Jéco 2018 Palais de la Mutualité, Lyon. Mardi 6 Novembre 2018, 17h-18h30

**Conférence : La révolution blockchain[[1]](#footnote-1)**

**Intervenants :**

* [Nicolas Barbaroux](http://www.journeeseconomie.org/index.php?arc=p4&num=1667): Maître de conférences en Économie, Université Jean Monnet & GATE Lyon Saint-Etienne
* [Richard Baron](http://www.journeeseconomie.org/index.php?arc=p4&num=1668): Maître de conférences en Informatique, Université Jean Monnet & GATE Lyon Saint-Etienne
* [Vincent Bignon](http://www.journeeseconomie.org/index.php?arc=p4&num=1669): Conseiller du directeur général des études et des relations internationales de la Banque de France[[2]](#footnote-2)
* [Sam Guilaume](http://www.journeeseconomie.org/index.php?arc=p4&num=1771) : Co-fondeur de Twin Peek, start-up incubée au B612

**Modérateur** : [Stéphane Marchand](http://www.journeeseconomie.org/index.php?arc=p4&num=1766), *Pour l'éco[[3]](#footnote-3)*

**Présentation du thème dans le programme des Jéco**

Les « monnaies virtuelles », définies par la Banque de France comme des « unités de compte virtuelles stockées sur un support électronique permettant à une communauté d’utilisateurs d’échanger entre eux des biens et des services sans avoir à recourir à la monnaie légale » ont suscité récemment autant d'enthousiasme que de craintes. Les monnaies virtuelles participent à l'émergence d'une nouvelle économie digitale où l'ensemble des transactions marchandes pourra se réaliser sans intervention des banques ou de n'importe quel autre tiers de confiance. Cependant, force est de reconnaître que la technologie blockchain sous-jacente à l'émission de ces nouvelles formes de monnaies demeure encore aujourd'hui opaque pour le grand public.

Pour y voir plus clair, les regards croisés des juristes, informaticiens et économistes seront utiles afin d'appréhender au mieux les changements structurels apportés par cette technologie. Les intervenants de cette session auront ainsi à cœur d'expliquer tout à la fois les mécanismes ainsi que les challenges que les monnaies virtuelles adressent pour la stabilité du système monétaire et financier.

Vidéo de la conférence : <http://www.touteconomie.org/index.php?arc=dc033d>

**Compte-rendu :**

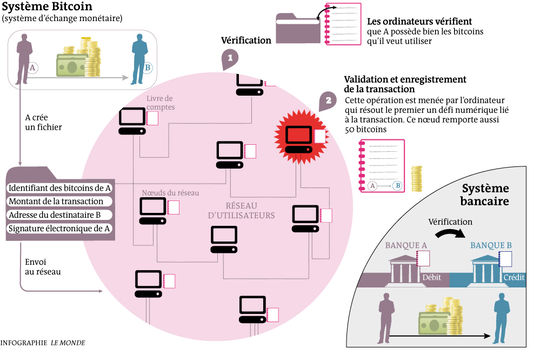
La conférence a été décomposée en deux temps : une présentation du thème par chaque intervenant, puis des réponses aux questions de l’auditoire.

**Nicolas Barbaroux** : Il s’agit d’une révolution du système de paiements et d’échanges. Quelle est la réalité de ces échanges ? La blockchain n’en concerne qu’une très faible partie (0,5 %).

Comment définir la blockchain ?

Il s’agit d’un registre distribué chargé d’enregistrer l’ensemble des opérations d’émission et de transfert de ces crypto-actifs entre les utilisateurs. Les transactions sont assemblées en bloc, puis ajoutées à une chaîne, ce qui donne au registre le nom de « chaîne de bloc » (ou blockchain). Les utilisateurs sont tous volontaires, l’État n’exerce pas de contrôle.

Schéma synthétique du fonctionnement de la blockchain : projection d’une diapo avec une infographie parue dans *Le Monde* : « paiement en monnaie virtuelle ».



Source : <https://www.lemonde.fr/sciences/article/2012/11/29/payer-et-vendre-sans-les-banques_1798066_1650684.html>

Avec un paiement en carte bleue, le back office a lieu en arrière plan. Avec la blockchain, on peut faire la même chose mais sans avoir besoin des banques, puisque les transactions passent par un réseau d’ordinateurs indépendamment de tout réseau bancaire.

Avec la blockchain, une relation entre la créance et la dette est effectuée. Des codes sont créés pour chaque transaction. Un code est associé à celui qui veut effectuer un achat : il devient anonyme, son identité est un numéro. Un autre code est créé pour le paiement et est envoyé dans un réseau partagé. Une vérification d’un ensemble de transactions est ensuite effectuée par un réseau d’ordinateurs. Les ordinateurs sont rémunérés dans la monnaie virtuelle de facture (ex : le bitcoin).

La vraie révolution réside dans un nouveau moyen de conclure des transactions par des algorithmes (pas besoin de banque).

**Richard Baron :**

La blockchain est une base de données enregistrées de manière sûre et définitive. Cette base est :

* distribuée (pas de manière uniforme mais à l’échelle mondiale tout de même)
* transparente : tout le monde peut accéder au contenu des blocs (pas à l’identité des utilisateurs mais à leur identifiant)
* sans organe central de contrôle : ces systèmes n’ont pas de nœud donnant l’ordre de tout contrôler.

Deux notions sont essentielles pour comprendre le fonctionnement de la blockchain :

* La fonction de hachage : elle calcule une empreinte (hash en anglais) caractéristique d’un ensemble de données. Connaissant cette empreinte, il est impossible de connaître la donnée initiale. C’est une fonction difficilement inversible.
* La cryptographie asymétrique : l’envoi d’un contenu codé par une clé.

Le chaînage des blocs

temps

En-tête bloc n – 1

-empreinte du bloc précédent

-nonce

-empreinte de la transaction

Contenu :

-transaction 1

-transaction 2

-transaction….

hachage

En-tête bloc n

-empreinte du bloc précédent

-nonce

-empreinte de la transaction

Contenu :

-transaction 1

-transaction 2

-transaction….

Dans l’en-tête, l’ensemble des informations n’est pas modifiable. Les mineurs interviennent au niveau du nonce. Le minage consiste à satisfaire des conditions. Dans l’exemple projeté la chaîne de caractères devait commencer par treize zéros. Les mineurs tirent des nonces (ici des nombres) au hasard pour que l’empreinte satisfasse la condition. Cette empreinte se fait sur des circuits spécialisés très chers à l’achat, coûteux en nombre et en énergie. Les puits de mineurs sont installés dans des pays où l’énergie coûte moins cher (par exemple la Chine, le Canada).

**Vincent Bignon**

Nos sociétés sont fondées sur des institutions vérifiant les informations et évitant la fraude. Les coûts de gestion correspondent à la vérification centralisée. Existe-t-il un équivalent qui ne serait pas lié à la technologie ? Oui : la communauté villageoise où l’information est distribuée, décentralisée et où on lutte contre les fausses rumeurs. Le développement économique consiste à construire des institutions pour ne pas avoir besoin de tous se connaître. Le coût de la vérification des informations est inférieur aux frais de gestion et de distribution de l’information par la blockchain (mineurs, électricité). Les questions qui se posent sont peut-on utiliser la blockchain pour les titres de propriété (fin des cadastres), pour remplacer les paiements en euros au quotidien ?

**Sam Guilaume**

L’entreprise Twin Peek a pour but de protéger les data individuelles qui constituent un patrimoine informationnel. Ce patrimoine est constitué de données que nous créons consciemment ou inconsciemment à travers notre vie numérique. Ce patrimoine a beaucoup de valeur.

L’utilisateur peut choisir une option entre la « confidentialité ultime » et « le revenu de mon patrimoine informationnel ». Il doit être possible et acceptable que l’utilisateur ne veuille rien partager. Le partage de données anonymisées sur la base de choix d’intention de projet de vie afin que la publicité soit adaptée aux projets en cours. Un individu existe de manière anonyme sous plusieurs entités (ex : avatar 25, avatar 26) pour ne pas que les GAFA puissent les assembler. Les moyens de paiement ne sont pas accordés à une identité virtuelle par les banques. La blockchain, par contre, permet de résoudre une impasse technologique : garantir l’anonymat et le KYC (« *know your customer* » ensemble d’informations recueillies sur les clients par les banques[[4]](#footnote-4)).

Quels sont les bénéfices inhérents à la technologie blockchain ?

* Certification de la preuve électroniquement
* Confidentialité : la blockchain n’est plus qu’un média d’échanges sécurisés de pair à pair
* Audiabilité : les consentements sont consignés et auditables
* Sécurité : la révocation de la certification est la protection d’urgence en cas de brèche.

**\*\*\*\*\***

**Réponses aux questions de l’auditoire**

1. Que penser de la citation de Nouriel Roubini disant que la blockchain est une vaste escroquerie[[5]](#footnote-5) ?

**Vincent Bignon**

La Banque de France décourage l’utilisation des blockchains pour les monnaies de type bitcoin car ces monnaies sont trop fluctuantes. Seules des monnaies connaissant une forte dépréciation (ex de la forte inflation au Venezuela, en Argentine) pourraient être concurrencées par les monnaies virtuelles. La décentralisation n’est pas une révolution en soi. Le commerçant n’a pas besoin de connaître mon identité pour accepter mon billet de banque. La révolution c’est qu’on a dans les échanges un intermédiaire qui n’est pas une banque.

**Sam Guilaume**

Les bitcoins sont un exemple de blockchain, il en existe d’autres. D’autres blockchains ne sont pas autant énergivores que le bitcoin.

**Richard Baron**

Nous disposons de peu d’informations sur les utilisateurs de la blockchain. Cela peut concerner un grand nombre de projets : santé, propriété intellectuelle (enregistrement de photographies par ex), *smart contrat, sublain chain* (chaîne d’approvisionnement).

1. La blockchain sert-elle à blanchir de l’argent ?

**Nicolas Barbaroux**

La Banque de Suède propose contre le blanchiment d’argent de ne plus utiliser de cash et de n’utiliser que des transactions numériques d’ici 2023. Le risque de blanchiment s’accroît avec les monnaies virtuelles décentralisées, néanmoins les nouvelles technologies peuvent aussi être utilisées dans la lutte contre le blanchiment.

**Vincent Bignon**

La lutte contre le blanchiment est un objectif justifiant que les sommes en espèces sont limitées à 1500 euros. Néanmoins quelle que soit la forme de la monnaie, la lutte contre l’argent immoralement et/ou illégalement acquis peut sembler paradoxale puisqu’un des avantages de la monnaie c’est d’être acceptée par tout le monde. Les banques centrales peuvent réglementer les monnaies virtuelles de la même manière qu’elles réglementent les autres monnaies. Les pièces ont remplacé les tablettes d’argile afin de mieux lever l’impôt, les billets pour lutter contre les crises financières. Peut-on lutter contre les crises du crédit ? C’est difficile, on peut accroître la confiance dans la monnaie pour faire diminuer ce risque.

**Richard Baron**

Un rapport d’Europol estime que la part des transactions illégales est comprise entre 3 et 6 %. Les transactions électroniques sont très faciles à surveiller (cf. NSA) puisque les enregistrements sont immuables, définitifs.

**Sam Guilaume**

La problématique repose sur le fait de ne pas révéler l’identité de celui qui paie.

1. Les banques vont-elles disparaître ?

**Nicolas Barbaroux**

La blockchain effectue le même travail qu’une banque mais pour une monnaie qui n’est pas officielle. Les commerçants sont libres d’accepter ou de refuser les monnaies virtuelles émises par des agents non bancaires. Pour Hayek ce sont les banques et non plus les États qui frapperaient la monnaie.

**Sam Guilaume**

On pourrait souhaiter la disparition des banques car elles ont un coût pour les contribuables et pour les consommateurs. La monnaie est un bien commun qui pourrait être géré par nous sans coût.

**Vincent Bignon**

Les banques permettent certes d’émettre des moyens de paiement qui ont déjà beaucoup changé, mais elle distribue aussi le crédit et les banques centrales évitent les crises de liquidité.

**Sam Guilaume**

Des algorithmes pourraient réaliser les intermédiations entre agents à besoin et à capacité de financement.

1. Pour les mineurs, la quantité limitée de bitcoins signifie-t-elle la fin du minage ?

**Richard Baron**

Les cryptomonnaies sont pour la plupart en quantité limitée. La vitesse d’émission est régulée. Le dernier bitcoin devrait être émis en 2140.

1. Pourrait-on lever l’anonymat dans certains cas ?

**Nicolas Barbaroux**

Aujourd’hui nous en sommes aux balbutiements dans la réglementation, la technologie va plus vite que la réglementation. Il s’agit d’un défi juridique et technique.

**Sam Guilaume**

Il faut se réjouir d’avoir une technologie inviolable. Le bitcoin n’est qu’une utilisation. Pour l’introduction en Bourse d’une monnaie virtuelle il est nécessaire d’être identifié.

**Richard Baron**

L’anonymat n’est pas total puisqu’il existe déjà des techniques d’enquête pour collecter des traces numériques.

1. *Ajout du webmestre. « Blockchain et cryptomonnaies », Primavera De Filippi, Coll. Que Sais-je ? 2018, 126 p., 9€.* [↑](#footnote-ref-1)
2. Parmi les publications de la Banque de France, ABC l’éco en bref « le bitcoin » paru en juillet 2018, téléchargeable : <https://abc-economie.banque-france.fr/leco-en-bref/le-bitcoin> [↑](#footnote-ref-2)
3. Le numéro 3 (novembre 2018) de ce magazine comporte un dossier intitulé « Monnaie contre cryptomonnaie qui va gagner ? » [↑](#footnote-ref-3)
4. Pour en savoir plus sur le KYC dans le secteur bancaire: <https://acpr.banque-france.fr/autoriser/fintech-et-innovation/nos-dossiers-thematiques/identification-et-connaissance-de-la-clientele-kyc> [↑](#footnote-ref-4)
5. Pour en savoir plus : <https://www.project-syndicate.org/commentary/blockchain-big-lie-by-nouriel-roubini-2018-10/french> [↑](#footnote-ref-5)