"Le bitcoin n'est pas fait pour le citoyen lambda"

Entretien réalisé par Ariane van Caloen

PROFESSEUR ÉMÉRITE UCL

Jean-Jacques Quisquater

Né en 1945, Jean-Jacques Quisquater fait partie des rares connaisseurs scientifiques en Belgique du bitcoin et des cryptomonnaies en général. Il porte aujourd'hui le titre de professeur ordinaire émérite UCLouvain (groupe UCL crypto) et chercheur associé au MIT. Après avoir fait des études d'ingénieur civil à Leuven, il a travaillé chez Philips, plus exactement dans leur laboratoire de recherche. *"Je m'occupais des puces, ce qui m'a amené sur la cryptographie. J'ai commencé en 1978, c'était le tout début"*, raconte-t-il. C'est ce que lui a permis d'être *"parmi les inventeurs des cartes à puces"*. Il a aussi vécu toute la difficile transition de Philips, qui n'a pas réussi à anticiper la fin du vinyle, un de ses coeurs de métiers et qui est devenue aujourd'hui une société spécialisée dans les objets de soins de beauté (sèche-cheveux, etc.) et l'électroménager. Une fois que le laboratoire de Philips a fermé, Jean-Jacques Quisquater s'est reconverti dans l'enseignement. Il a commencé comme professeur invité à l'UCL en 1991 avant d'être nommé en 1997 quand il avait 52 ans. Sa carrière académique a duré 15 ans durant lesquels il a beaucoup voyagé à travers le monde. Il a aussi accompagné une quarantaine d'étudiants doctorants. En parallèle, il a créé sa société de consultance Math Rizk, qui est toujours opérationnelle. *"C'est un jeu de mot. À l'époque Matrix faisait référence à Internet"*, précise-t-il. Tout au long de sa carrière, il a bénéficié de contrats de recherche pour 14 millions d'euros, que ce soit de l'UCL, de la Région wallonne ou de la Commission européenne.

12,5 bitcoins toutes les dix minutes

Une récompense Comment crée-t-on un bitcoin ? *"C'est une récompense attribuée à un certain nombre d'acteurs dans le système bitcoin qui ont fait une série de vérifications correctement. Aujourd'hui, il y a 12,5 bitcoins émis toutes les dix minutes. Et cela va être de moins en moins au fil du temps. On les appelle les mineurs, ce qui est un bon terme car cela fait allusion aux gens qui vont dans les mines d'or"*, explique Jean-Jacques Quisquater. *"Tout le monde fait un calcul et le premier qui trouve le bon résultat décroche le bitcoin. C'est du pur hasard, c'est un coup de chance"*, poursuit-il. L'inventeur du bitcoin a eu comme idée de donner une équation à tout le monde. Et le premier qui l'a résolue est comme le mineur qui trouvé de l'or. *"C'est la meilleure idée qu'il a eue. Mais ce qu'il n'avait pas imaginé c'est qu'il y aurait des fermes colossales d'ordinateurs qui tournent en même temps pour se donner plus de chance de trouver l'équation et consomment autant d'électricité qu'une grande ville."*

Comme à Las Vegas Pourrait-on faire une comparaison avec les machines à sous à Las Vegas quand par chance elles crachent des pièces de monnaies sous l'impulsion de gros bras qui actionnent la machine ? *"C'est une image qui me plaît."*

Comment expliquer la chute des cours des cryptomonnaies ? Assiste-t-on à l'éclatement d'une bulle ?

Je ne sais pas si c'est l'éclatement d'une bulle, c'est en tout cas un dégonflement. Les économistes diraient qu'on est dans une phase de consolidation. Le bitcoin n'existe que depuis dix ans. Durant les premières années, personne n'y croyait. Il a été créé en 2008 et était opérationnel en 2009 au moment où il y avait une crise financière très importante. Il a été conçu comme une possibilité d'échapper à cette bulle financière. Il a eu trop de succès à un moment donné. Les gens ont voulu acheter cet actif car il devenait rare. Rappelons que le nombre de bitcoins est limité. Les cours ont peut-être monté un peu trop vite. Ce n'est pas seulement vrai pour les bitcoins. Il y a à peu près 2 000 cryptomonnaies actuellement. Un quart d'entre elles sont mortes.

Pourquoi sont-elles mortes ?

Elles sont descendues au-dessous d'un cours raisonnable. Car bien souvent il n'y avait rien derrière. Beaucoup de cryptomonnaies aujourd'hui sont adossées à un bien, qui est vendu ou acheté. On pourrait imaginer des panneaux solaires vendus entre voisins par le biais d'une cryptomonnaie. Cette cryptomonnaie ne mourra pas tant que les panneaux existeront.

Certaines cryptomonnaies reposent sur des mécanismes où les fluctuations de cours n'existent pas. D'autres sont indexées sur le dollar. Celles-là sont beaucoup plus stables. En revanche, certaines cryptomonnaies lancées il y a moins d'un an fluctuent dans une fourchette de 1 à 100. Cela n'inspire pas confiance et jette le discrédit sur les cryptomonnaies. Tous les mécanismes boursiers bien connus se retrouvent sur le marché des cryptomonnaies.

Le bitcoin a-t-il quelque chose en plus que les autres cryptomonnaies ?

Le bitcoin a été un modèle relativement bien pensé. Il y a des défauts, mais qui ne sont pas directement visibles. Il ne faut pas dire que le bitcoin, c'est fini. Cela représente une masse d'argent colossale qui a atteint un ordre de grandeur équivalent à la dette belge. Aujourd'hui, c'est presque 10 fois de moins. Qui est perdant ? Les pertes encaissées par les investisseurs

sont certainement moins élevées que les pertes de la valeur du bitcoin. Ce qui veut dire qu'on a créé de l'argent. D'une certaine façon, le bitcoin, c'est aussi une planche à billets. Des bitcoins ont été créés mais contre un service, mais un service qui ne sert à rien.

Qu'est-ce qui vous permet de dire que ce n'est pas fini pour le bitcoin ?

Il y a trop d'acteurs, trop de personnes qui ont investi là-dedans. C'est pour cela que je dis qu'on est dans une phase de consolidation, qui sera peut-être aussi une phase de plus grande sagesse. Il est vraisemblablement trop tard pour miser sur le bitcoin. La sagesse va être de l'utiliser comme monnaie d'échange.

Le problème du bitcoin, c'est que son nombre est limité. Ce qui, comme l'avait imaginé son inventeur, doit normalement augmenter sa valeur. D'où la notion de dixième de bitcoin, qui s'appelle le satochi. Ce mécanisme n'est actuellement pas en marche.

N'est-ce pas dû à la concurrence apportée par la création d'autres cryptomonnaies ?

En effet. Le programme pour créer du bitcoin était public, c'était de l'*open source*. Dès le moment où le modèle était divulgué, c'était facile de le copier.

En quoi les cryptomonnaies et le bitcoin en particulier ont quelque chose de génial ?

C'est quand même assez extraordinaire qu'on ait pu aussi facilement et aussi vite créer des cryptomonnaies qui font concurrence à des monnaies d'État. Il y a un an et demi, la directrice du FMI, Christine Lagarde, a prédit un bel avenir pour le bitcoin. Elle a aussi estimé que les banques allaient disparaître. Cela a joué dans le succès des cryptomonnaies. Elle a fait ces déclarations quand les cours du bitcoin s'emballaient. C'est peut-être dû à un effet de mode mais il fallait quand même oser le dire.

En permettant l'anonymat, le bitcoin n'est-il pas un canal très utilisé pour le blanchiment ?

Oui et non. Vraisemblablement que les grandes entités d'espionnage, qu'elles soient russe, chinoise, américaine, française, anglaise, peuvent savoir qui est derrière les numéros et donc briser cet anonymat.

Pensez-vous que cet argument de blanchiment justifierait l'interdiction du bitcoin ?

Je reste dubitatif sur cet argument de blanchiment. Comment recycler si ce n'est en achetant d'autres cryptomonnaies ? Si les blanchisseurs veulent convertir des cryptomonnaies dans le circuit habituel, ils devront se soumettre aux règles de ce circuit et donc justifier d'où vient cet argent. Il y a bien sûr du blanchiment, mais est-ce très différent d'aller d'un paradis fiscal vers un autre paradis fiscal ? Je ne vois pas en quoi c'est pire qu'avant ? Vous savez, il n'y a rien de nouveau. Après la guerre 40-45, il y a eu la loi Gutt qui supprimait la valeur légale de tous les billets de 100 francs et plus. Les Belges qui avaient amassé de l'argent noir ont acheté des timbres. Et je vous assure que certains en ont acheté pour le restant de leur vie !

Que conseillerez-vous à ceux qui veulent investir dans le bitcoin ?

Je dirais que ce n'est pas à mettre dans les mains d'un citoyen lambda. C'est trop compliqué, trop fluctuant. Ce n'est pas pour le commun des mortels.

"Il ne faut pas utiliser la blockchain n'importe où ou n'importe comment"

La blockchain, la technologie derrière le bitcoin, est-elle révolutionnaire ?

Au début, beaucoup de monde s'est intéressé au bitcoin sans mettre en avant la blockchain. Une couverture de l'hebdomadaire *The Economist* a servi de déclic pour l'engouement actuel. Car la blockchain est une vieille technologie qui remonte à la fin des années 1980. Des brevets le prouvent. Mais elle n'avait pas trouvé son succès. Le principe de la blockchain est très simple et n'est pas fondamentalement génial. C'est un système de registre sous forme numérique, consultable et immuable. Il reprend toutes les opérations du passé. Y ajouter un acte authentifié devant témoin comme devant le notaire, cela équivaut à la création d'une opération de bitcoin.

La technologie n'est donc pas révolutionnaire...

Les Américains qui avaient fait breveter la technologie ont créé une société, Surety qui existe toujours, pour faire de la 'notarisation'. Ils n'appelaient pas cela blockchain. Je n'ai toujours pas trouvé qui est la personne qui a utilisé ce mot pour la première fois.

Quel est l'avantage que toutes les transactions soient consultables ?

Cela permet d'éviter la double dépense. La blockchain permet de tracer chaque

bitcoin et donc de détecter si vous en êtes encore le détenteur ou pas. On peut créer des faux bitcoins mais on ne peut pas utiliser deux fois un bitcoin.

La blockchain est aussi à la mode dans le monde de l'entreprise ?

Oui. Il existe une société qui s'appelle Gartner. C'est une société de consultance très écoutée y compris par les banques. Tous les ans, ils publient une liste des dix mots qui font faire le buzz. Il y a blockchain, intelligence artificielle, etc. Je soupçonne beaucoup de patrons d'avoir un copion pour sortir ça au bon moment.

Croyez-vous à des applications élargies de la blockchain ?

Oui. Mais, il ne faut pas l'utiliser n'importe où ou n'importe comment. Bien souvent, il y a une solution sans blockchain qui est sans doute aussi bonne si pas meilleure.

Un exemple ?

Toutes les bases de données peuvent être remplacées par une blockchain. Si vous utilisez la blockchain de façon systématique, vous ne savez pratiquement plus faire de mise à jour, vous ne savez plus faire des modifications. Dans le cas des bitcoins, c'est naturel d'employer la blockchain. Ce qu'on veut mémoriser, c'est le fait qu'un bitcoin a déjà été utilisé par une personne à tel moment. Si vous n'avez pas besoin de cet ordre, il y a d'autres outils, qui s'appellent des bases de données.

Dans quelle mesure la blockchain peut s'accommoder de la directive européenne RGPD sur la protection des données ?

Effectivement, il y a une contradiction entre la blockchain et le RGPD. Un, parce qu'il y a le droit à l'oubli qui n'existe pas avec la blockchain. Deux, les modifications sont très difficiles ou impossibles à faire selon le contexte. Trois : il n'y a pas de responsable. S'il y a une réclamation, à qui s'adresser ?

Est-ce un problème ?

Oui, mais cela ne veut pas dire qu'il n'y a pas de solution. Il faut aussi rappeler que le RGPD porte sur les données personnelles. Pensez aux données médicales. En cas d'urgence, on doit pouvoir les ouvrir. Ce qui veut dire que dans le contexte actuel, on ne pourrait pas utiliser la blockchain.

"La blockchain permet de tracer chaque bitcoin et donc de détecter si vous en êtes encore le détenteur ou pas. On peut créer des faux bitcoins mais on ne peut pas utiliser deux fois un bitcoin."