



'Bitcoin', 'blockchain', c'est quoi ?

ou

Monnaies cryptographiques & blockchains

INRIA Saclay, 23 juin 2016

Jean-Paul Delahaye

Université de Lille 1

CRISTAL : Centre de recherche en informatique, signal et automatique de Lille,

UMR 9189 CNRS, Bât M3-ext 59655 Villeneuve d'Ascq Cedex

Email : delahaye@lifl.fr <http://www.lifl.fr/~delahaye/>



Promouvoir les crypto-monnaies et les blockchains ?

Pour les questions :

Est-ce que le *bitcoin* et les blockchain favorisent la fraude, le blanchiment, les trafics, les terroristes ?

Pyramide de Ponzi ?

Faut-il y placer son argent

Est-ce tout va échouer (comme "The DAO" récemment) ?

Est-ce une bonne chose pour l'économie, le citoyen, l'Etat ?



- Une étonnante monnaie a été créée en 2009 par **Satoshi Nakamoto** : le *bitcoin*
- Elle s'appuie sur une *blockchain* qui se révèle une idée aux applications potentielles plus larges que la création de monnaies décentralisées.

- Le *bitcoin* n'est pas "*virtuel*" :

Le 21 juin 2016 : 1 *bitcoin* = 590 euros = 676 dollars

15 590 000 *bitcoins* en circulation

= 9,2 milliards d'euros = 10,6 milliards de dollars

1 *bitcoin* = 13 dollars le 1 janvier 2013

1 *bitcoin* = 763 dollars le 1 janvier 2014

1 *bitcoin* = 297 dollars le 1 janvier 2015

1 *bitcoin* = 435 dollars le 1 janvier 2016

Plus de 500 millions de \$ investis dans des sociétés liées au *bitcoin* depuis trois ans

5600 nœuds (full node) 100 000 mineurs taille blockchain : 72 giga-octets

Nombre total d'euros en circulation sous la forme de pièces et billets :
pour une valeur de **1035 milliards de dollars** en 2009

Nombre total de dollars en circulation sous la forme de pièces et billets :
pour une valeur de **850 milliards de dollars** en 2009

Nombre total de devises dans le monde en circulation sous la forme de pièces et billets :
pour une valeur de plus de **4000 milliards de dollars** en 2009

source : <http://www.24hgold.com/francais/contributor.aspx?article=2150340402G10020&contributor=Mike+Hewitt>.

Patrimoine total des Français (principalement de l'immobilier) :
10 544 milliards d'euros en 2012

source INSEE

Accord de Bretton-Woods 1946-1971 : **35 dollars = 1 once d'or**

Fin de la convertibilité du dollar en or : **15 août 1971** (Nixon)

Plus aucune monnaie ne repose sur l'or, mais sur la "confiance".
On parle de **monnaies fiduciaires** (fiducia = confiance en latin)

En 2016 une once d'or = 1200 dollars

Le dollar a perdu 97% de sa valeur depuis qu'il n'est plus convertible.

C'est le travail de l'inflation.

Les 97% perdus par les détenteurs de dollars sont dans les poches de l'état américain.

- Le *bitcoin* n'est pas "*virtuel*" :

Le 25 mai 2016 : 1 *bitcoin* = 402 euros = 451 dollars

15 584 000 *bitcoins* en circulation

= 6,264 milliards d'euros = 7,028 milliards de dollars

1 *bitcoin* = 13 dollars le 1 janvier 2013

1 *bitcoin* = 763 dollars le 1 janvier 2014

1 *bitcoin* = 297 dollars le 1 janvier 2015

1 *bitcoin* = 435 dollars le 1 janvier 2016

Plus de 500 millions de \$ investis dans des sociétés liées au *bitcoin* depuis trois ans

5600 nœuds (full node) 100 000 mineurs taille blockchain : 70 giga-octets

- Le *bitcoin* n'est pas "*virtuel*" :

Le 11 avril 2016 : 1 *bitcoin* = 369 euros = 422 dollars

15 418 000 *bitcoins* en circulation

= 5,69 milliards d'euros = 6,51 milliards de dollars

1 *bitcoin* = 13 dollars le 1 janvier 2013

1 *bitcoin* = 763 dollars le 1 janvier 2014

1 *bitcoin* = 297 dollars le 1 janvier 2015

1 *bitcoin* = 435 dollars le 1 janvier 2016

Plus de 500 millions de \$ investis dans des sociétés liées au *bitcoin* depuis trois ans

7000 nœuds

100 000 mineurs

taille blockchain : 65 giga-octets

- Le *bitcoin* n'est pas "*virtuel*" :

Le 10 mars 2016 : 1 *bitcoin* = 376 euros = 415 dollars

15 299 950 *bitcoins* en circulation

= 5,75 milliards d'euros = 6,35 milliards de dollars

1 *bitcoin* = 13 dollars le 1 janvier 2013

1 *bitcoin* = 763 dollars le 1 janvier 2014

1 *bitcoin* = 297 dollars le 1 janvier 2015

1 *bitcoin* = 435 dollars le 1 janvier 2016

Plus de 500 millions de \$ investis dans des sociétés liées au *bitcoin* depuis trois ans

5000 nœuds

100 000 mineurs

taille blockchain : 62 giga-octets

- Le *bitcoin* n'est pas "*virtuel*" :

Le 11 janvier 2016 : 1 *bitcoin* = 410 euros = 446 dollars

15 071 525 000 *bitcoins* en circulation

= 6,18 milliards d'euros = 6,72 milliards de dollars

1 *bitcoin* = 13 dollars le 1 janvier 2013

1 *bitcoin* = 763 dollars le 1 janvier 2014

1 *bitcoin* = 297 dollars le 1 janvier 2015

1 *bitcoin* = 435 dollars le 1 janvier 2016

Plus de 500 millions de \$ investis dans des sociétés liées au *bitcoin* depuis trois ans

5000 nœuds

100 000 mineurs











taille blockchain : 50 giga-octets



Le 21 juin 2016



Jun 2015-juin2016

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)
1	 Bitcoin	\$ 10,613,319,095	\$ 676.71	15,683,750 BTC	\$ 214,744,000	-10.07 %
2	 Ethereum	\$ 1,035,562,436	\$ 12.75	81,237,149 ETH	\$ 47,559,800	11.14 %
3	 Ripple	\$ 227,652,925	\$ 0.006484	35,108,326,973 XRP *	\$ 2,431,820	-4.24 %
4	 Litecoin	\$ 221,585,897	\$ 4.78	46,323,351 LTC	\$ 8,527,180	-12.82 %
5	 The DAO	\$ 96,227,609	\$ 0.082051	1,172,775,159 DAO *	\$ 4,399,710	16.84 %
6	 Dash	\$ 51,727,625	\$ 7.91	6,535,912 DASH	\$ 631,239	-0.67 %
7	 NEM	\$ 43,742,970	\$ 0.004860	8,999,999,999 XEM *	\$ 1,800,740	-19.97 %
8	 Lisk	\$ 34,988,200	\$ 0.349882	100,000,000 LSK *	\$ 1,870,340	7.02 %
9	 MaidSafeCoin	\$ 32,915,359	\$ 0.072733	452,552,412 MAID *	\$ 546,440	4.66 %
10	 Dogecoin	\$ 32,726,495	\$ 0.000312	104,848,925,825 DOGE	\$ 618,379	-7.27 %

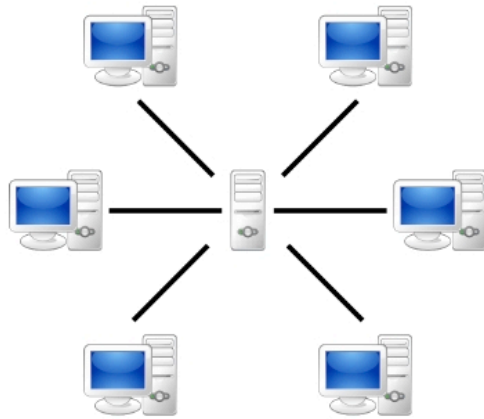
Le 21 juin 2016

- **Les monnaies électroniques ne sont pas une nouveauté.**
- **Opérations bancaires = *jeux d'écritures opérés dans les mémoires des ordinateurs.***
- **L'informatisation du transfert d'argent n'engendre pas de catastrophes.**
- **Les crises financières ne sont pas dues au dysfonctionnement ou à la fraude informatique.**

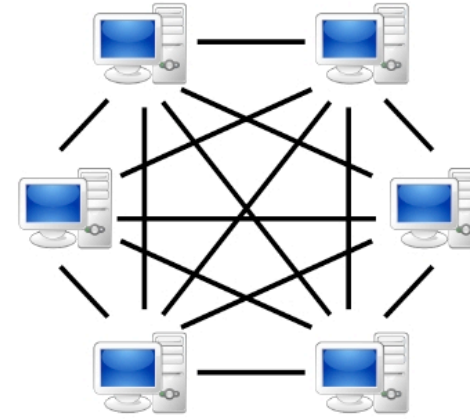
- Aujourd'hui toute monnaie repose sur une *autorité centrale*.
- C'est le cas aussi des *pseudo-monnaies privées*
 - le *dollar Linden* de *Second Life*,
 - les *miles* des compagnies aériennes,
 - les *points* que votre superette inscrit sur votre compte à chaque passage aux caisses.
 - les *monnaies locales* : *Pêche* à Montreuil, *Lac* à Grigny, *Lien* à Saint-Etienne, etc.



- Les *bitcoins* s'autorégulent sans autorité centrale, grâce à un réseau P2P (pair à pair).



Centralisé



P2P

- **Tout est public :**
 - les protocoles de bases,
 - les algorithmes cryptographiques utilisés,
 - les programmes (C++, Python, JavaScript),
 - les données des comptes.

- Chacun peut savoir combien, il y a de *bitcoins* sur chaque compte et vérifier les transactions.

- Cela n'empêche pas un forme *d'anonymat*.



Comptes, porte-monnaie



- Posséder des *bitcoins*, c'est connaître une suite de caractères.
- Une personne peut posséder *plusieurs comptes*.
- Ouvrir un *compte* ne coûte rien et il n'est pas nécessaire de s'identifier pour en créer.
- Chaque *compte* comporte :
 - le **montant** en *bitcoins* de l'argent qu'il contient,
 - une **clef publique** (c'est le numéro du compte),
 - et une **clef privée** qui doit absolument rester secrète.

- Le *numéro secret*

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*

1CC3X2gu58d6wXUWMffpuzN9JAfTUWu4Kj

- Tout support est bon pour conserver les données d'un compte :
un papier, une clef USB, un disque dur, sa mémoire
- Vous gérez vos comptes à l'aide d'un logiciel appelé "wallet" (ou "porte-monnaie").
- Vous pouvez confier la gestion de vos comptes à un tiers.



Exemple de wallet : <https://multibit.org/>

Marché	Monnaie	Dernier
Bitstamp	USD	612,65

Porte-monnaie

Description de votre portefeuille
 0,0252506 BTC (\$15,47)

Description de votre portefeuille
 0 BTC (\$0,00)

Nouveau porte-monnaie

Envoyer Requête Transactions

Adresse

Nom d'transaction

Montant BTC = \$ **Envoyer**

Nouveau **Supprimer** Adresses auxquelles envoyer des bitcoins

Étiquette ^	Adresse
30 maiC	13cia2KGVASavNmRs4niK5RSRfwkB1uLAu

Comment avoir des *bitcoins* ?

- 1 **Recevoir des *bitcoins*** qu'un détenteur vous envoie en échange d'un bien, ou d'argent.
- 2 **Utiliser un distributeur.** Il y en a un à la *Maison du bitcoin*, 35 rue du Caire à Paris.



3 Utiliser une plateforme d'échange qui permet des achats en *euros* de *bitcoins*

Exemple : <https://paymium.com/>

4 Gagner des *bitcoins* en participant aux opérations de contrôle de la monnaie : *minage*.

La gestion des comptes doit être menée soigneusement !

Certains comptes sont gardés « au froid ».

L'argent, c'est la mémoire

Le *bitcoin* se fonde sur la théorie « *Money is memory* » de Narayana Kocherlakota.



=



Argent = Mémoire

Cette idée s'exprime ici sous la forme :

- **Toutes les transactions opérées depuis le début des *bitcoins* sont publiques.**
- **Le nombre de *bitcoins* émis est connu, ainsi que le contenu de chaque compte.**
- **Seul celui qui connaît la clef secrète d'un compte peut dépenser son contenu.**
- **Tout le monde peut participer au calcul de la répartition des *bitcoins* entre comptes.**

- La *cryptographie mathématique* n'est pas utilisée pour cacher de l'information, mais
 - pour **signer les transactions**,
 - pour ordonner les transactions dans la **blockchain** (utilisation des **fonctions de hachage**),
 - pour organiser le contrôle et créer de nouveaux *bitcoins* ("**preuves de travail**", "**minage**")

- Toute transaction est **irréversible**. C'est original.



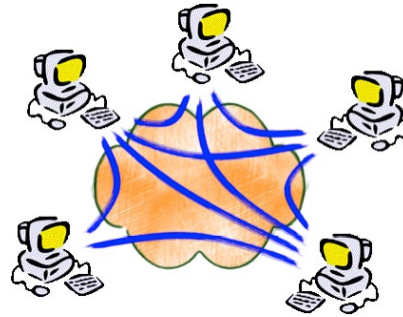


L'absence d'autorité centrale et l'anonymat des comptes ont une conséquence :

Un transfert est rapide et presque sans frais.

Une fois effectué, il est impossible d'agir sur le compte ayant reçu vos bitcoins.

Modèle simplifié du *bitcoin*.



Modèle simplifié du *bitcoin*.

- Un *fichier de compte* que chaque utilisateur (la liste en est fixée) met à jour en permanence.
- Ce *fichier de compte* contient toutes les transactions passées et permet donc de savoir

la somme présente sur chaque compte

- À chaque transaction, tous les utilisateurs sont consultés, et donnent leur accord, après avoir contrôlé que celui qui dépense l'argent le possède.
- Une fois l'accord obtenu, la transaction a lieu, et chacun met à jour son *fichier de compte*.

Modèle simplifié du *bitcoin*.

- Gérer une caisse entre une **dizaine d'amis** qui décideraient par exemple : **1 unité = 1 euro.**
- Si Jean dépense 100 euros dans "la vraie vie", ses 9 amis en versent chacun 10 sur son compte.
- Au départ, pas besoin de faire de versement, chacun se voit attribuer par exemple 1000 unités.
- Pour mettre fin au système, on rééquilibre les comptes et on oublie le *fichier de compte*.

C'est un système parfait. C'est l'idée du *bitcoin*

Modèle simplifié du *bitcoin*.

- Transposer cela sur le réseau et à une échelle plus grande est *impossible* :

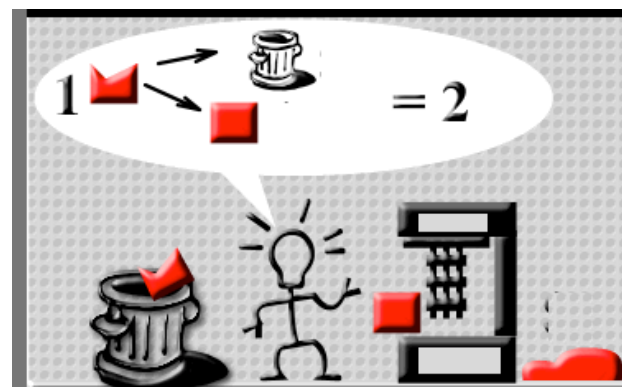
les échanges électroniques ne sont ni parfaits, ni instantanés.

- Certaines parties d'un réseau sont parfois déconnectées.
- Tous les utilisateurs de *bitcoins* ne souhaitent pas participer à la vérification des transactions.
- Il est ennuyeux que la liste des utilisateurs soit fixée.

Il faut perfectionner le modèle !

Le protocole de Nakamoto :

- Des **nouveaux utilisateurs** (comptes) peuvent s'introduire à chaque instant ou se retirer.
- **Suivre** les opérations sur les comptes est facultatif.
- Un **change flottant** permet à la valeur du *bitcoin* d'évoluer.
Aucune valeur n'est attribuée au départ au *bitcoin* .
Celle-ci s'établit spontanément, puis évolue en fonction de **l'offre et de la demande**.
5 octobre 2009 : Publication du premier taux de change bitcoin/dollar. Un bitcoin vaut 0,001 USD.
21 mai 2010 : Hanyecz [achète une pizza pour 10 000 bitcoins](#).
- Résistant aux *pannes* possibles de certaines machines,
à la *coupure* du réseau,
aux *délais de transmission* entre nœuds.



Les doubles dépenses : grave problème !

Le bitcoin tient par l'accord unanime sur les comptes.



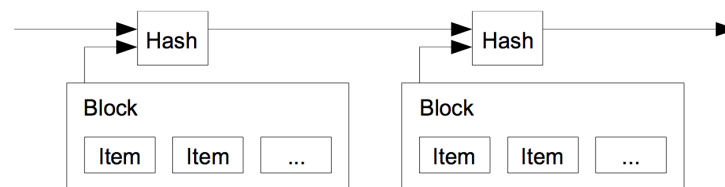
C'est obtenu grâce à la construction cryptographique qui assure que

- personne ne peut augmenter le total des *bitcoins*,
- ni modifier des comptes sans que tout le monde le découvre rapidement.

Une page de transactions toutes les 10 minutes



- Le *cahier de compte* = le *registre* = la **blockchain** évolue par ajout d'une nouvelle *page de transactions* (nommée **block**) toutes les 10 minutes.



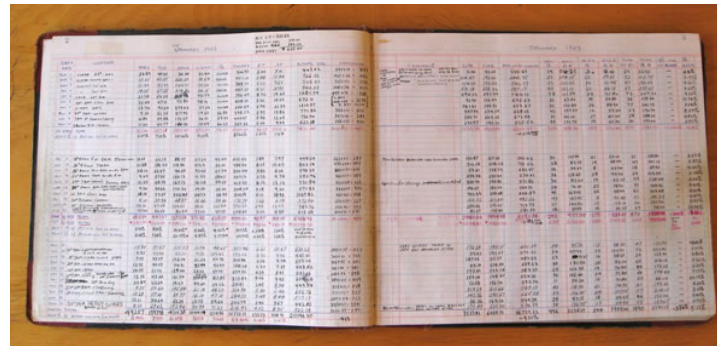
- Chaque page est validée par ceux qui participent à la gestion des comptes.
- Il y a donc **2 types d'utilisateurs** :
 - les utilisateurs simples &
 - ceux qui gèrent une copie de la *blockchain* (environ **76 gigaoctets en juin 2016**).
Ils sont environ 6000.
- Pour inciter à participer, un concours rémunéré se déroule en permanence.
- Un "tirage" désigne toutes les 10 minutes celui qui ajoute la page à la *blockchain*.
- Il est rémunéré par **25 (puis 12,5) bitcoins créés ex nihilo** + les commissions facultatives
- Quand la page est ajoutée, cela valide les transactions qui y apparaissent.

La création de bitcoins toutes les 10 minutes est la seule possible.

Tous les bitcoins existants sont apparus de cette façon.



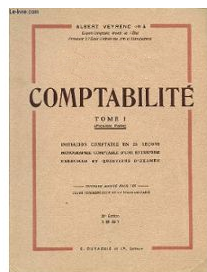
Déroulement d'une transaction



- Lors d'une transaction, les nœuds contrôleurs consultent la *blockchain* et vérifient que le compte qui envoie des *bitcoins* les a vraiment.
- Si le compte en question vient juste de recevoir des *bitcoins* (ils n'apparaissent pas sur la *blockchain*), elle sera refusée.
- Il faut donc attendre environ 10 minutes entre la réception d'une somme et sa dépense.

Le cahier de compte peut être exploré à partir de :

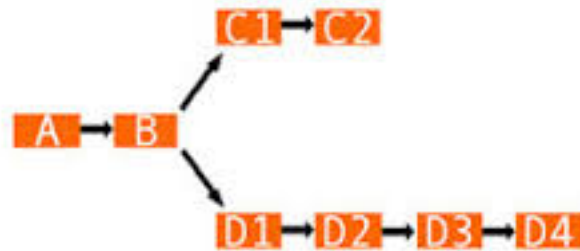
<http://blockchain.info/fr>.



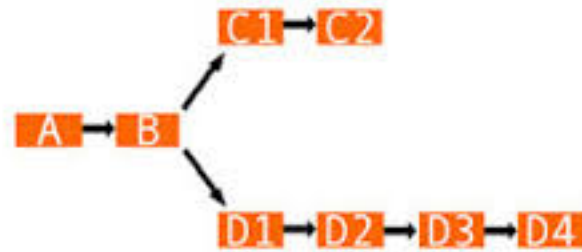
a6188235442621c67e369851b...	< 1 minute	12.13 BTC	<ul style="list-style-type: none"> • Les adresses les plus populaires - Adresses qui ont reçu le plus de paiements • Blocs orphelins - Blocs valides qui ne font pas partie de la chaîne principale bitcoin • Transactions non confirmées - Transactions en attente d'être inclus dans un bloc • Les grosses transactions - Les 100 plus grandes transactions des 50.000 dernières transactions • Double dépense - Double dépense détectée dans les 500 000 dernières transactions • Transactions étranges - Transactions dont nous n'avons pas pu décoder l'adresse de sortie • Statistiques de la piscine minière - Diagramme à secteurs montrant la part de marché des plus importantes piscines minières Bitcoin • Globe des nœuds bitcoin - Globe WebGL montrant les nœuds bitcoin (Requiert Chrome ou Safari) • Liste des nœuds Bitcoin - Un journal regroupant les nœuds bitcoin auxquels blockchain.info s'est connecté • Liste des nœuds - Une liste des super-nœuds-bitcoin les plus connectés • Inventaire des rejets - Les blocs et les transactions qui ont été rejetées par nos nœuds • Mots Adresse - Marquez vos adresses Bitcoin publics. • Mon portefeuille - Gérez votre argent avec le portefeuille Bitcoin le plus avancé sur le web.
cd2489152... (LuckyBit red ↗)	< 1 minute	0.001 BTC	
9555c8bd5... (BTCBlockBet.com-24.414 percent ↗)	< 1 minute	0.019 BTC	
2b6da6567b2e512529791c639...	< 1 minute	0.025 BTC	
09c37bb21498a2deb5e02b102...	< 1 minute	1.165 BTC	
32c61d9c9... (SatoshiBONES 37.5pct ↗)	< 1 minute	0.02 BTC	

Dédoublément de la blockchain (fork)

- Parfois 2 ajouts au cahier se font quasi-simultanément dans 2 parties éloignées du réseau.
- Cela crée temporairement un *dédoublément de la blockchain*.



- Les 2 versions peuvent contenir une dernière page différente. Cela rend possible une double dépense.
- Un procédé de *remise en ordre* du système est prévu.



- Les blockchains continuent chacune de leur côté à ajouter des pages toutes les 10 minutes.
- Les ajouts de pages ne se font pas à la même vitesse exactement.
- La blockchain ayant une "contenu en calcul" le plus grand est considérée comme la bonne.
- Cette règle conduit à l'élimination d'une des blockchains et donc à la

reconstitution d'un état cohérent du système avec une seule blockchain



*Pour être certain qu'une transaction est définitivement valide
il faut non pas attendre 10 minutes, mais plusieurs fois 10 minutes.*

*On considère qu'**une heure** produit une garantie parfaite.
(c'est en train de changer !)*



Principes parfaitement décrits dans l'article d'octobre 2008 de Satoshi Nakamoto :

Nakamoto

5. Network

The steps to run the network are as follows:

- 1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block.
- 3) Each node works on finding a difficult proof-of-work for its block.
- 4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
- 5) Nodes accept the block only if all transactions in it are valid and not already spent.
- 6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.



Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

Le système conçu par Nakamoto se consolide au fur et à mesure
que des gens s'y intéressent



Argument simple... (et un peu naïf) :

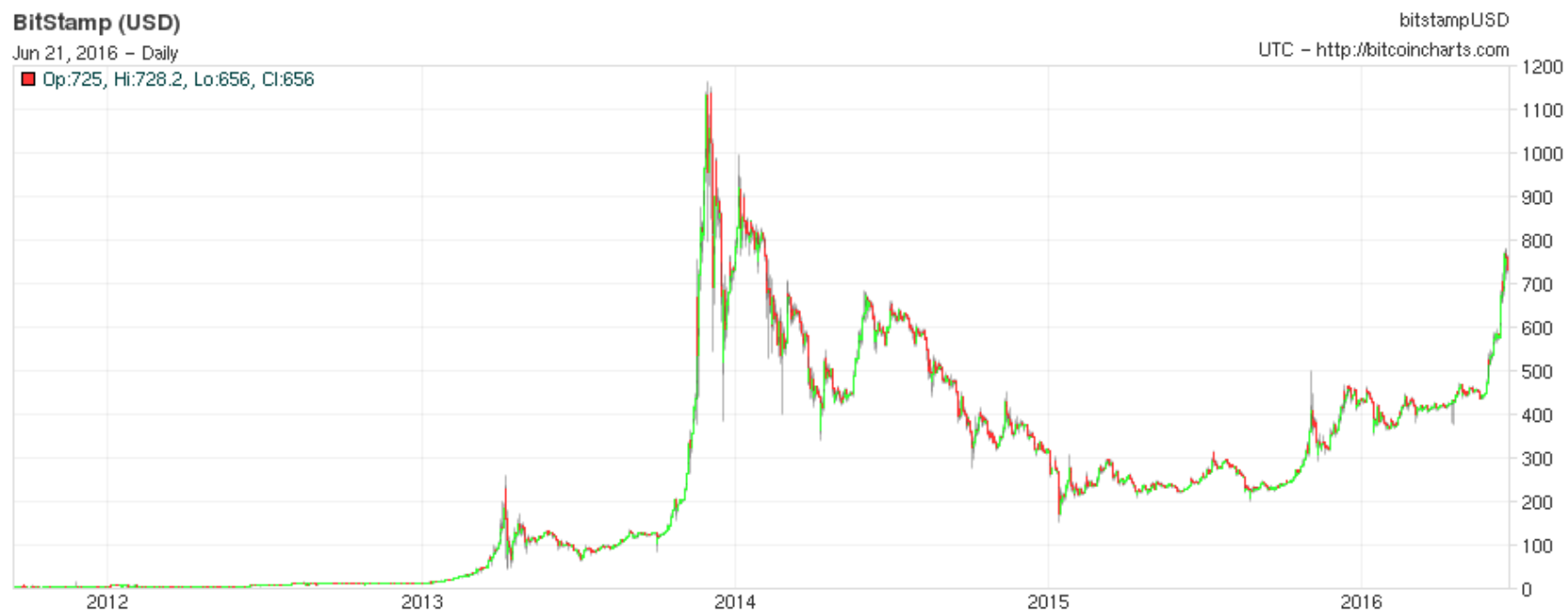
Plus le cours du *bitcoin* monte =>

=> plus il devient intéressant de miner des *bitcoins* =>

=> plus nombreux sont ceux qui minent =>

=> plus le *bitcoin* devient robuste, y compris aux attaques d'acteurs puissants, et donc =>

=> plus son cours a des chances de monter.



21 juin 2016

- Le *bitcoin* n'est pas "*virtuel*" :

Le 21 juin 2016 : 1 *bitcoin* = 590 euros = 676 dollars

15 590 000 *bitcoins* en circulation

= 9,2 milliards d'euros = 10,6 milliards de dollars

1 *bitcoin* = 13 dollars le 1 janvier 2013

1 *bitcoin* = 763 dollars le 1 janvier 2014

1 *bitcoin* = 297 dollars le 1 janvier 2015

1 *bitcoin* = 435 dollars le 1 janvier 2016

Plus de 500 millions de \$ investis dans des sociétés liées au *bitcoin* depuis trois ans

5600 nœuds (full node) 100 000 mineurs taille blockchain : 72 giga-octets

Le minage : une ruée vers l'or numérique



- Désignation des gagnants des 25 *bitcoins* toutes les 10 minutes.
(seulement 12,5 *bitcoins* à partir du 10 juillet 2016)
- Un processus de *preuve de travail* en assure l'honnêteté et l'imprévisibilité.
- On a d'autant *plus de chances* de gagner qu'on a *plus de puissance de calcul*.

Il s'agit d'inverser partiellement la fonction de hachage SHA256

Le travail fait par les machines pour tenter de gagner porte le nom de *minage*,

Ceux qui participent sont les *mineurs de bitcoins*



- Miner est tentant puisque **25 bitcoins = environ 17000 euros (juin 2016)**

- *Les mineurs de bitcoins se sont multipliés.*

6000 nœuds 100 000 mineurs

Pool de mineurs



- Les *mineurs de bitcoins* ont progressivement perfectionné leurs outils.
- Cartes graphiques.
- Cartes spécialisées (circuits ASIC).















- Le système s'ajuste pour que le temps moyen de 10 minutes ne diminue pas.

Tous les 2016 blocks (14 jours),
le système calcule le temps moyen entre 2 blocks,
ajuste la difficulté de la preuve de travail pour qu'il reste 10 minutes.

- La consommation électrique consacrée au minage est considérable.
la consommation d'électricité pour le minage serait équivalente à la consommation d'électricité du Danemark en 2020
- Le phénomène ressemble à une *ruée vers l'or*

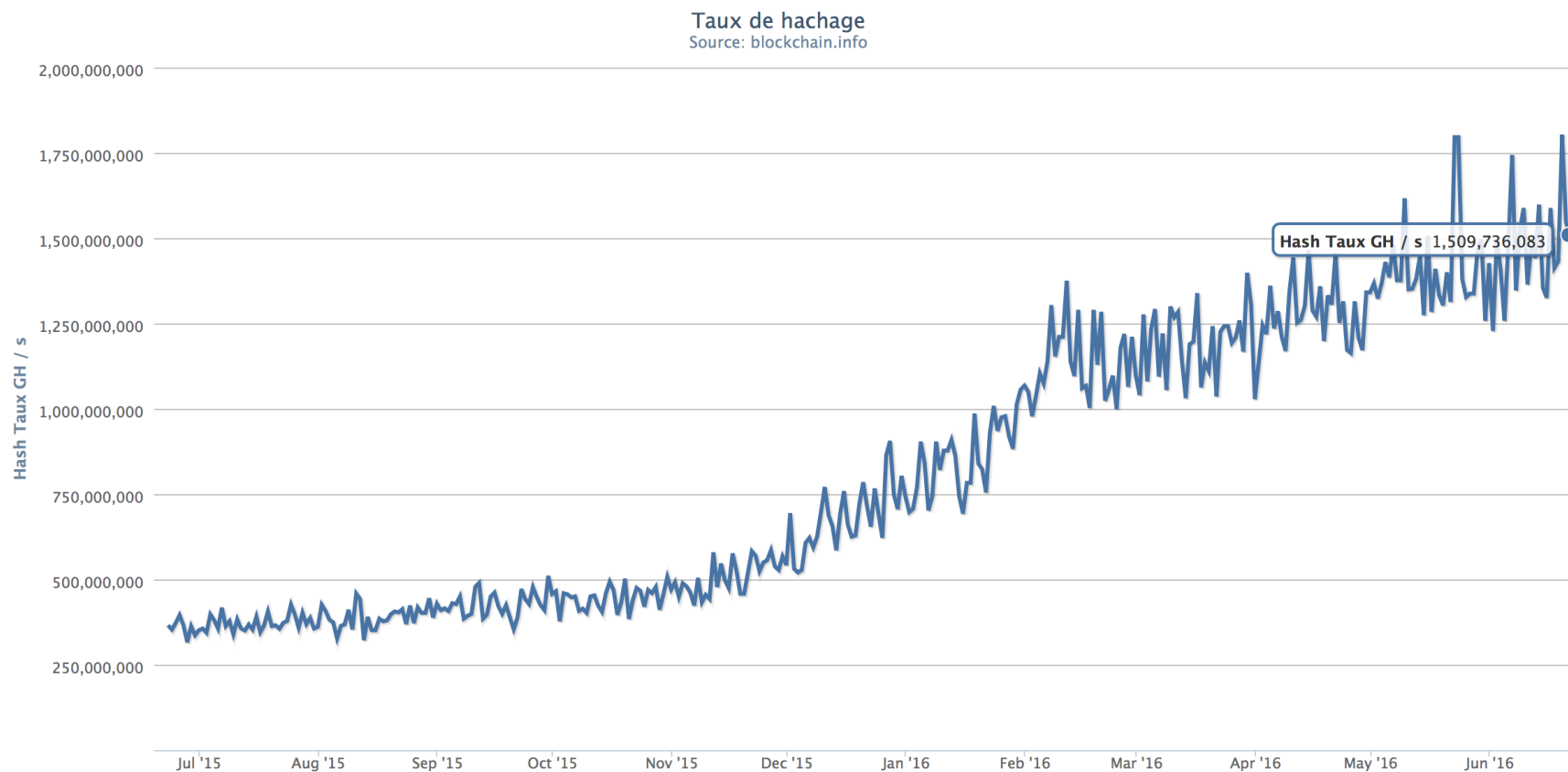


Cent mille fois le plus puissant des ordinateurs !!!

- La puissance consacrée au minage de *bitcoins* est donnée par : <http://bitcoinwatch.com/>
4 230 000 pétaflops (2015)
(1 pétaflops = 10^{15} opérations en virgule flottante par seconde)
- C'est plus de **100 000 fois la puissance du plus puissant ordinateur du monde**



Tianhe-2 (MilkyWay-2) - TH-IVB-FEP Cluster, Intel Xeon

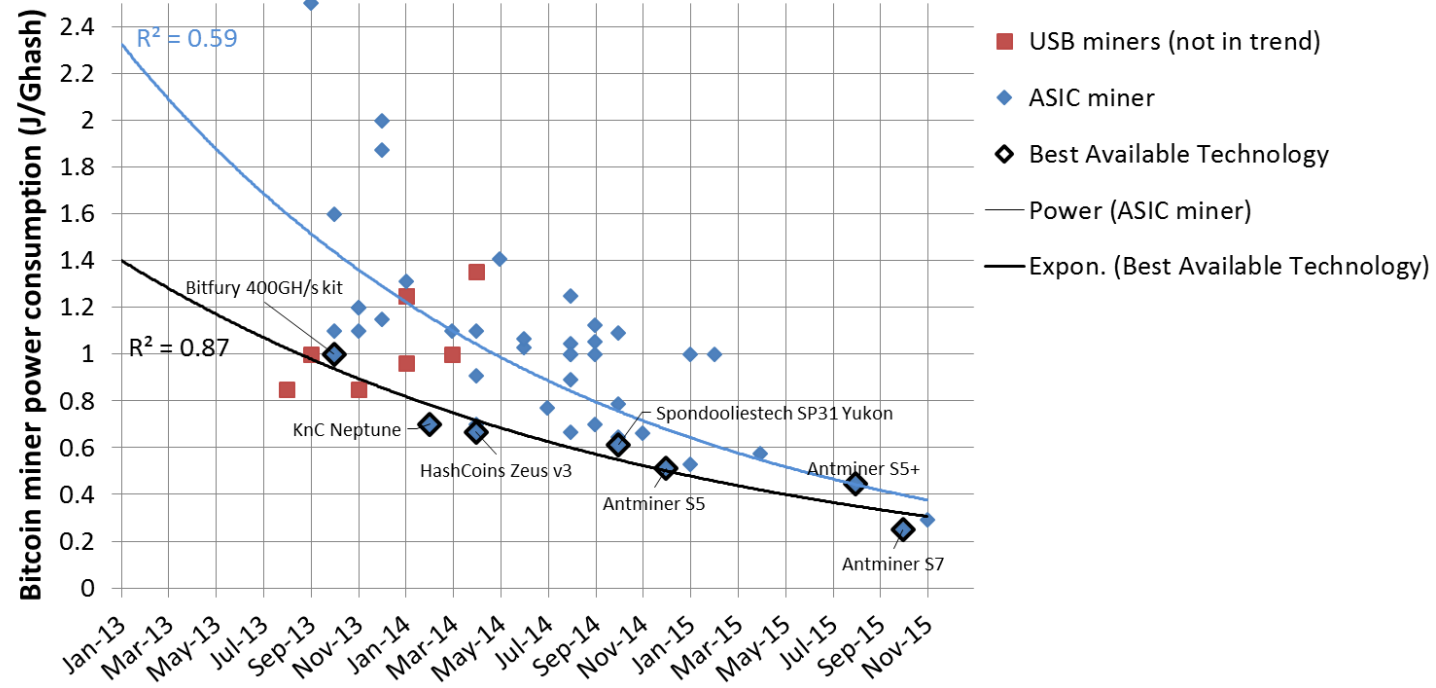


Evolution du *taux de hash* de l'ensemble des mineurs en *Gigahash par seconde* (21-6-2016)

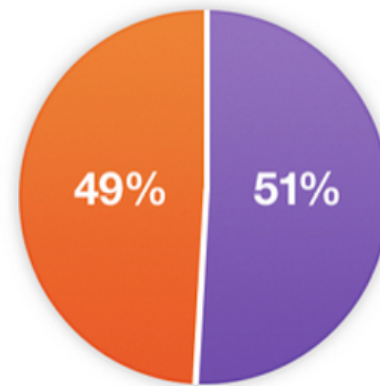
21 juin 2016 :

1 500 000 000 Gigahash = $1,6 \cdot 10^{18}$ calculs

de SHA256 par seconde !!!!



Progrès de la capacité à calculer des "hash" par joule dépensé.



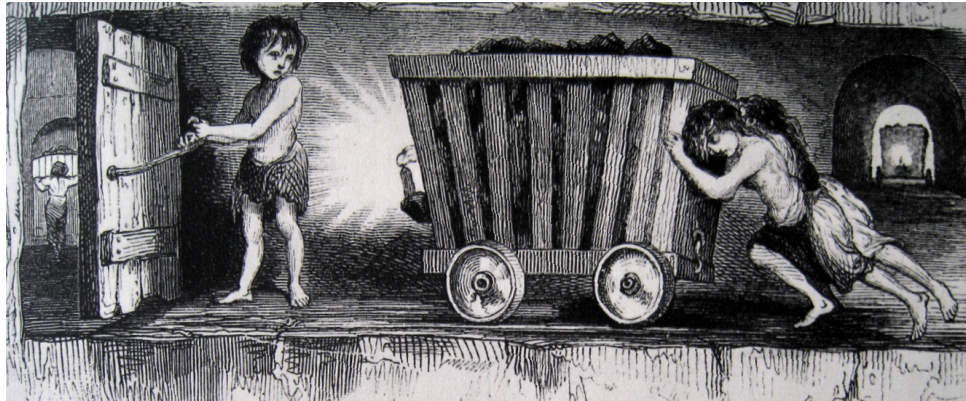
Si un acteur dispose de la moitié de la puissance consacrée au minage,
alors, il peut perturber le fonctionnement de la monnaie *bitcoin*.

- Un énorme gâchis ?
- Les défenseurs du *bitcoin* remarquent que
pour les autres monnaies, c'est la même situation.
- C'est peut-être évitable ?

Primecoin

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- Sunny King
- Les calculs faits font découvrir des **chaînes de nombres premiers.**
- Juillet 2013 : nouvelle crypto-monnaie *Primecoin*



Minage

- En utilisant son ordinateur pour miner, on n'a presque aucune chance de gagner des *bitcoins*.
- Création de «guildes (pool) de mineurs».
- Un vrai problème avec les 51%.

Autres systèmes possibles pour encourager la surveillance de la blockchain

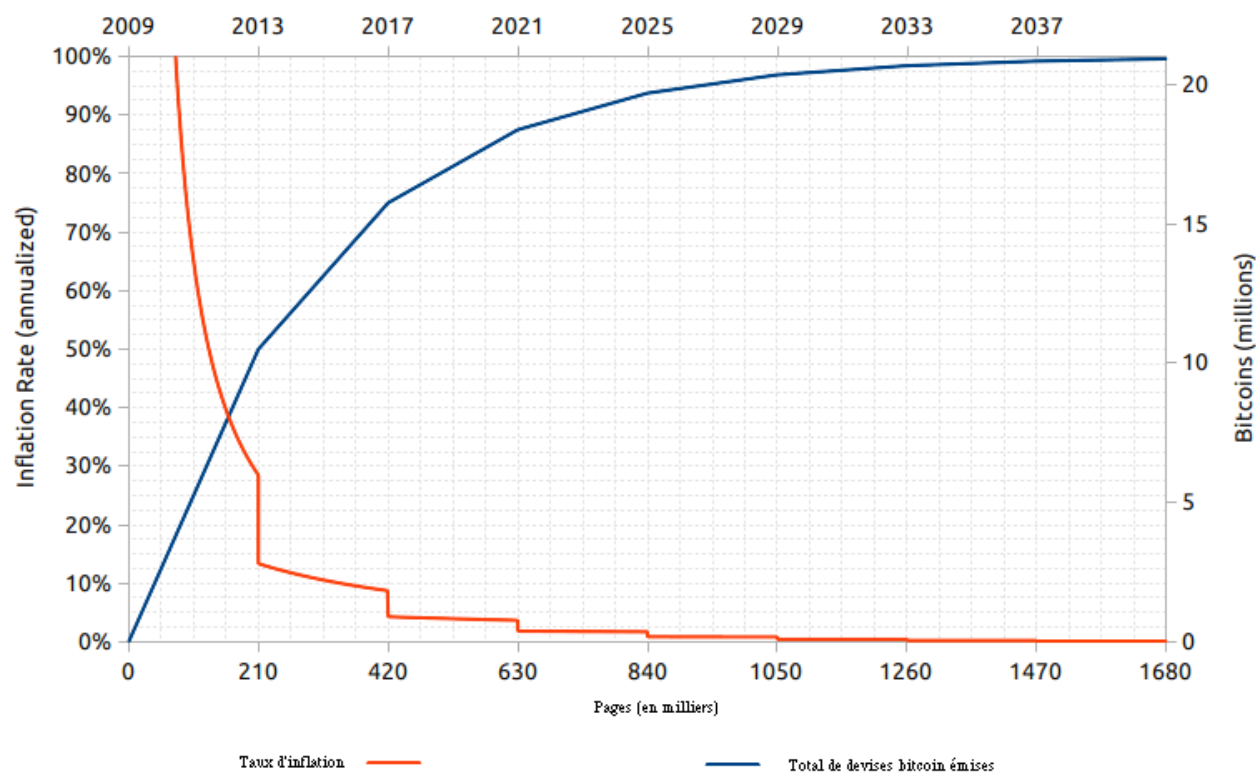
- Minage basée sur la mémoire (Permacoin)
- Minage basée sur la quantité de devises détenue (Proof of stake)
(Ethereum envisage de passer à un système de "Proof of stake".)
- Proof of burn (on accepte de perdre —de brûler— quelques devises)
- Doutes concernant ces alternatives ?

Vingt-et-un millions de *bitcoins* en tout

- Tous les 4 ans (= 210 000 blocs), la somme distribuée est divisée par deux.
- Au départ : **50 *bitcoins***. • Novembre 2012 : **25 *bitcoins***. • **12,5 *bitcoins*** en juillet 2016.
- Un *bitcoin* peut être divisé en unités plus petites : **cent millionième de *bitcoin* (= *satoshi*)**
- Le processus d'émission de nouveaux *bitcoins* aura cessé en 2140.

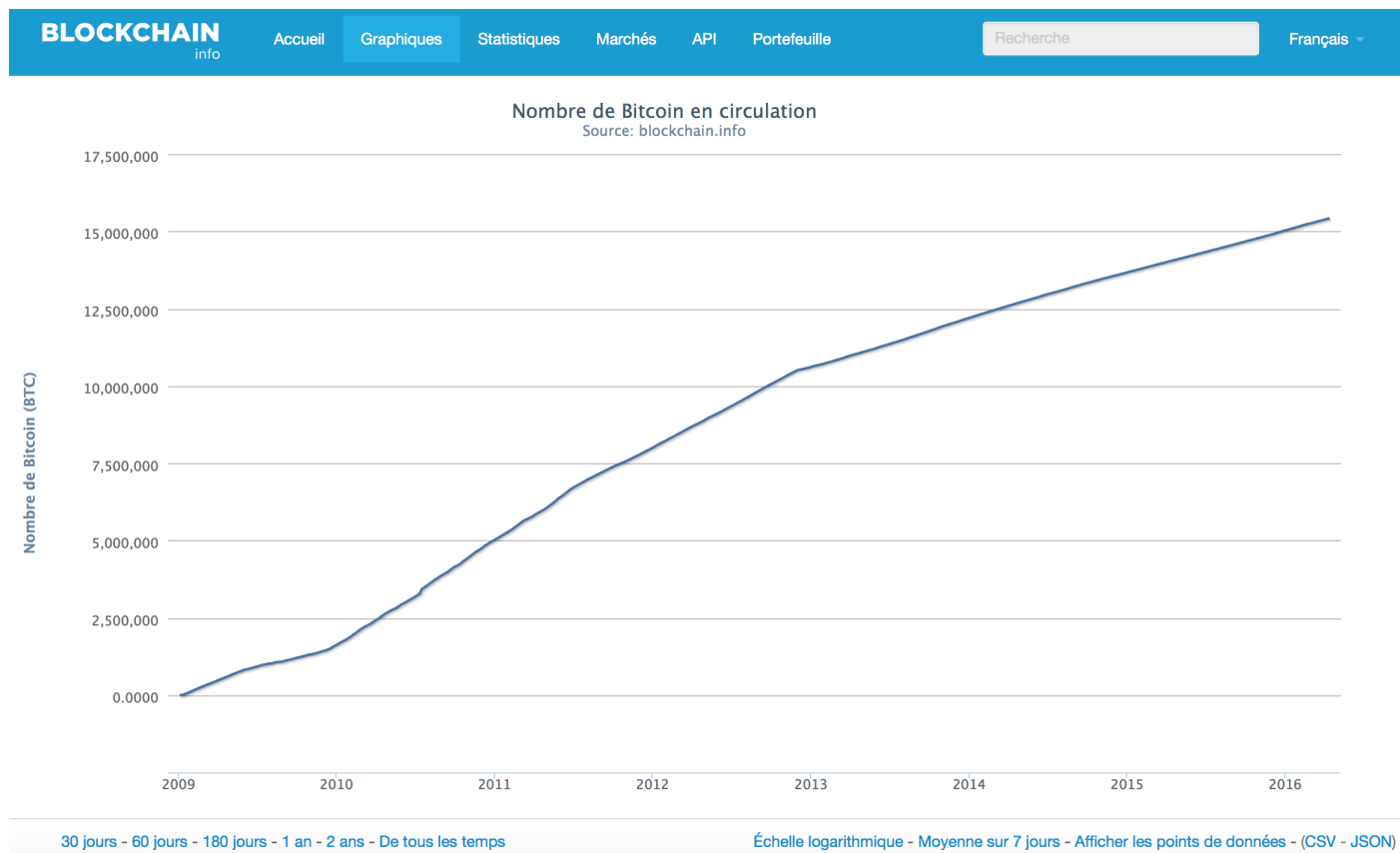
Il y aura alors un total de 21 millions de *bitcoins*.

À partir de cette date, aucun nouveau *bitcoin* ne sera plus jamais créé.



$$210000 * (50 + 25 + 12,5 + 6,25 + 3,125 + \dots) =$$

21 000 000 Bitcoins



Courbe réelle du nombre de bitcoins en circulation

- On peut donner une commission à chaque transaction.



- L'intérêt de miner sera donc préservé, même au-delà de 2140.
Aujourd'hui devenu important.

Problèmes actuels (2016) :

- Passer de "block" de 1 mega-octet à des "block" plus gros.
ou coder autrement les transactions ou ne rien changer
- Dispute Bitcoin XT / classic / unlimited (prévoir plus de ressources par nœud) vs
Bitcoin Core (maintenir les ressources aussi faibles que possible pour les nœuds)
- Véritable guerre
- 7 transactions par seconde ou plus ? (Visa : 2000 transactions par seconde en moyenne)
- Problème avec la Chine (qui détient plus de la moitié de la puissance de minage)
- Conceptions différentes de l'avenir du Bitcoin
- Problème de gouvernance ?
- Sidechain
- Ethereum (smart contract)

L'impossible devenu réalité... et valeur

Mais c'est une expérience !

- La page <http://www.bitcoin.fr/pages/Cours-du-bitcoin> indiquait clairement :

***Le bitcoin est une expérience inédite.
N'y investissez que le temps et l'argent
que vous pouvez vous permettre de perdre.***

La monnaie *bitcoin* tient assez bien depuis 7 ans.

Les avis sont partagés sur son avenir et son intérêt.

Est-ce que vraiment une monnaie décentralisée est viable ?

Est-ce que vraiment une monnaie décentralisée est souhaitable ?



Les blockchains

Registre (= fichier)

partagé (= multiplié sur un réseau P2P)

infalsifiable (= protégé par des primitives cryptographiques)

indestructible (presque... car multiplié)

ouvert (même si des informations chiffrées peuvent s'y trouver)

**composé de "blocs" successivement validés, datés et conservés
par ordre chronologique**

Dans un monde où la quantité d'interactions explose, [...] le modèle de la confiance externalisée ne peut pas faire face à tout et s'essouffle.

La tentation est alors grande pour le régulateur, le tiers de confiance, de réclamer encore plus de moyens afin de faire face à cet accroissement du nombre de transactions.

Malheureusement, cette méthode se heurte à la loi des rendements décroissants : à partir d'un certain seuil, plus on augmente les moyens, plus le système devient dysfonctionnel. Le modèle de la confiance dans la communauté, lui, est bien plus « scalable » et permet de faire face à la montée en charge du nombre d'interactions. [...]

Ce que propose la blockchain est un modèle encore plus puissant que le modèle de la confiance communautaire, c'est un modèle où la confiance transactionnelle est fiable, auditable par tous et distribuée grâce à un mécanisme d'obtention d'un consensus décentralisé.

Yves CASEAU Serge SOUDOPLATOFF mai 2016

Là où le monde ancien ne se pensait qu'en mode « diffusion », et surtout diffusion de masse, l'Internet a montré que tout le monde pouvait être créateur et diffuseur de contenus [...]

Là où le monde ancien raisonne en logique de « fournisseur vers client », Internet a montré la faisabilité de modèles d'échanges entre pairs à grande échelle.

Tout ceci ne pouvait que s'appliquer un jour au modèle transactionnel : là où le monde ancien pense qu'il faut obligatoirement un tiers de confiance, là où l'Internet 2.0 passe encore par des organismes proposant des plateformes de mise en relations, le modèle de la blockchain montre qu'on peut s'en passer et créer un pur modèle pair à pair.

En ce sens, la blockchain est la version transactionnelle des réseaux de pair à pair.

Yves CASEAU Serge SOUDOPLATOFF mai 2016

Applications possibles (en dehors d'une monnaie)

A

Dépôt d'informations datées permettant d'attester qu'une information était bien détenue par une certaine personne à une date donnée (se substituerait aux enveloppes Soleau de l'INPI).

L'information peut être chiffrée ; quand on voudra rendre public le contenu on donnera la clef.

On peut aussi ne déposer sur la blockchain que l'empreinte du fichier (on perd l'indestructibilité).

B

Courier électronique

Il pourra être chiffré ou non, mais il sera infalsifiable et indestructible.

On peut aussi, pour les courriers trop volumineux, ne déposer que l'empreinte (on perd d'indestructibilité)

C

Dépôt de diplômes

La blockchain serait par exemple gérée par toutes les universités et écoles, qui elles-seules pourraient y écrire (en ajoutant une signature propre à chacune pour plus de sécurité)

D

Smart Contract

Plusieurs signatures, déclenchement lié à des évènements particuliers (variation de cours, d'indices divers, etc.), à des dates atteintes.

Possibilité d'utiliser un langage Turing-complet pour programmer ces "contrats" (comme avec Ethereum)

E

Certificats de propriété, cadastres, engagements.

F

Opérations financières

G

Votes

H

Brevets, certificats d'antériorité

I

**Jeux (prouvablement "fair"), paris,
plateforme de prédiction**

J

**Fond d'investissement automatique et décentralisé : il reçoit de
l'argent, il organise des votes, il investit dans les projets
sélectionnés par les votes.**

Plus généralement :

DAO Decentralized autonomous organizations

Blockchain Use Cases: Comprehensive Analysis & Startups Involved



Attention !

Il faut résoudre de nombreuses questions pour concevoir une application blockchain (car le concept n'est pas très précis)

1

Sera-t-elle totalement publique ?

**Ou seulement publique en lecture, et privée en écriture
ou d'usage réservé à une collectivité réduite ?**

2

Ecrira-t-on en clair ou en chiffrant ce qu'on écrit (ou un mixte) ?

Signera-t-on ce qu'on y écrit ?

3

Sera-t-elle associée à une monnaie cryptographique ?

Quelles en seront alors les caractéristiques ?

4

**Quel système d'incitation est prévu
pour encourager les "full nodes" ?**

Que devient le risque d'attaque 51% ?

Comment éviter la concentration du pouvoir ?

5

Envisage-t-on vraiment qu'il n'y ait aucun contrôle centralisé, ou est-ce qu'on fixe un ensemble limité d'administrateurs et de détenteurs de la blockchain ?

6

Souhaite-t-on limiter ce qui est écrit sur la blockchain :

- on peut envisager de n'écrire que des empreintes de fichiers qui seraient présents ailleurs ;**
- on peut envisager que la blockchain soit découpée et que chaque détenteur n'en garde qu'une partie (par exemple un dixième).**

7

Quelles sont précisément les primitives cryptographiques utilisées ?

Qu'est-il prévu pour les changer si cela se révèle nécessaire ?

8

**La programmation des actions sur la blockchain est-elle limitée
(comme pour le bitcoin)**

ou Turing-complète (comme pour Ethereum) ?

C'est le problème du langage des "smart contract"

9

Comment se fait l'évolution (mises à jour, gestion de crise)

Problème de la gouvernance :

- elle peut être ouverte (comme pour le bitcoin)
ou plus ou moins privée.**

Quelques événements récents

30 juillet 2015 : Lancement Ethereum

15 septembre 2015 : création de R3 CEV : entreprise réunissant 42 banques pour étudier et développer les blockchains

1er mai 2016, "*The DAO*" (*Decentralized autonomous organisation*) est créé par le déploiement des smart-contracts sur Ethereum.

The DAO est une "entreprise" destinée à collecter des fonds pour financer des projets autour de Ethereum.

Elle "collecte" l'équivalent de 150 millions de dollars en quelques jours

17 juin 2016, Attaque grave de The DAO qui se fait soustraire l'équivalent de 50 millions de dollars.
Baisse sensible temporaire de l'Ether

Prise de conscience qu'il faudrait être prudent avant de confier à un "smart contract" des sommes importantes car par nature on ne peut pas les corriger rapidement.

Soft-fork ou hard-fork en discussion ?

Crise ???



Pourquoi est-ce que le bitcoin n'a pas inventé plus tôt ?

Avant 2008, il était impossible d'envisager une telle monnaie.

Progrès récents.

-a-

Il fallait un réseau mondial fiable

-b-

Rien de possible non plus sans d'importantes puissances de calcul et de mémorisation informatique.

-C-

Les avancées de la cryptographie mathématique.

Le *bitcoin* est le résultat des progrès dans la compréhension et la mise au point de primitives cryptographiques.

(arithmétique, théorie de la complexité, algorithmique fine, etc.)

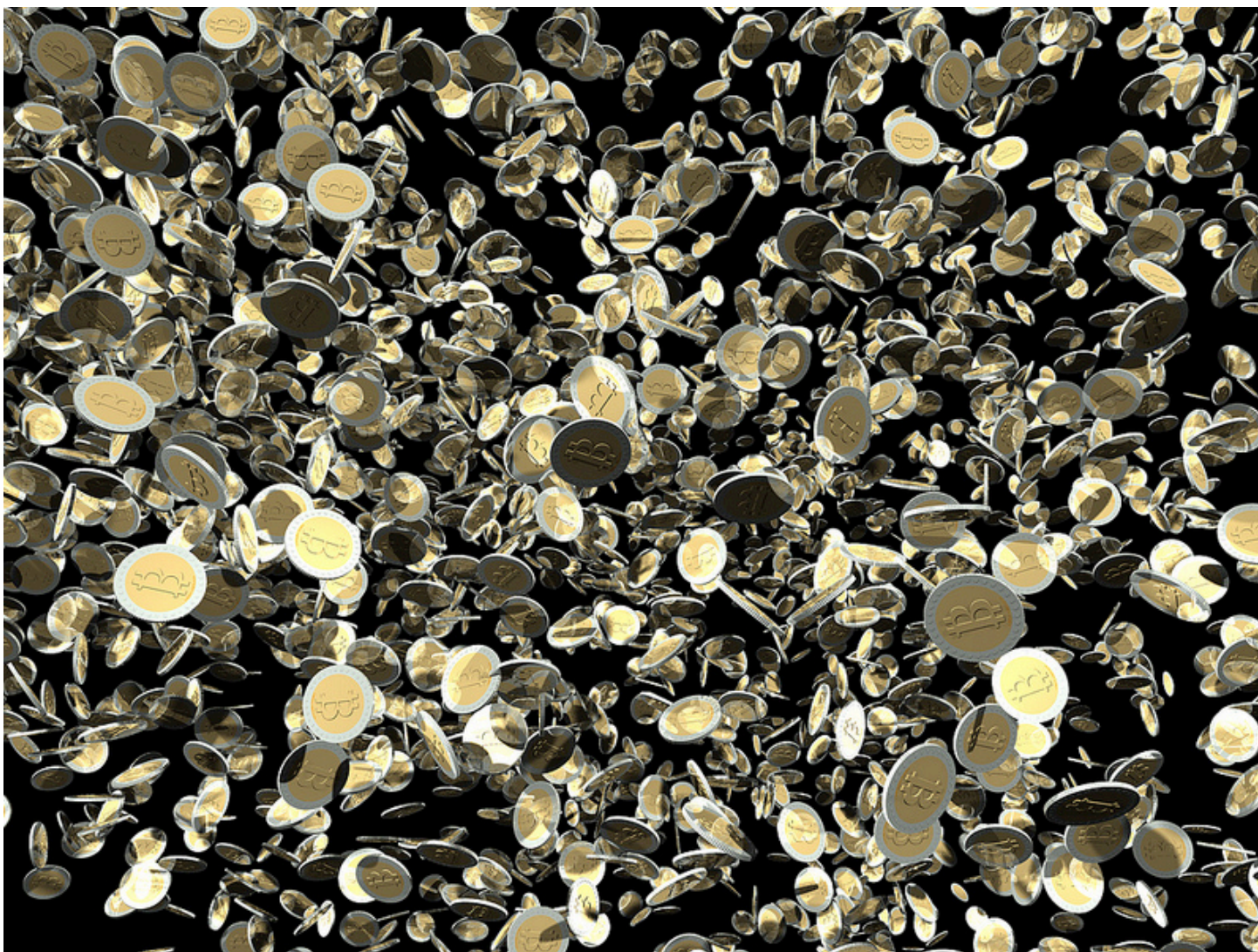
Tout vient de la science cryptographique, donc les mathématiques.

-d-

Essentielle aussi est la communauté des passionnés — un peu anarchistes — qui s'occupe des programmes libres et des réseaux P2P.

Ils rendent possible l'utilisation pratique des *bitcoins* gratuitement en évitant qu'un groupe, une banque ou un État ne s'empare de ce qui est une monnaie commune, universelle et — certains le disent — démocratique.





La naissance du *bitcoin*

Le mystérieux Satoshi Nakamoto



- Le *bitcoin* a été défini en 2008 par un personnage qui se présente sous le nom de *Satoshi Nakamoto*.
- Il a écrit qu'il avait travaillé deux ans à la conception de sa monnaie.
- Satoshi Nakamoto garde l'anonymat.
- Il se peut qu'il s'agisse en fait d'un groupe de plusieurs personnes.
- Vue la façon dont le protocole qui gère la nouvelle monnaie numérique a été fixé, il est certain que Nakamoto possède des connaissances de très bon niveau en cryptographie.
- On analyse la façon dont il s'est exprimé, on établit des listes de personnes ayant les compétences requises ...et on spéculé.



- Des arguments assez forts semblent désigner
Nick Szabo

- **L'anonymat** des utilisateurs des *bitcoins* est assuré par le fait que seuls les numéros de compte et les contenus des comptes sont nécessaires pour gérer la *blockchain*.
- L'anonymat n'est pas absolu.
- On peut suivre le déplacement des *bitcoins* d'un compte à l'autre.
- Au moment de transformer des *bitcoins* en euros l'anonymat est encore plus difficile.

**Des chercheurs, dont Sergio Lerner, en étudiant la *blockchain* concluent que :
Nakamoto possède probablement l'équivalent de 10% des *bitcoins* émis à ce jour.**

- Au lancement de la monnaie, Nakamoto fut le seul à «miner les *bitcoins* ».

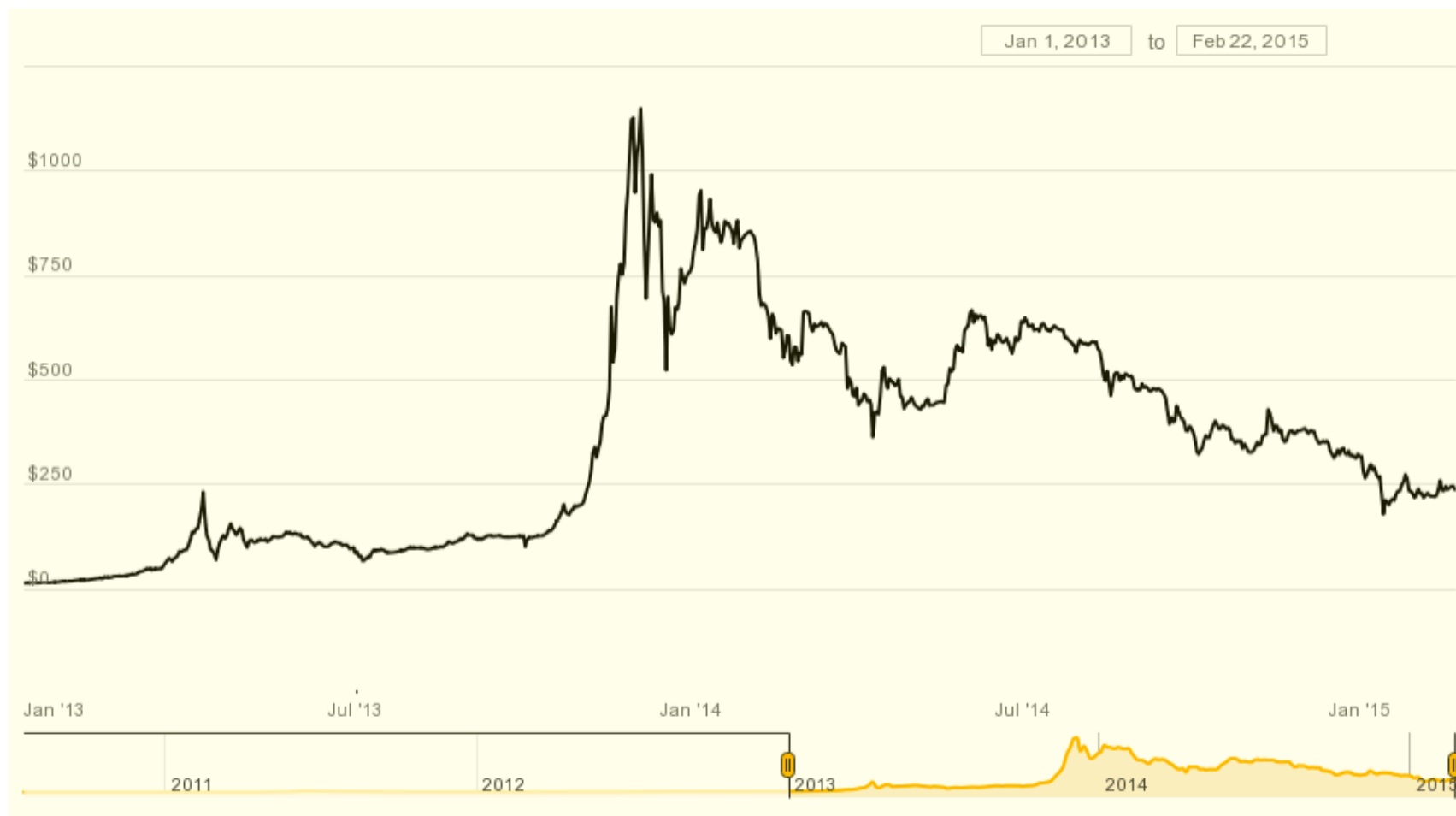
Il lui sera sans doute difficile de remettre sa fortune sur le marché sans dévoiler son identité.



Les cours, la capitalisation, les «bulles»



- La première page du cahier de compte du *bitcoins* a été publiée le 3 janvier 2009.
- Les *bitcoins* sont émis à un rythme régulier.
- 50 *bitcoins* nouveaux ont été créés toutes les 10 minutes, jusqu'au 22 novembre 2012.
- 25 nouveaux *bitcoins* sont créés aujourd'hui toutes les 10 minutes.
- Le nombre de *bitcoins* émis sera divisé par 2 tous les quatre ans.
- Le total des *bitcoins* émis ne dépassera jamais 21 millions.

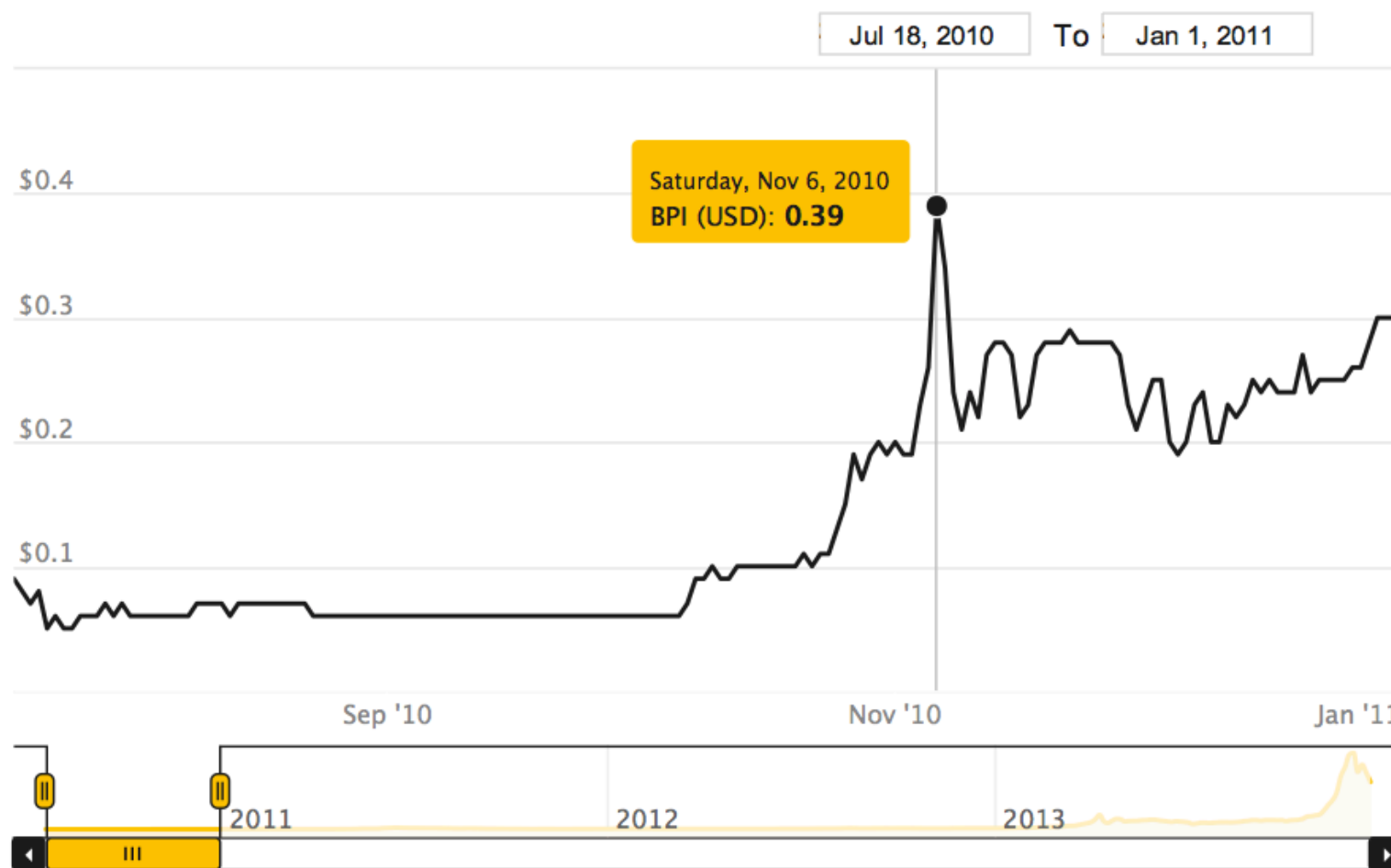




Les cinq bulles du *bitcoin*

- Les montées brusques du *bitcoins*, suivies de baisses ne sont pas un phénomène nouveau.
- Il y a déjà eu «5 bulles».
- Ces «bulles» doivent-elles vraiment être appelée des «bulles» ?
À chaque fois, le cours finit par se stabiliser au-dessus de sa valeur d'avant la «bulle»
- Il semblerait plus sage de parler de «bouffée de volatilité».

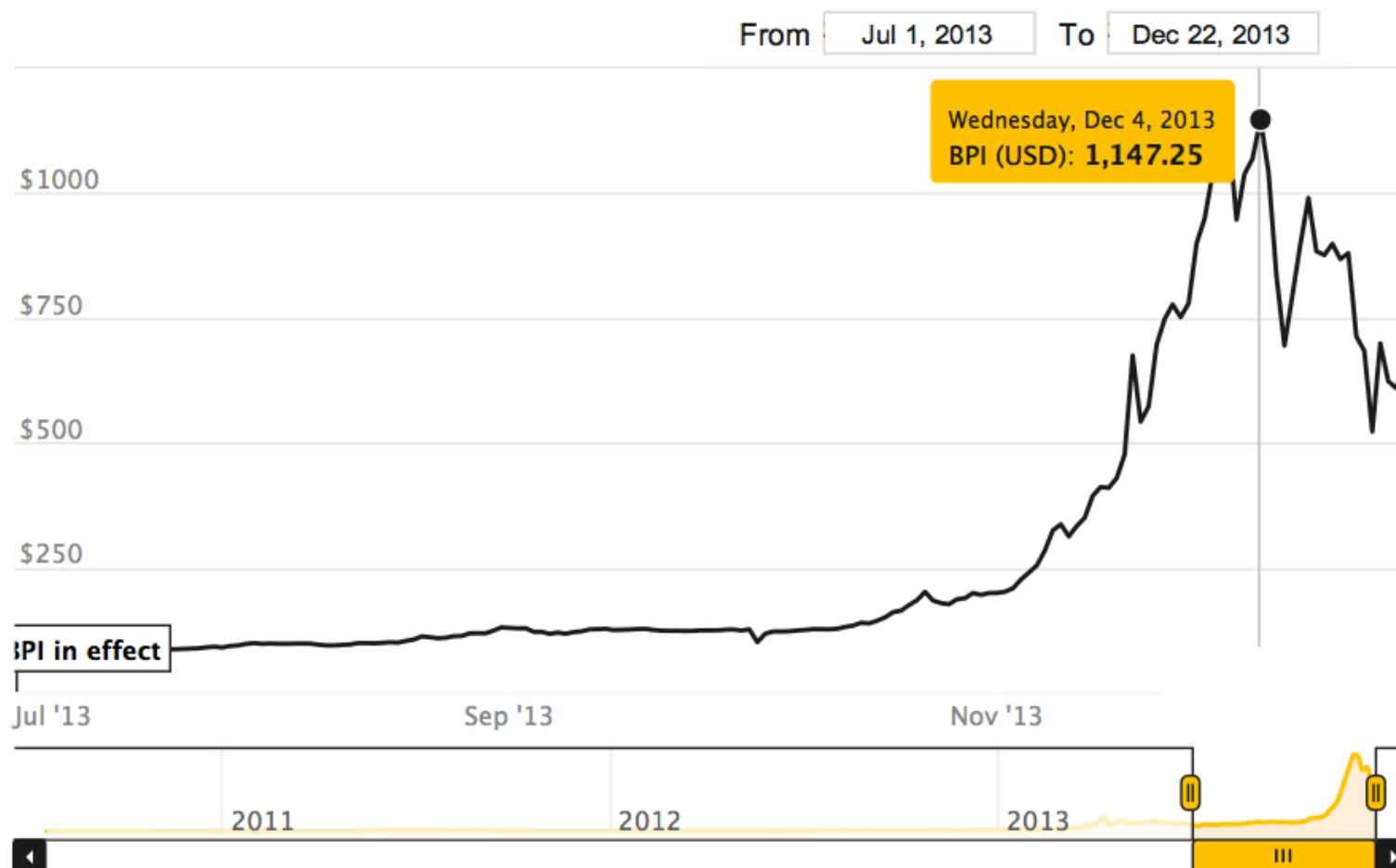






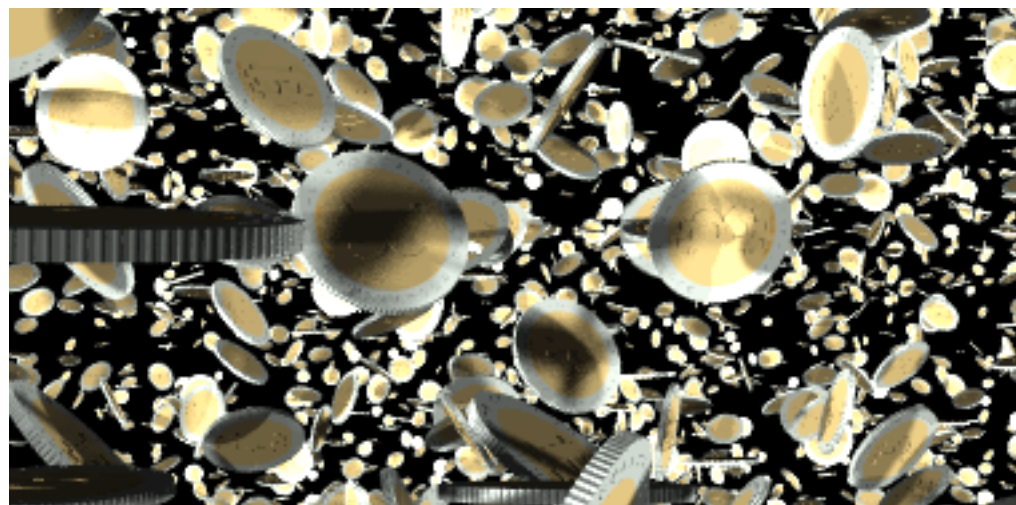








Forces et fragilités des *bitcoins*





Nouveautés, forces et qualités des *bitcoins*

- La monnaie *bitcoin* est basée sur un réseau pair à pair (P2P) et des logiciels libres et gratuits. Elle est donc indépendante de toute banque, n'est soumise à aucune autorité centralisée et offre une transparence complète.
- Les transactions de *bitcoins* sont rapides et irréversibles (après un délai d'une heure ou moins). Personne ne peut agir sur les *bitcoins* de vos comptes sans votre consentement.
- Il n'y a pas de frais de transaction ou de gestion, ou ils sont minimes (électricité, réseau, commissions volontaires et déterminées par l'utilisateur).

- Le nombre de *bitcoins* est rigoureusement fixé et ne dépassera jamais 21 millions. Avec les *bitcoins*, vous échappez au risque qu'un acteur dominant (une banque centrale) décide de faire fonctionner la planche à billets, et par ce moyen indirect vous prenez de l'argent par l'inflation créée.

***Une once d'or valait 35\$ en 1971 quand la convertibilité a été abandonnée.
Elle en vaut environ 1200 aujourd'hui : le dollar a perdu 97% de la valeur !!!***

- Anonymat : le réseau fonctionne à partir de comptes. Posséder un compte c'est connaître la clef privée qui lui est associée. L'identité des utilisateurs n'est utile à aucun moment. L'anonymat n'est cependant pas total

- Un *bitcoin* peut être divisé en fractions de *bitcoin* jusqu'au : $1/100\ 000\ 000$.

- Le *bitcoin* (à cause du nombre maximum de *bitcoins* en circulation) est (probablement) intrinsèquement déflationniste : il prend petit à petit de la valeur.

Non seulement vos économies ne sont pas rongées par l'inflation, mais elles s'apprécient... à moins que vous perdiez tout parce que le protocole *bitcoin* s'effondre.

- Le *bitcoin* a été conçu pour que l'intérêt de ceux qui s'en occupent est qu'il fonctionne bien, et plus il prend de la valeur plus les contrôles sont nombreux.
- Les protocoles et programmes permettant la gestion des transactions peuvent évoluer, mais cela ne peut se faire que par vote et donc dans l'intérêt de tous.



Doutes, fragilités et risques des *bitcoins*

- L'anonymat de Nakamoto l'inventeur et les *bitcoins* qu'il a gagnés facilement au départ de la monnaie créent un sentiment désagréable et font craindre une combine.
- Aujourd'hui le *bitcoin* est économiquement tout petit à côté des autres monnaies auxquelles il ne peut donc pas prétendre se substituer : il y a quelques milliards de dollars en *bitcoins*, alors que la devise américaine par exemple a été émise à hauteur de 1 200 milliards (uniquement en billets).
- La monnaie *bitcoin* repose sur des protocoles cryptographiques dont la robustesse n'est pas démontré.
Il faut faire confiance à **l'état de l'art public** en cryptographique.

- Le système de gestion des *bitcoins* repose sur un ensemble de protocoles qui ont été rendus opérationnels par des programmes. Des erreurs peuvent s'y trouver.
- Le *bitcoin* reste assez **compliqué** à comprendre et donc suscite la méfiance du plus grand nombre.
Le *bitcoin* est peut-être génial, mais c'est une monnaie de geek !
- Relativement peu de sites et peu de commerçants acceptent les *bitcoins* aujourd'hui.



- Le *bitcoin* favorise le blanchiment d'argent sale, facilite les trafics en tout genre, et permet la fraude fiscale.

- Le *bitcoin* semble intrinsèquement déflationniste ce que certains considèrent comme négatif car cela constitue un frein à la circulation de l'argent, et surtout,

- Le cours du bitcoin est très volatil du fait des incertitudes qui l'entourent encore.

- Le *bitcoin* pourrait être l'objet d'interdictions ou de contrôles stricts imposés par des États voulant protéger leurs propres monnaies.
- Il n'est pas impossible que le *bitcoin* soit victime d'attaques menées par des agences comme la NSA qui tenteraient de briser toute confiance en lui, pour maintenir les monopoles monétaires actuels.
- L'anonymat y est imparfait.
- Le succès des *bitcoins* a inspiré toutes sortes d'autres Nakamoto et des dizaines de nouvelles crypto-monnaies directement copiées sur lui ont vu le jour récemment. Certaines un peu différentes et encore mieux conçues pourraient capter l'intérêt et faire se déplacer l'argent misé aujourd'hui sur les *bitcoins*.

- L'évolution possible des protocoles et programmes —prévue mais au fonctionnement délicat— conduit à la mise en place d'une forme d'administration centralisée constituée par l'ensemble des nœuds les plus puissants du réseau collectif de contrôle. Cela ferait à terme ressembler le *bitcoins* aux monnaies usuelles dont Nakamoto voulait se démarquer.

Sur ce point voir : Joshua Kroll, Ian Davey, Edward Felten, The Economics of bitcoin Mining, or bitcoins in the Presence of Adversaries, The Twelfth Workshop on the Economics of Information Security, 2013.



La signature par cryptographie à double clef



- Un protocole de signature à double clef est la donnée de deux fonctions f et g
- Alice dispose de deux clefs A_{pri} (clef privée) et A_{pub} (clef publique).
- La clef A_{pub} est transmise à tout le monde, mais la clef A_{pri} n'est connue que par Alice.
Si le protocole est bon, il est impossible en pratique de déduire A_{pri} à partir de A_{pub} .
- Les deux fonctions f et g servent à signer un message, et à lire la signature.

Soit M un message à signer. Alice applique f aux données A_{pri} et M

$$f(A_{\text{pri}}, M) = M' \quad \text{ce sera le message signé par Alice}$$

- Toute personne ayant en main M' et connaissant la clef publique d'Alice vérifiera qu'Alice a signé :

$$g(A_{\text{pub}}, M') = M$$

- Alice peut en fait transmettre à la fois **M** et **M'**, **M'** servant seulement à contrôler que Alice a bien signé **M**.

Il existe de nombreuses façons de choisir les fonctions f et g .

Celle qui sert pour la monnaie *bitcoin* est basée sur la cryptographie à **courbes elliptiques**, dite ECDSA (**Elliptic Curve Digital Signature Algorithm**).

La courbe employée est **secp256k1**.

Une autre solution aurait pu être le **RSA** (Rivest-Shamir-Adleman) plus connu mais demandant des clefs plus longues.

Et si le protocole de signature était cassé ?



- Si quelqu'un disposant d'une clef publique A_{pub} savait calculer facilement la clef privée associée A_{pri} , alors cette personne serait en mesure de **dépenser le contenu de tous les comptes**.
- À condition de le faire progressivement pour ne pas sa faire repérer cette personne serait très riche !
- Les détenteurs des comptes ne s'en apercevraient que lorsque consultant la somme liée à leur compte (et donc allant lire le *cahier de compte*) ils découvriraient que leur compte est vide.
- Notons que ce *vidage* des comptes peut s'opérer même si le porte-monnaie est sur un disque dur déconnecté du réseau et éteint, même si la clef privée du porte-monnaie n'est écrite que sur une feuille de papier, et même si elle est perdue.

- On considère que personne ne disposera jamais du moyen pratique de calculer A_{pri} à partir de A_{pub} , ou que si cela se produit, la faiblesse du protocole de signature aura été repérée et qu'on aura opéré à temps le changement de cette partie du protocole *bitcoin*.
- La possibilité d'adapter et donc de corriger des faiblesses qu'on repèrerait dans le protocole *bitcoin* est prévue dans le protocole *bitcoin*.

Protocole d'une transaction

Alice veut faire un paiement en *bitcoins* à **Bernard**.

Leurs ordinateurs vont opérer une série d'échanges.

Ces échanges sont gérés automatiquement par le logiciel installé sur leur ordinateur.

La transaction qui résulte des échanges entre Alice et Bernard sera publique et permettra la mise à jour par tous du *cahier de compte*.

- Alice souhaite envoyer N *bitcoins* à Bernard.
- Bernard communique sa clé publique B_{pub} à Alice.
- Alice constitue un message M de transaction contenant
la clé publique de Bernard $[B_{pub}]$ la somme $[N]$ à transférer $[M = B_{pub}N]$ (et d'autres choses)

$$M = [B_{pub}] + [N] + [B_{pub}N]$$

- Alice signe la transaction \mathbf{M} avec sa clé privée, c'est-à-dire calcule une suite de symboles $\mathbf{M}' = f(\mathbf{A}_{\text{pri}}, \mathbf{M})$ qui avec sa clé publique redonne \mathbf{M} :

$$g(\mathbf{A}_{\text{pub}}, f(\mathbf{A}_{\text{pri}}, \mathbf{M})) = g(\mathbf{A}_{\text{pub}}, \mathbf{M}') = \mathbf{M}$$

- Alice diffuse la transaction signée $\mathbf{M} + \mathbf{M}'$ sur le réseau afin qu'elle soit vue par tout le monde.

En regardant cette transaction, tout le monde voit qu'Alice veut transférer \mathbf{N} *bitcoins* à Bernard.

Personne d'autre qu'Alice ne peut envoyer une telle transaction sur le réseau.

Son envoi est donc la preuve qu'Alice est d'accord pour le transfert.

Tout le monde considérera donc le transfert comme valide.

Le hachage et les preuves de travail

- Une fonction de hachage est une fonction h qui à toute suite de symboles S 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 $h(S) = R$.
- Si h est une fonction de hachage cryptographique 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.
- 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.

Ceux qui prétendent avoir trouvé S ont fourni un travail 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 jusqu'à obtenir un double 6

(il faudrait en moyenne qu'il les lance 36 fois pour réussir).

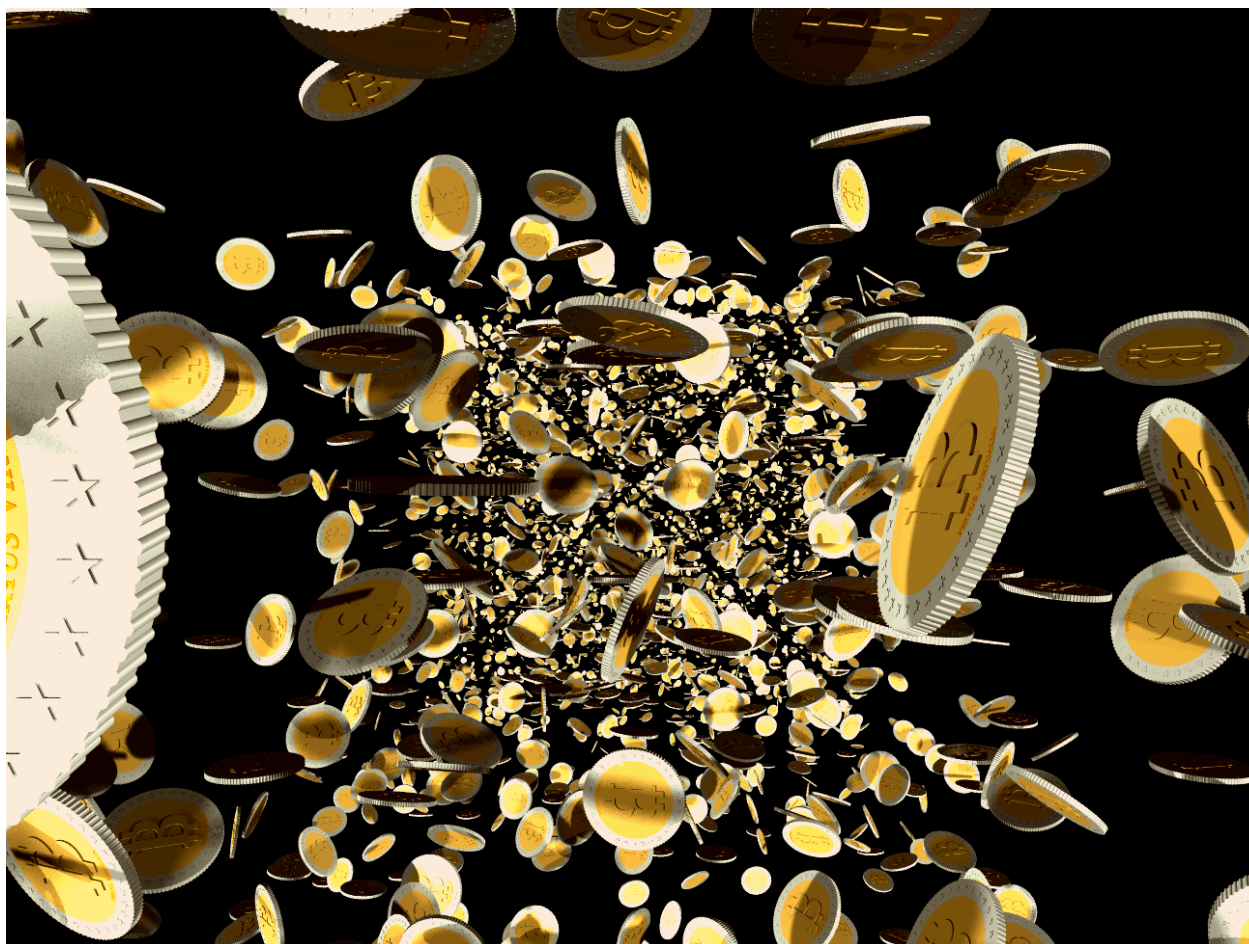
- On vérifiera facilement que les **S** prétendument trouvés sont bons, en en demandant la communication, et en calculant $h(\mathbf{S})$ qui doit être un résultat avec k '0' en tête.

La technique de la *preuve de travail* est au cœur du système des *bitcoins*.

- Elle est utilisée pour le tirage au sort de celui qui ajoute une page de compte au *cahier de compte*, et remporte toutes les dix minutes, 25 nouveaux *bitcoins*.
- Ceux qui participent se lancent dans la recherche du **S (associé à la page qu'ils veulent ajouter)**, le premier qui en trouve un est le gagnant.
- Ajustable en faisant varier l'entier *k*, les preuves de travail exigées pour emporter les 25 *bitcoins* créés toutes les 10 minutes sont devenues de plus en plus difficiles au cours des mois.
- Depuis que des puces spécialisées ont été conçues pour calculer très vite les ***h(S)*** la difficulté du travail demandé a été augmentée.

Cela de façon à ce que le temps moyen entre deux gains reste toujours de 10 minutes environ.

La fonction SHA-256 est utilisée par bitcoin.



Des avis tranchés !



Contre

- 4 décembre 2013, Georges Ugeux (Banquier d'Affaires) :

Le bitcoin est une « monnaie » de casino qui profite à des manipulateurs incontrôlés.

Lorsque le château de cartes s'effondrera, qui seront les victimes ? Ceux et celles qui, inconscients du danger, se retrouveront avec des jetons de 900 dollars et découvriront qu'ils ne valent plus rien.

- 14 décembre 2013, Olivier Pastré :

Le bitcoin, c'est Madoff, ça s'appelle une pyramide de Ponzi, et ça va se casser la gueule.

- 5 décembre 2013, Laurent Pensolle :

Le plus incroyable, quand on prend un peu de recul, c'est que les gouvernements laissent faire ce qui est de facto de la fausse monnaie.

Cela ressemble à un schéma de Ponzi, où les entrants ne créent aucune valeur.

Le système ne tient que parce que les prix montent.

La monnaie est un service public. Il revient donc à l'Etat d'en avoir la seule responsabilité, dans un cadre démocratique [...] et d'interdire toute alternative.

- 5 décembre 2013, La Banque de France (Focus n°10) :

Les bitcoins : une monnaie non régulée qui n'offre aucune garantie.

[...] Une conception qui alimente la spéculation.

[...] Des plates-formes internet proposent, sans aucune garantie de prix ni de liquidité, l'achat/vente de bitcoins contre des devises ayant cours légal.

[...] Par son caractère anonyme, le bitcoin favorise le contournement des règles relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

[...] Même si le bitcoin ne remplit pas à ce jour les conditions pour devenir un support d'investissement crédible et poser ainsi un risque significatif pour la stabilité financière, il représente un risque financier certain pour les acteurs qui le détiennent.

[...] N'offrant aucune garantie de sécurité, de convertibilité et de valeur, le bitcoin présente peu ou pas d'intérêt pour une utilisation par les acteurs économiques, au-delà des aspects marketing et publicitaire, tout en les exposant à des risques importants.

[...] En limitant la quantité maximale de bitcoins pouvant être créée et en faisant fluctuer le rythme de création au cours du temps, les concepteurs ont « organisé » la pénurie de cette monnaie virtuelle et lui ont ainsi conféré son caractère hautement spéculatif.

- 5 décembre 2013, Alan Greenspan :

I Guess bitcoin Is a Bubble.

You really have to stretch your imagination to infer what the intrinsic value of bitcoin is.

I haven't been able to do it.

But if you ask me, 'Is this a bubble in bitcoin?' 'Yeah, it's a bubble.

- 28 décembre 2013, Paul Krugman **bitcoin is evil.**

Pour



- 2008, Satoshi Nakamoto :

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.

As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.

The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

- 20 janvier 2012, Pierre Noizat :

Mais à la différence de l'or, les bitcoins peuvent être divisés indéfiniment et n'impliquent aucun frais de stockage.

Si l'économie bitcoin devait croître à hauteur de 5% du PIB des Etats-Unis (c'est-à-dire 725 milliards de dollars) et en supposant une vélocité monétaire du bitcoin égale à 50, équivalente au dollar pour les petits montants, un bitcoin représenterait l'équivalent de 700\$. Cela équivaldrait à une valeur projetée de 15 milliards de dollars pour le réseau bitcoin. C'est un ordre de grandeur cohérent avec la capitalisation boursière de Visa, Inc. (55 milliards de dollars) ou de MasterCard (39 milliards de dollars).

Acheter des bitcoins aujourd'hui, c'est acheter des actions pour un nouveau réseau mondial de transactions électroniques.

Dans une transaction électronique en ligne, le prix exprimé en devise universelle peut facilement être ajusté en temps réel par rapport à un taux de change variable. C'est uniquement pour les transactions qui ne sont pas en ligne que la stabilité des prix est une exigence pour toute devise universelle.

La déflation des prix augmente l'attractivité des bitcoins en tant que valeur refuge et n'affecte que marginalement son application en que moyen d'échange.

Dans une économie mondialisée, la naissance d'une ou de plusieurs devises universelles est inéluctable dès lors qu'elle est technologiquement faisable et économiquement souhaitable.

bitcoin peut fortement améliorer l'efficacité des transferts d'argent là où il y en a le plus besoin, notamment pour l'aide au développement.

Bitcoin peut profiter de la généralisation des téléphones mobiles dans les pays en voie de développement pour permettre de transférer de l'argent directement, sans passer par des intermédiaires, qu'ils soient bureaucratiques ou bancaires.

Cette technologie permet à la fois un nouveau type de transaction sur le réseau et une nouvelle devise universelle.

Il est permis d'espérer qu'une organisation similaire (à celle d'internet) puisse également superviser les caractéristiques techniques du protocole bitcoin.

Cela permettrait à bitcoin de préserver son intégrité et son potentiel d'innovation face aux aléas des mesures macro-économiques.

- 13 décembre 2013, Simon Phipps :

The Internet is creating a society where each of us can play the roles previously reserved for corporations without needing an intermediary.

We can start businesses, trade goods, conduct relationships, publish, editorialize, and conduct politics, all without needing an intermediary to empower us.

A currency we can use as we engage in those activities is a natural complement and vehicle.

As the meshed society matures, our need for digital money is inevitable.

- 16 décembre 2013, Cameron Winklevoss :

A scenario for bitcoin is a 400 billion USD dollar market cap,
so **40,000 USD a coin**, but I believe it could be much larger.

It will probably happen much faster than anyone imagines.

- 18 décembre 2013, Steve Kirsch :

Buy bitcoins now.

Take 5 percent of your net worth, and put it into bitcoin. [...]

You won't be sorry.

I think for the next few years, any time you buy bitcoins and hold onto them, and then sell it, you'll make substantial amounts of money.

You'll be so happy.”

- 22 décembre 2013, Gannon LeBlanc :

With more people taking interest in this fascinating real-world economic experiment, we are going to see bitcoin enter the everyday consumer's life.

We're also seeing bitcoin coincide with a generation more mobile than ever.

Millennials can use bitcoins in any country, without having to convert their currency.

There is no need to find a currency exchange building, no need to worry about conversion rates, no need to worry about a lot of the problems with government-issued currency.

bitcoin also connects young people in disparate countries with each other so they can pay each other easily for services like software development and intellectual property.

It connects businesses directly with customers in a more direct way than any “middlemen” like PayPal or a credit card companies.

It’s economic freedom unlike anything seen before.

bitcoins can be an investment, a medium of exchange, and much more.

It’s also a challenge to the status quo and proof that the free market can produce a private currency that works.

bitcoin is loved and embraced by young bright individuals who see the potential future that bitcoin and what it represents and can be.

