Jean-Paul Delahaye Laboratoire d'Informatique Fondamentale de Lille (UMR **CNRS** 8022)

La cryptographie réinvente la monnaie : le *Bitcoin*.

Jean-Paul Delahaye,
Laboratoire d'Informatique Fondamentale de Lille, UMR 8022 CNRS,
Bât M3-ext 59655 Villeneuve d'Ascq Cedex
email : delahaye@lifl.fr

6 février 2014

En 2008, un évènement important s'est produit qui sera un jour inscrit dans les livres d'histoire :

une nouvelle façon de concevoir la monnaie a été proposée qui remet en cause les anciennes idées sur cette institution.

• En octobre 2008, Satoshi Nakamoto publie sur internet un texte décrivant comment il est possible grâce aux réseaux et à la cryptographie mathématique moderne de mettre en place une monnaie qui n'a besoin d'aucun contrôle centralisé pour fonctionner.

• Le 3 janvier 2009 : les programmes nécessaires au lancement de cette *crypto-monnaie* sont prêts.

• Le ***Bitcoin*** est créé.

- Débuts confidentiels : seuls quelques cryptologues s'y intéressent.
- Cours dérisoire en 2009 et 2010. Ensuite, elle prend son envol.
- Début 2013, un *Bitcoin* vaut **une dizaine d'euros**.
- 2013 : décollage du *Bitcoin* qui acquiert une ***notoriété mondiale***.
- Cours multiplié par 50 en un an : **580 euros, le 1 janvier 2014.**
- La capitalisation totale des *Bitcoins* atteint alors plus de **6 milliards d'euros.**


Bitcoin
From Jan 1, 2013 To Feb 1, 2014
Wednesday, Dec 4, 2013
BPI (USD): 1,147.25
$1000
$750
$500
$250
$0
Jan '13
May '13
Sep '13
Jan '14
2011
2012
2013
2014

=

• À partir de rien, la cryptologie mathématique vient de créer des devises numériques qui s'échangent contre de l'argent sonnant et trébuchant.

• Un étudiant Norvégien —Christoffer Kock— qui avait acquis 25 euros de *Bitcoins* en 2009, les a revendu en 2013 et s'est acheté un appartement à Oslo. (27 $ -> un million de $ environ)

Quelle est l'idée de cette monnaie ?
En quoi est-elle une révolution ?
Doit-on la craindre ou se réjouir de sa création ?

Miraculeuses mathématiques

• L'idée de cette monnaie est que, grâce à un ***subtil agencement*** de protocoles cryptographiques :

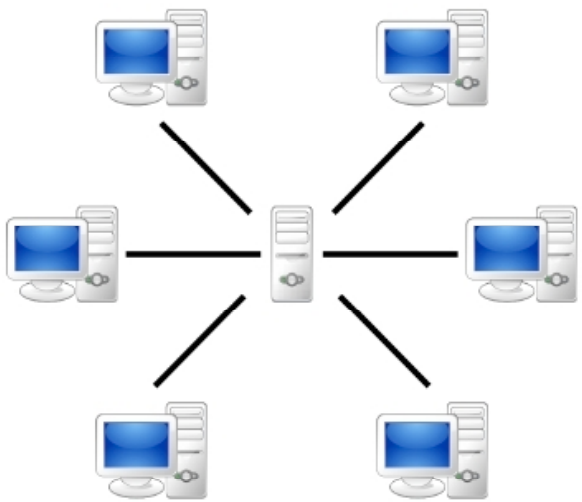
on peut émettre une monnaie dont le contrôle se fera collectivement sur un réseau P2P (sans autorité centrale)

• Le protocole de Nakamoto a été rendu possible grâce aux progrès de la **cryptographie**.

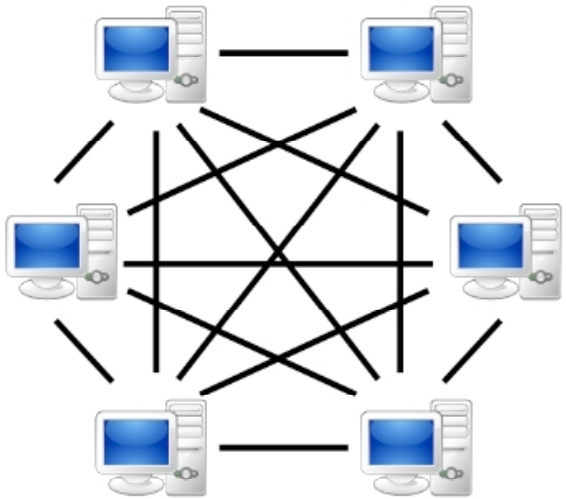
• Elle a inventé des primitives de chiffrage, de signatures, de «preuve de travail» etc.

• Elles autorisent la réalisation de dispositifs numériques qu'on pensait impossibles.

• Le protocole *Bitcoin* doit aussi son existence à la puissance informatique dont chacun dispose et qui fait, qu'avec son ordinateur personnel, il peut participer au contrôle de la monnaie *Bitcoin* au sein d'un **réseau décentralisé P2P (la blockchain pèse environ 13 giga-octets)**



Centralisé



P2P

• Ceux qui le souhaitent peuvent :

- **télécharger** des logiciels libres et ouverts (dont le code est accessible à tous) et

- **participer** à la surveillance de la monnaie *Bitcoin*,

- c'est-à-dire **vérifier** que personne ne crée de *Bitcoins* non prévus par le protocole, et que toutes les transactions se déroulent conformément aux règles définies.

Comment avoir des *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 :

l'anonymat des détenteurs de *Bitcoins* est une caractéristique de cette monnaie.

• Chaque compte possède **deux numéros**. (cryptographie à double clef)

- Le ***numéro secret*** (qu'il faut absolument garder pour soi, car quiconque en dispose peut dépenser le contenu du compte),

`E9 87 3D 79 C6 D8 7D C0 FB 6A 57 78 63 33 89 F4 45 32 13 30 3D A6 1F 20 BD 67 FC 23 3A A3 32 62`

- Le ***numéro public*** que vous communiquerez. C'est une adresse qui permet de recevoir des *Bitcoins*. 1CC3X2gu58d6wXUWMffpuzN9JAfTUWu4Kj

A

On obtient des *Bitcoins*, soit en en achetant contre de l'argent usuel sur les plateformes d'échange : elles prennent vos euros et vous envoient en retour des *Bitcoins* qui s'inscrivent sur votre compte.

B

On peut aussi en acquérir en faisant du commerce :

vous vendez un livre à quelqu'un qui vous paie en versant des *Bitcoins* sur votre compte.

C

Une troisième façon d'obtenir des *Bitcoins* est de **participer à la surveillance de la monnaie**.

- Ceux qui acceptent de mener la surveillance sont ***les mineurs de Bitcoins***.
- Le travail fourni reçoit une récompense comme des mineurs dans une mine de métal précieux.
- Cette récompense est de 25 *Bitcoins* toutes les 10 minutes.
- Elle est attribuée à un seul mineur tiré au sort.

Cela rend la monnaie plus solide.

La probabilité que votre machine soit choisie pour recevoir les 25 *Bitcoins* distribués est faible.

La probabilité de gagner est proportionnelle votre puissance.

Dureté et persistance des *Bitcoins*

• Les *Bitcoins* n'existent pas matériellement.

• Ils n'existent que sur le réseau.

• Ils sont le résultat d'un consensus entre utilisateurs.

• Grâce aux informations présentes sur le réseau et que chacun peut consulter et contrôler, on sait quelles sommes d'argent se trouvent sur les comptes.

• L'ensemble des comptes est stocké dans un fichier du réseau P2P la *blockchain*.

Le protocole cryptographique de la monnaie assure que :

- **personne ne peut manipuler les comptes,**
- **fausser les transactions,**
- **ou émettre d'autres *Bitcoins* que ceux qui sont prévus.**

Il y en a 12 millions de bitcoins aujourd'hui.

Leur nombre ne dépassera jamais 21 millions
(ce maximum est inscrit dans le protocole).

La robustesse du protocole —confirmée par 5 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.

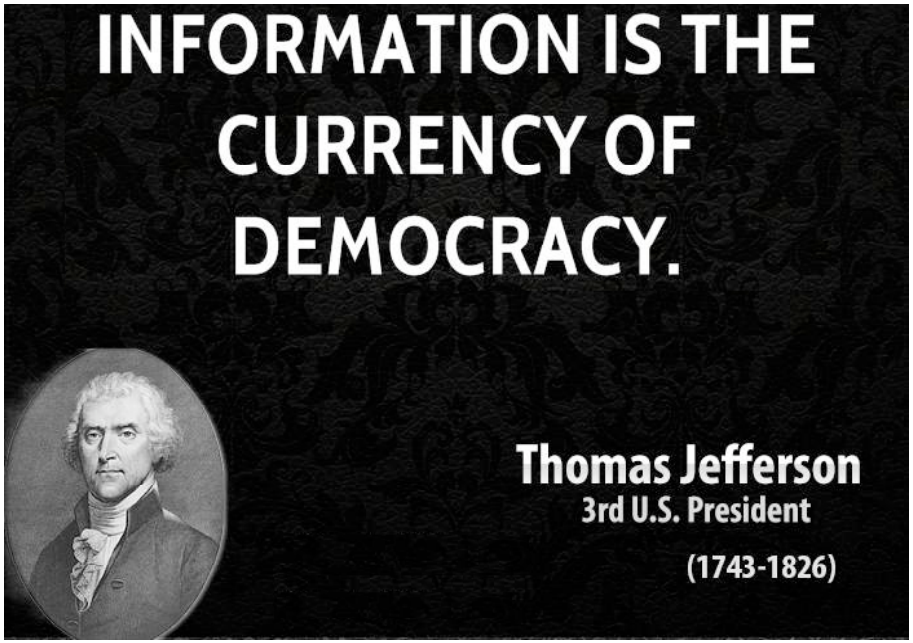
La cryptographie a réussi à créer des objets virtuels infalsifiables, aussi résistants et persistants que s'ils étaient faits de métal.

On peut les faire circuler à la vitesse de la lumière (c'est un des avantages des *Bitcoins* sur toutes les autres monnaies) sans coût, d'un endroit à l'autre du monde.

Comme toute monnaie, le *Bitcoin* ne tient que par *la confiance* de ses utilisateurs.

Celle-ci s'établit non pas parce qu'une banque centrale émettrice prétend se porter garant des devises qu'elle émet,
mais parce que le protocole cryptographique empêche quiconque de truquer les comptes.

La nouveauté principale de cette crypto-monnaie est que cet argent numérique n'est contrôlé par aucune banque centrale et qu'elle est gérée collectivement —***démocratiquement*** disent certains— par tous ceux qui le souhaitent et qui se surveillent mutuellement.



• Les caractéristiques des *Bitcoins* ont des conséquences positives dont (a priori) une protection des détenteurs de *Bitcoins* contre **l'inflation**.

• Celle-ci provient habituellement de l'émission 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 (et qui est de plus en plus faible, au cours du temps) n'est possible.
• A priori, il ne peut donc pas y avoir dévaluation de la monnaie.
• Certains prétendent que, le *Bitcoin* est déflationniste : il ne pourrait que **prendre de la valeur** !

Incertitudes et risques

Malheureusement les propriétés de la monnaie *Bitcoin* ont aussi des **conséquences négatives.**

• Il faut être très attentif lors de la manipulation de son compte. Si un pirate réussit à trouver votre numéro secret en s'introduisant sur votre ordinateur, il pourra en dépenser entièrement le contenu.
C'est déjà arrivé.

• N'effacez pas votre porte-monnaie numérique par erreur, il serait définitivement perdu.
C'est déjà arrivé.

• L'anonymat (partiel) des comptes intéresse toutes sortes de gens peu recommandables qui utilisent le ***Bitcoin*** pour échapper au fisc ou mener des trafics en tout genre.

• Le fait qu'aucun contrôle centralisé ne soit opéré par une autorité centrale a pour conséquence que le cours des ***Bitcoins*** est soumis à de fortes variations spéculatives.

• Il a été affirmé que le cours du ***Bitcoin*** est manipulé par ceux qui en détiennent beaucoup.

• La valeur du ***Bitcoin*** varie de plusieurs pourcents par jour, et il est arrivé qu'elle varie de plus de 40% dans une même journée. Cela rend difficile son usage pour le commerce !

• Le fait qu'elle soit concurrente des monnaies des banques centrales a pour conséquence que les États lui sont souvent hostiles, et que des réglementations existent limitant son usage, ou même l'interdisant. L'évolution de ces réglementations sera essentielle pour l'avenir du *Bitcoin*.

• Tous les programmes contribuant au fonctionnement de la monnaie *Bitcoin* sont libres et publics, donc il est facile de concevoir et de faire fonctionner d'autres monnaies du même type.

il existe aujourd'hui plus de 80 monnaies cryptographiques basées sur les mêmes principes que le *Bitcoin* et lui faisant concurrence.

Quel avenir ?

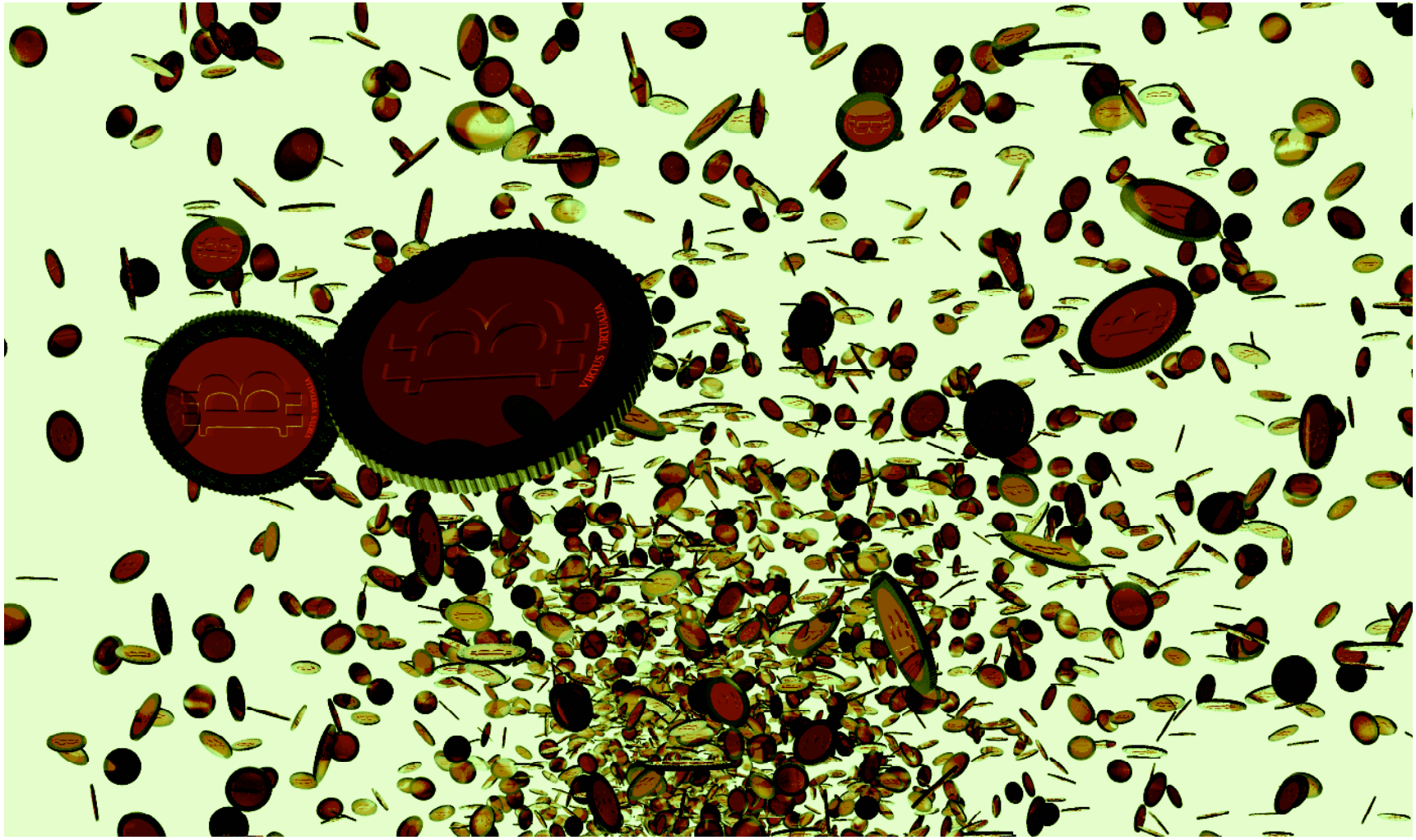
Que va devenir cette monnaie née des mathématiques ?
Aucune monnaie de ce type n'a jamais existé.

«Son cours élevé aujourd'hui est une **bulle** qui éclatera :
ceux qui en achètent finiront par tout perdre.»

«Le ***Bitcoin*** possède des propriétés telles qu'il est utile pour mener des transactions rapides, sans coût et anonymes.»

«Il permet de conserver de l'argent à l'abri de l'inflation, sous une forme discrète»

«Son cours va monter quand les utilisateurs seront plus nombreux.



Bibliographie

• Banque de France, *Dangers liés au développement des monnaies virtuelles, l'exemple du Bitcoin*, 2013 :
http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf

• Blockchain, *Information et statistiques sur le cahier des comptes Bitcoin* :
https://blockchain.info/fr

• Jean-Paul Delahaye, *Bitcoin, la crypto-monnaie*, Pour la science, pages 76-81, déc 2013 :
http://www.lifl.fr/~delahaye/pls/2013/241.pdf

• Jean-Paul Delahaye, *Blog SciLog*, décembre 2013 :
http://www.scilogs.fr/complexites/plaidoyer-pour-le-bitcoin/

• Jean-Paul Delahaye, *Le Bitcoin, une monnaie révolutionnaire*, janvier 2014 :
http://www.lifl.fr/~delahaye/Bitcoin/Bitcoin.pdf

- Michael Nilsen, *How the Bitcoin protocole actually works*, 2013 : http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

- Pierre Noizat, *Bitcoin Book*, 2012 : ISBN-10: 2954310103

- Wikipedia, *Bitcoin* : http://fr.wikipedia.org/wiki/Bitcoin