaque par « déni de service ». C'est pourquoi a été prévu un mécanisme qui interdit cela. Lorsqu'on demande à utiliser un programme déposé sur la blockchain, il faut associer à cette demande une certaine somme, très faible, mais cruciale pour le bon fonctionnement de l'ensemble du système.

Ces sommes dépensées par les utilisateurs d'un programme récompensent des membres du réseau, les nœuds principaux ou « mineurs », qui organisent l'évolution et le contrôle de la blockchain. Les autres utilisateurs se contentent de profiter de l'ordinateur-monde sans participer à son contrôle. Les commissions empêchent les programmes trop gourmands en puissance de tout faire s'effondrer, encouragent les programmes économes en calcul, interdisent les attaques par déni de service et incitent à participer à la surveillance de la blockchain et donc à l'exécution commune de tous les programmes qu'elle porte.

Ajoutons que les mineurs fixent un prix pour les opérations qu'ils exécutent sur la blockchain et si le prix que propose un utilisateur simple de programme est trop faible, les opérations de ce programme attendent. L'utilisateur d'un programme doit proposer une commission raisonnable pour que sa

Bitcoin et Ethereum

Le réseau pair à pair du bitcoin, qui a donné naissance à la monnaie bitcoin, a quelques défauts que le réseau Ethereum, dont est issue la monnaie ether, a tenté de corriger. Voici quelques points de comparaison.

– Le nombre total de bitcoins qui seront émis est 21 millions, et leur émission va en décroissant : aujourd'hui, 12,5 bitcoins sont émis toutes les 10 minutes. Les ethers sont émis à raison de 5 toutes les 12 secondes, et ce rythme restera inchangé. Le nombre d'ethers en circulation continuera donc de croître indéfiniment, mais le nombre d'ethers émis par an sera de plus en plus faible comparé au nombre d'éthers déjà en circulation. La pression d'inflation créée par les nouvelles émissions tendra donc vers zéro, comme pour le bitcoin.

– L'ordinateur-monde du bitcoin ne peut qu'effectuer des transactions entre comptes : sa blockchain est une liste ordonnée de transactions. L'ordinateur-monde d'Ethereum effectue des opérations plus complexes. Sa blockchain contient des transactions et des programmes qui sont exécutés sans que personne ne puisse en prendre le contrôle ou les arrêter. Cela permet donc facilement la création d'organisations autonomes décentralisées (DAO), outil de base de la création de confiance entre entités indépendantes.

– La taille des pages de la blockchain du bitcoin est limitée et exige un accord entre les mineurs pour évoluer, accord introuvable aujourd'hui. La taille des pages de la blockchain Ethereum n'est pas bornée.

– Le nombre de transactions par seconde que peut traiter le réseau bitcoin est d'environ 5. Pour Ethereum, c'est environ trois fois plus.

– Le coût d'une transaction entre comptes bitcoin est en principe gratuit, sauf qu'il faut accepter de payer une commission directement liée à la taille de la transaction pour qu'elle soit validée (cette obligation récente résulte du problème de la taille bornée des pages de la blockchain). Le coût d'une transaction pour l'ether dépend de sa complexité et de l'utilisation qu'elle fait des ressources des machines exécutant les programmes.

- La valeur des bitcoins en circulation est aujourd'hui (en septembre 2016) dix fois supérieure à celle des ethers.

- Les équipes travaillant autour du bitcoin sont sensiblement plus nombreuses que celles travaillant pour l'ether.

– Le procédé d'incitation à participer à la surveillance de la blockchain du bitcoin, appelé « preuve de travail », a conduit au développement de puces spécialisées (ASIC) et à une compétition, jugée absurde, provoquant une dépense électrique considérable et une concentration des mineurs aujourd'hui majoritairement en Chine. Le procédé équivalent pour Ethereum ne permet pas, semble-t-il, le développement de puces spécialisées et évite donc plusieurs des inconvénients du bitcoin.

© Fat Jackey ; Anastasiia Bakal/shutterstock.com

demande soit prise en compte. Un marché s'établit entre les mineurs et les utilisateurs. Le système, subtil, est fondé sur des idées économiques qui y jouent un rôle régulateur. Ces constructions informatiques modernes que sont les ordinateurs à blockchain ont, en leur cœur même, des unités de valeur économique qu'ils manipulent et sans lesquelles ils ne pourraient pas exister. Il faut maîtriser une forme d'« économie numérique fondamentale » pour concevoir les ordinateurs à blockchain et cela implique en particulier que les programmes déposés sur la blockchain constituent eux-mêmes des acteurs économiques.

Limites et dangers divers

Tout ce que nous avons dit est très réjouissant et semble parfait… en théorie. La délicatesse et la fragilité de ces constructions, on s'en doute, créent des risques et des difficultés. Cette informatique du futur est dans une phase expérimentale qui n'exclut pas les accidents, voire les catastrophes.

Citons six points délicats pour lesquels des progrès sont à faire avant d'envisager une utilisation à grande échelle des ordinateurs à blockchain :

– l'accroissement de la taille de la blockchain ne doit pas être sans limite, de même que la quantité de calcul exécutée par les mineurs d'un ordinateur à blockchain. On espère profiter de l'augmentation de la puissance des dispositifs informatiques, qui, selon la loi de Moore, double tous les deux ans. Cependant, cela ne permet pas tout, d'autant que la loi de Moore s'essouffle. Le trop grand succès d'un ordinateur-monde provoquerait un problème d'encombrement, voire le paralyserait ;

– les algorithmes cryptographiques utilisés pour assurer l'intégrité de la blockchain, la signature des transactions et le bon fonctionnement d'un réseau pair à pair ne sont pas sûrs à 100 %. L'exploitation d'une faille dans l'un d'eux pourrait tout démolir, d'où le soin particulier qui doit présider à leur choix et la nécessité de prévoir des procédures efficaces de substitution d'un algorithme par un autre en cas de faiblesse identifiée ;

– les programmes, même s'ils sont publics, ne sont pas nécessairement sans erreurs. Leurs bugs peuvent entraîner de graves dysfonctionnements, voire autoriser un pirate ayant repéré l'un d'eux à s'emparer de l'argent stocké dans le compte d'une DAO.

C'est ce qui s'est produit le 17 juin 2016, quand l'exploitation d'une erreur dans le programme d'une DAO de la blockchain d'Ethereum a permis à un programmeur malin (resté anonyme) de s'emparer temporairement de l'équivalent de 50 millions d'euros. Heureusement, le pirate informatique n'a pas pu les faire sortir de la blockchain et en profiter. Une opération appelée *hard fork* a permis de rendre l'argent déplacé à ceux à qui il appartenait, et tout est rentré dans l'ordre le 9 juillet, à la nuance près que des utilisateurs insatisfaits de la méthode de traitement du problème ont donné naissance à une version concurrente d'Ethereum. La leçon de cette catastrophe évitée de justesse est que les programmes pour les ordinateurs à blockchain doivent être écrits avec un soin extrême, sans doute en utilisant les méthodes mises en œuvre dans l'industrie aéronautique et les systèmes embarqués ;

– la gouvernance d'un système tel qu'Ethereum est délicate. En théorie, il n'y en a pas besoin, et seules certaines évolutions majeures du système sont effectuées à la suite du vote des mineurs qui détiennent collectivement une forme de pouvoir « démocratique » sur le système. Cependant, en cas d'urgence, une réaction rapide est parfois indispensable. Une réflexion approfondie doit être menée pour résoudre ce dilemme entre automaticité du système, utile à la création de la confiance, et réactivité, essentielle dans certaines situations ;

– rien n'empêche une DAO d'avoir été conçue pour exploiter ses utilisateurs au bénéfice de son créateur. Il faut donc pouvoir exercer un certain contrôle sur les DAO créées. Comment l'organiser sans annuler les bénéfices des principes fondateurs des DAO ?

– dernier point : le statut légal et juridique des DAO est à concevoir et définir précisément. Cela ne sera pas simple.

Expérimentale aujourd'hui, cette nouvelle technologie des ordinateurs-mondes nous réserve toutes sortes de surprises ! ■

L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

Le projet Ethereum : https://www.ethereum.org https://www.ethereum-france.com

Understanding Ethereum, *CoinDesk*, 2016 : http://bit.ly/2cTEHMK.

J.-P. Delahaye, **Les blockchains, clefs d'un nouveau monde**, *Pour la Science*, n° 449, pp. 80-85, mars 2015 ; **Bitcoin, la cryptomonnaie**, *Pour la Science*, n° 434, pp. 80-85, décembre 2013.

A. Kosba *et al.*, **Hawk : The blockchain model of cryptography and privacy-preserving smart contracts**, 2015 (https:// eprint.iacr.org/2015/675.pdf).

Retrouvez la rubrique Logique & calcul sur www.pourlascience.fr

SCIENCE & FICTION

Interstellar : plongée dans le tesseract

Dans le film de Christopher Nolan, les tableaux noirs cachent plusieurs éléments de la physique théorique d'aujourd'hui. Décryptage.

Roland LEHOUCQ et Jean-Sébastien STEYER

En pleine catastrophe écologique majeure, la Terre se meurt. À court de ressources, l'humanité est à l'agonie. Un groupe de scientifiques reclus cherche une solution et propulse une petite équipe dans l'espace en quête d'une nouvelle Terre. Après un long voyage, le héros finit sa course dans un trou noir pour nous apprendre que, finalement, seul l'amour transcende l'espace et le temps.

L'accroche du film *Interstellar* (Christopher Nolan 2014), héritier revendiqué de *2001, l'Odyssée de l'espace*, est certes un peu faible. Mais cette œuvre n'en a pas moins un intérêt pédagogique, tant la science y est présente et tant la volonté du réalisateur de bien faire est incontestable. Christopher Nolan s'est d'ailleurs attaché les conseils du physicien américain Kip Thorne, spécialiste de la théorie de la relativité générale et qui a beaucoup travaillé sur le concept de trou de ver.

Dans le film, le professeur Brand tente de bâtir une théorie capable de rendre compte simultanément de toutes les interactions fondamentales – la gravitation et les interactions à l'échelle microscopique. Le professeur explique que la mise au point de cette « théorie du tout » pourrait sauver l'humanité. Outre la naïveté d'une telle prétention, il est intéressant de se demander si les équations fugitivement montrées sur les immenses tableaux noirs de son bureau ont la moindre signification pour un physicien.

Sur le premier tableau *(page ci-contre, à gauche)*, un dessin représente notre Univers comme une surface ou « brane » *(our brane 0)* prise en sandwich entre deux autres *(confining brane 1, confining brane 2)*, décalées par rapport à la nôtre dans une dimension perpendiculaire. Clairement, le professeur Brand construit sa théorie dans un superespace – le *bulk* – ayant plus de dimensions que nous n'en percevons.

Coll. Christophel © 2013 Warner Bros Entertainment Inc. / Paramount Pictures Corporation

LE FILM *INTERSTELLAR* entraîne le spectateur à travers des trous de ver et sur des exoplanètes tout en essayant de coller le plus possible à la rigueur scientifique.

En 1999, les physiciens américains Lisa Randall et Raman Sundrum proposèrent justement un modèle selon lequel notre univers n'est qu'un sous-ensemble d'une structure ayant davantage de dimensions. Ce *bulk* y est décrit par un espace à cinq dimensions qualifié d'anti de Sitter (noté AdS_5 sur le tableau). La motivation des deux physiciens était d'expliquer la faiblesse de la gravitation vis-à-vis des autres interactions à l'échelle microscopique : ainsi, l'attraction gravitationnelle entre le proton et l'électron d'un atome d'hydrogène est 10^{39} fois plus faible que la force électrique qui les lie.

Imaginons alors que notre univers tridimensionnel soit plongé dans un espace doté d'une dimension spatiale supplémentaire et que toutes les interactions restent confinées dans les trois dimensions usuelles, sauf la gravité. Comme elle peut s'étendre dans toutes les dimensions, la gravité semblerait alors subir des « fuites », qui se traduiraient par son apparente faiblesse dans notre espace tridimensionnel.

L'intimidante formule du second tableau confirme cette interprétation. Elle exprime l'« action effective » de la théorie du professeur