Lille, SSAAL : 14 décembre 2018

Les blockchains : où en sommes-nous ?

Jean-Paul Delahaye,
CRISTAL : Centre de recherche en informatique, signal et automatique de Lille,
UMR 9189 **CNRS**

https://www.investopedia.com/terms/b/bitcoin.asp

Aug. 18, 2008: The domain name bitcoin.org is registered.

Oct. 31, 2008: Satoshi Nakamoto on The Cryptography Mailing list at metzdowd.com:

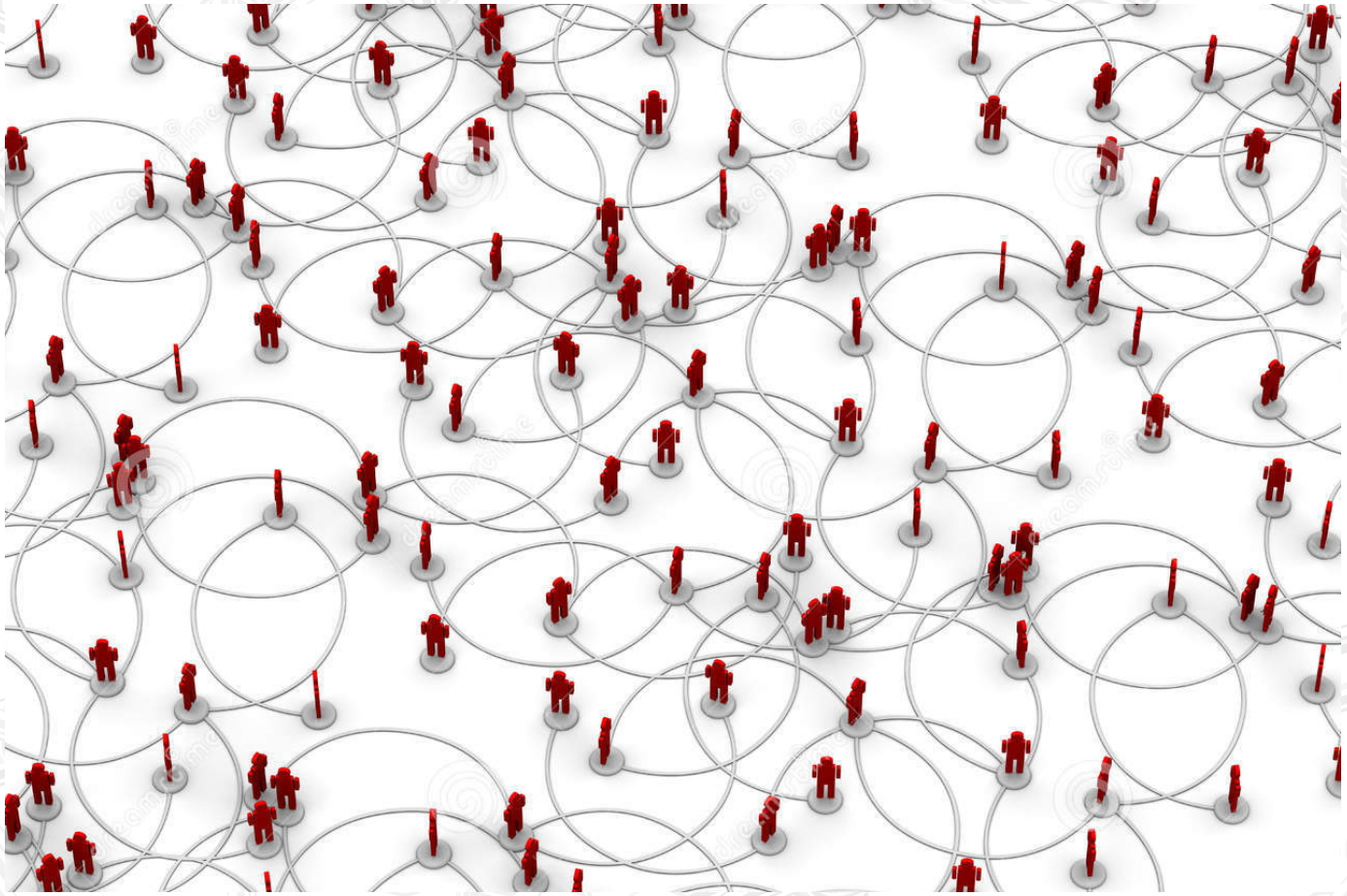
"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. The paper is available at http://www.bitcoin.org/bitcoin.pdf."

"Bitcoin: A Peer-to-Peer Electronic Cash System."

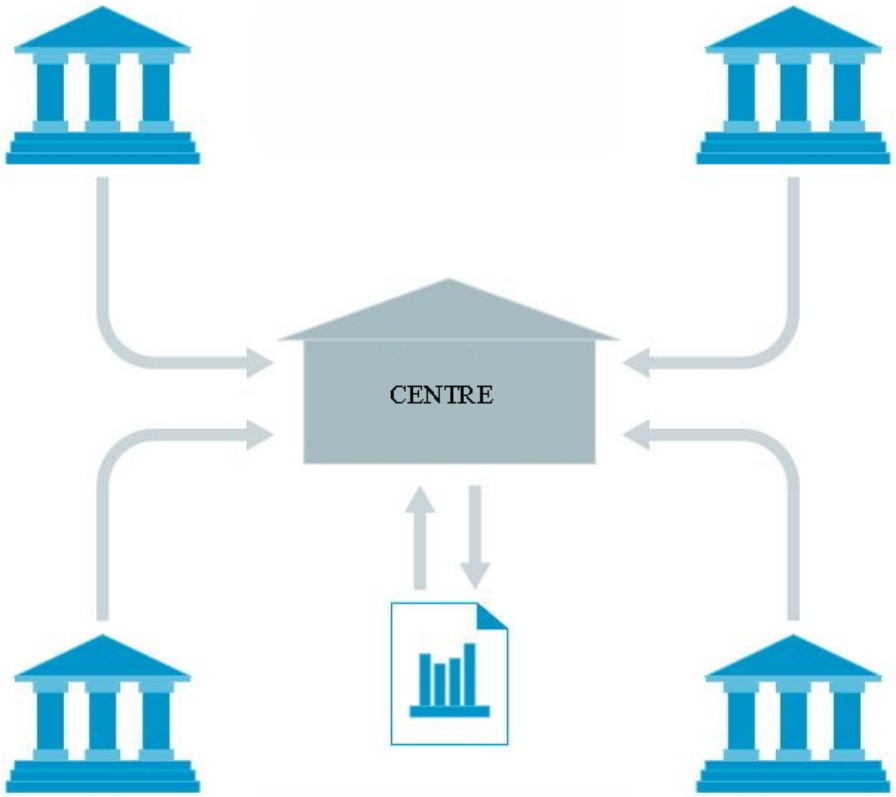
Blockchain : un fichier ouvert à tous, inneffaçable.

Chaque page est datée. Elles sont liées entre elles, en une longue chaîne indestructible.

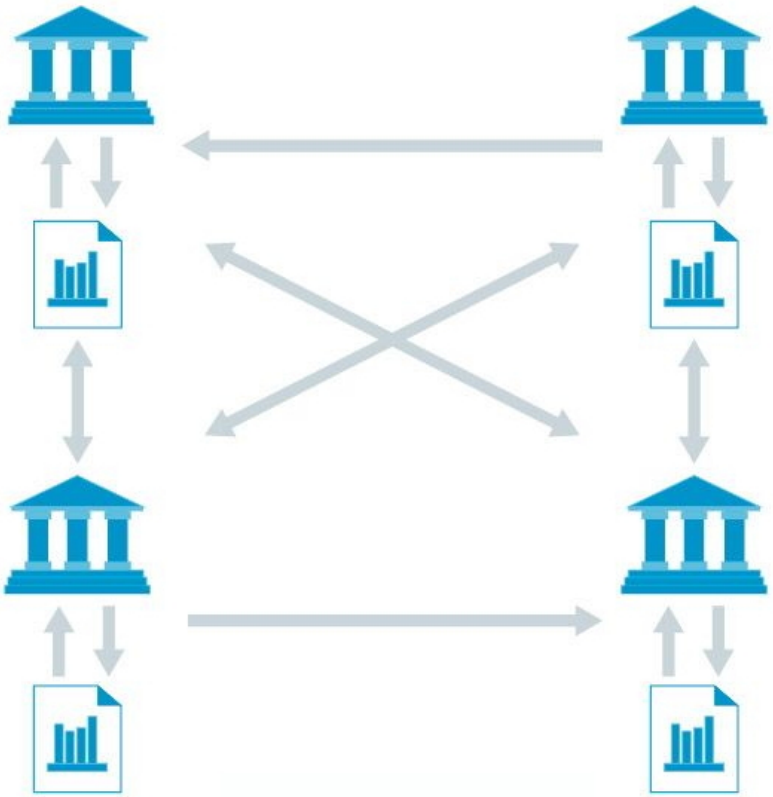
Une copie en chaque nœud d'un réseau pair-à-pair



Moyen pour partager une vérité.



Centralisé

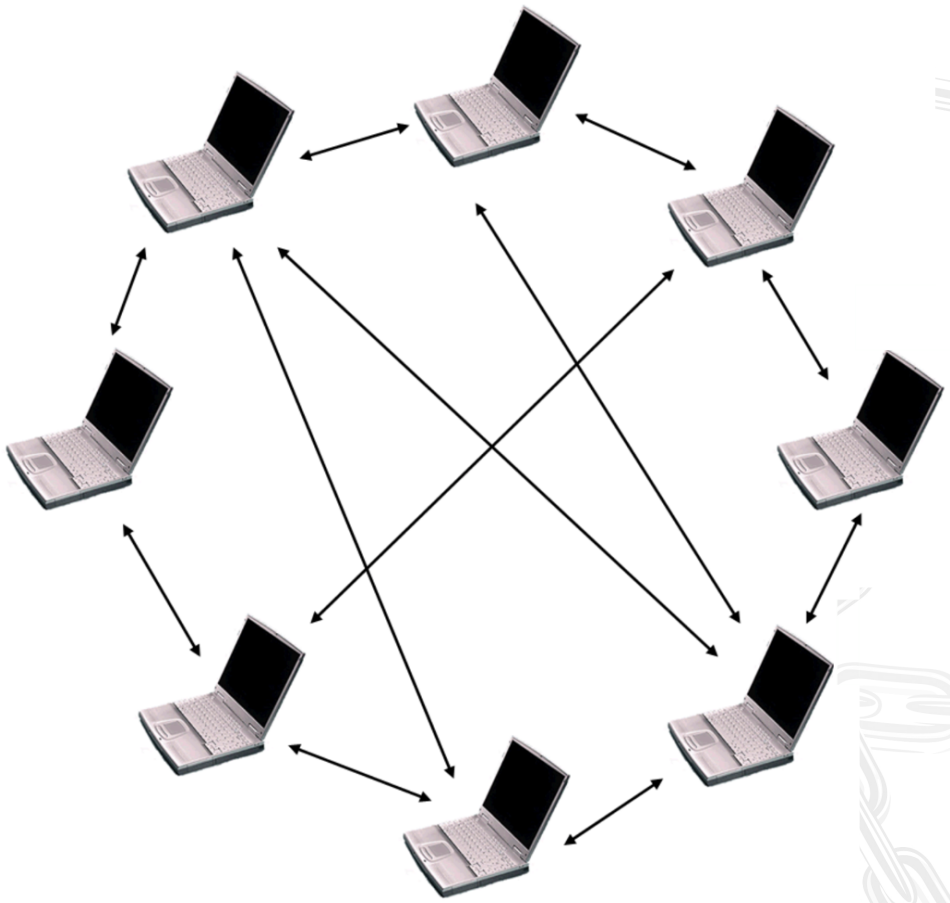


non centralisé (P2P)

Pas de tiers de confiance.
La sécurité est assurée par la cryptographie

Sécurité assurée aussi car chaque nœud contrôle chaque opération.

Consensus. Confiance.



Technologie blockchain.

Blockchain : le fichier
Blockchain : le réseau
Blockchain : le protocole

Décentralisée, partagée, sécurisée.

Définition d'une blockchain :

Registre (= fichier)

partagé (= multiplié sur un réseau P2P)

infalsifiable (= protégé par des primitives cryptographiques)

indestructible (presque... car multiplié)

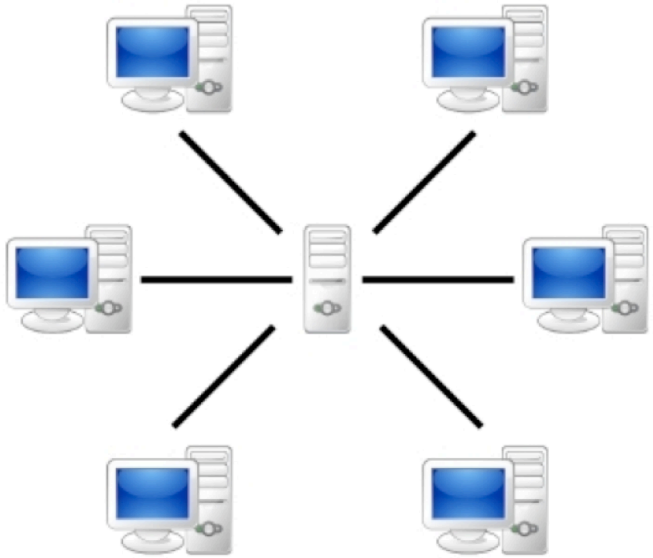
composé de "blocs" (ou pages) successivement validés, datés et conservés par ordre chronologique.

Variantes :

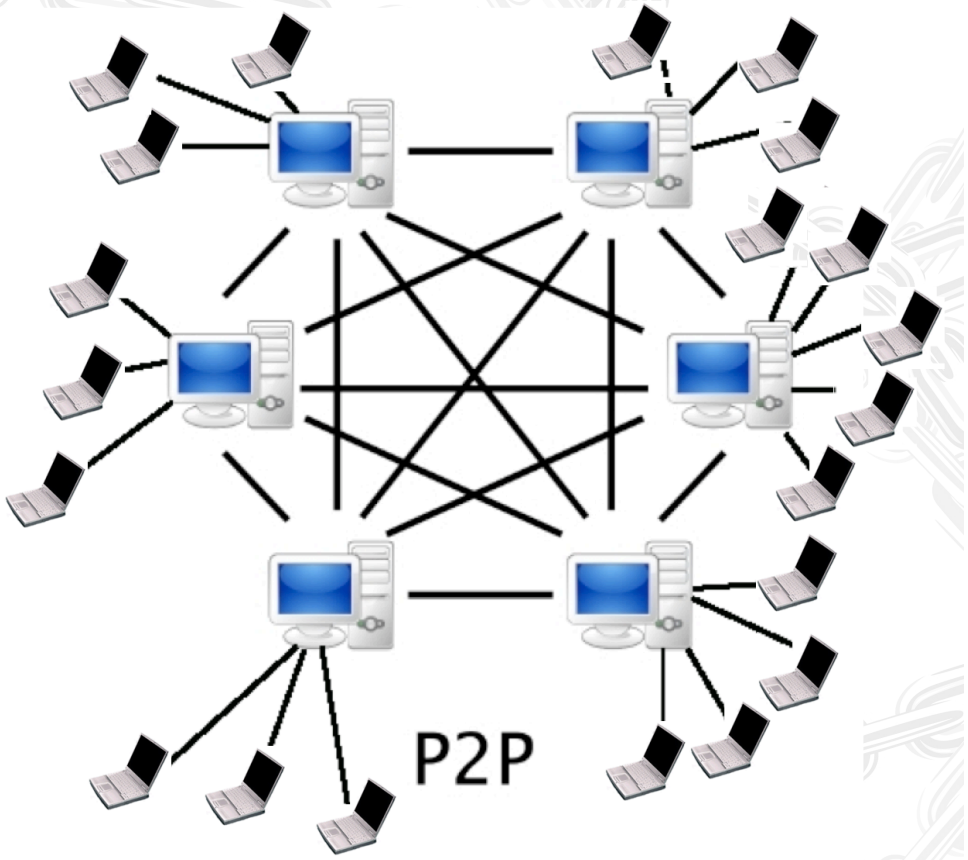
Fichier : *ouvert en écriture, ouvert en lecture ou semi-ouvert.*

Réseau : *ouvert ou "permissionned".*

Identité des utilisateurs : *masquée ou déclarée.*



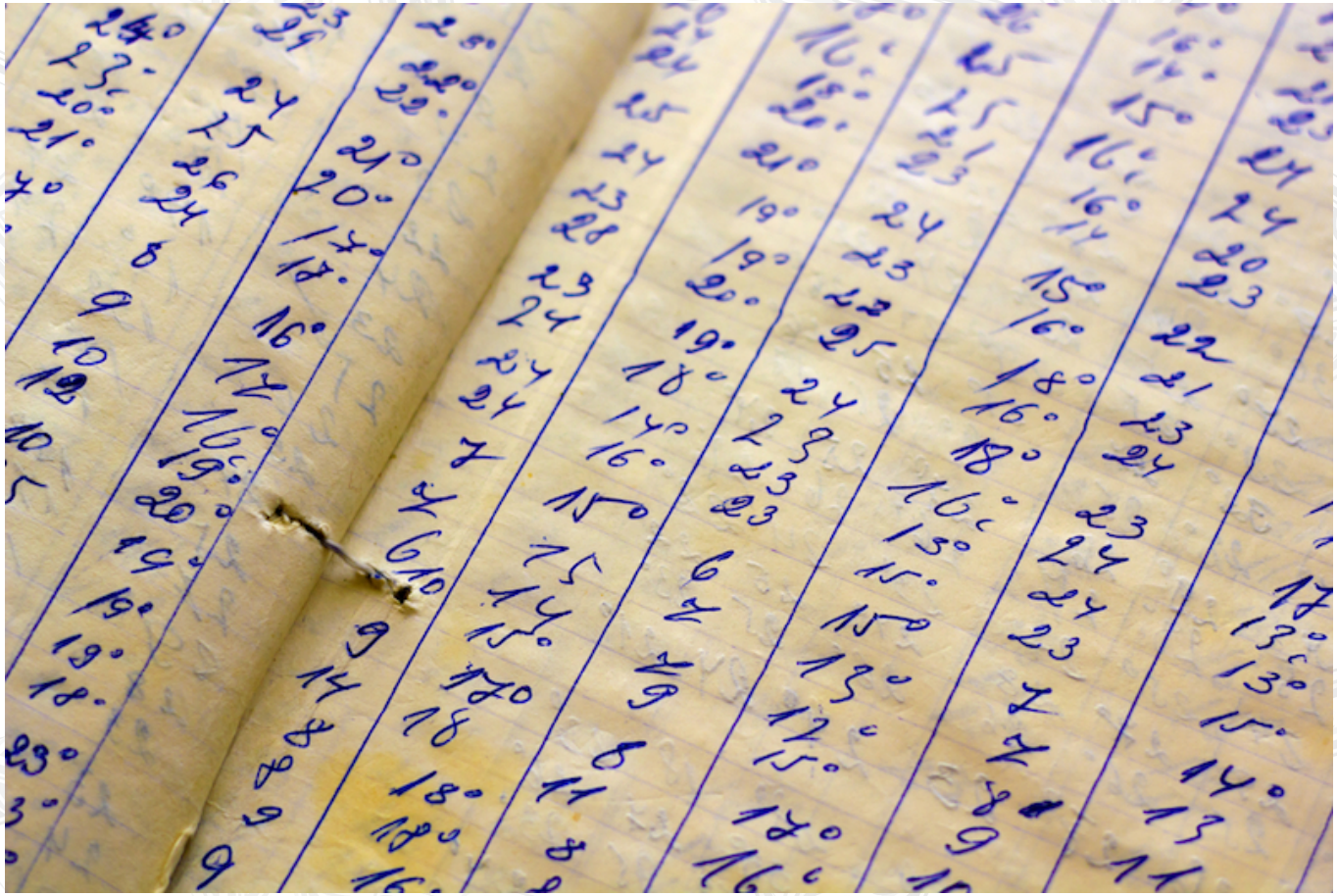
Centralisé



Les **monnaies cryptographiques** sont un cas particulier.

Plus de 2000 en décembre 2018.

Blockchain : cahier de compte



Bitcoin : naissance du réseau 3 janvier 2009, 18h15

Satoshi Nakamoto

Latest Blocks

Height	Age	Transactions	Mined by	Size
484628	21 minutes ago	333		852064
484627	23 minutes ago	2074		994427
484626	26 minutes ago	2225		981480
484625	an hour ago	442	SlushPool	213859
484624	an hour ago	1455		970991

See all blocks

Latest Transactions

Hash	Value Out
223863b68d8c3f663a9490cf50a47f521ab7a52c86885…	0.232767 BTC
501b75256754c4ed07c6e081d73aa2a1f79c1e1b0332…	367.8311466 BTC
9333eae828cf7bcc5ea65a5a69b547a1620cd674226b…	8.23786164 BTC
e22cd7d273c2b1712b25697306d14f9a319e55f85ef4f…	8.24215848 BTC
c8cb46f688703a2fd16ba5f1bad5ff46ca0ef2cc233d7f…	8.2539891 BTC

About Block Explorer

Bitcoin Block Explorer is an open source web tool that allows you to view information about blocks, addresses, and transactions on the Bitcoin blockchain. The source code is on GitHub.

What is bitcoin?

Public Bitcoin API: Machine readable stats & blockchain info can be accessed directly through the REST and Websockets APIs.

Testnet is Bitcoin's sandbox. Block Explorer supports viewing both the testnet and mainnet blockchains.

Thanks to Private Internet Access for hosting the site. They provide a VPN Service that accepts Bitcoin.

Le bitcoin depuis le premier exposé x 7,8 :

19-9-2014 : 424 $ ---> 14-12-2018 : 3318 $

Cryptocurrencies: 2068 · Markets: 15681 · Market Cap: $122 609 720 146 · 24h Vol: $15 274 005 850 · BTC Dominance: 54.7%

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$67 044 073 458	$3 851,05	$5 599 360 791	17 409 287 BTC
2	XRP	$13 658 722 039	$0,338696	$439 853 821	40 327 341 704 XRP *
3	Ethereum	$10 674 892 222	$103,01	$2 146 909 008	103 629 592 ETH
4	Stellar	$2 630 641 771	$0,137264	$76 073 759	19 164 799 206 XLM *
5	Bitcoin Cash	$2 167 833 118	$123,91	$110 153 237	17 495 213 BCH
6	EOS	$1 985 349 625	$2,19	$879 446 087	906 245 118 EOS *
7	Tether	$1 853 198 722	$0,998264	$3 366 014 740	1 856 421 736 USDT *

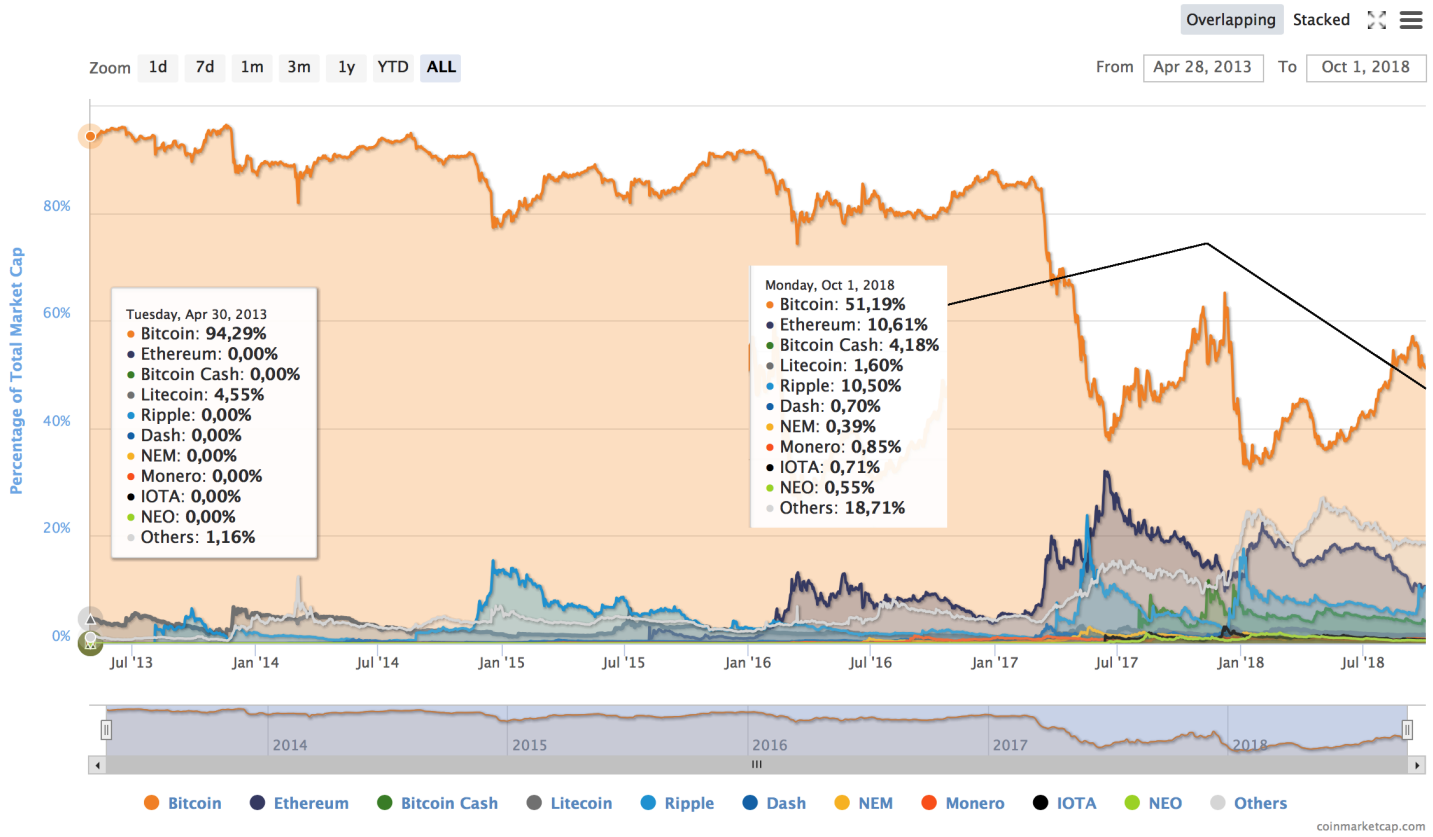
Le 6 décembre 2018

#	Name	Market Cap	Price
1	Bitcoin	$67 044 073 458	$3 851,05
2	XRP	$13 658 722 039	$0,338696
3	Ethereum	$10 674 892 222	$103,01
4	Stellar	$2 630 641 771	$0,137264
5	Bitcoin Cash	$2 167 833 118	$123,91
6	EOS	$1 985 349 625	$2,19
7	Tether	$1 853 198 722	$0,998264

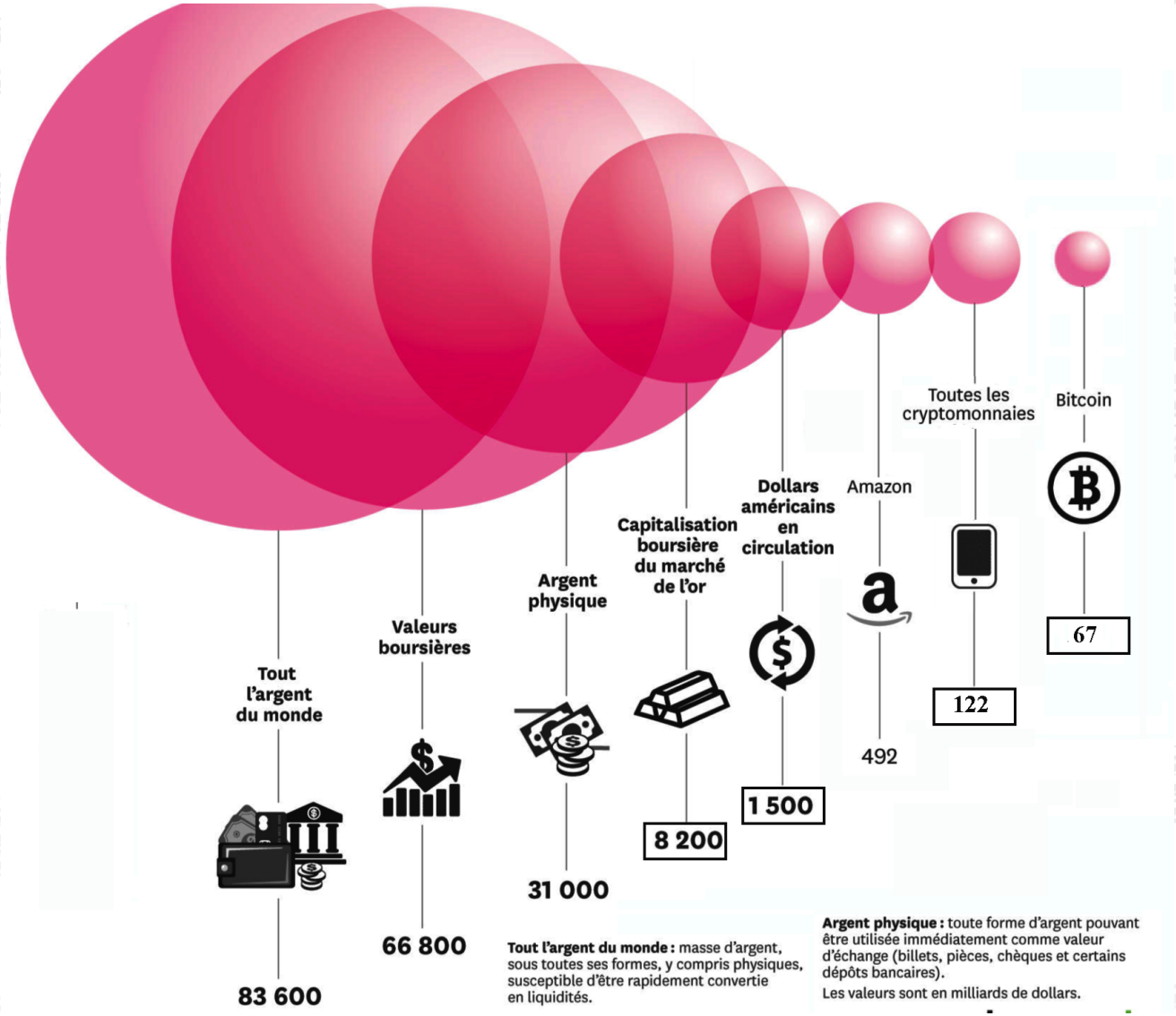
#	Name	Market Cap	Price
8	Litecoin	$1 770 134 448	$29,77
9	Bitcoin SV	$1 587 394 537	$90,82
10	TRON	$949 411 088	$0,014353
11	Cardano	$908 175 433	$0,035028
12	Monero	$872 265 331	$52,47
13	Binance Coin	$773 833 364	$5,92
14	IOTA	$733 898 792	$0,264037

6 décembre 2018 : 67 milliards de dollars en bitcoins en circulation
122 milliards de dollars en monnaies cryptographiques diverses

Le bitcoin 19-9-2014 : 424 $ ---> 14-12-2018 : 3318 $



Importance relative du Bitcoin de 94% en 2013 à 54% en décembre 2018


Tout l'argent du monde
83 600
Valeurs boursières
66 800
Argent physique
31 000
Capitalisation boursière du marché de l'or
8 200
Dollars américains en circulation
1 500
Amazon
492
Toutes les cryptomonnaies
122
Bitcoin
67
Tout l'argent du monde : masse d'argent, sous toutes ses formes, y compris physiques, susceptible d'être rapidement convertie en liquidités.
Argent physique : toute forme d'argent pouvant être utilisée immédiatement comme valeur d'échange (billets, pièces, chèques et certains dépôts bancaires).
Les valeurs sont en milliards de dollars.

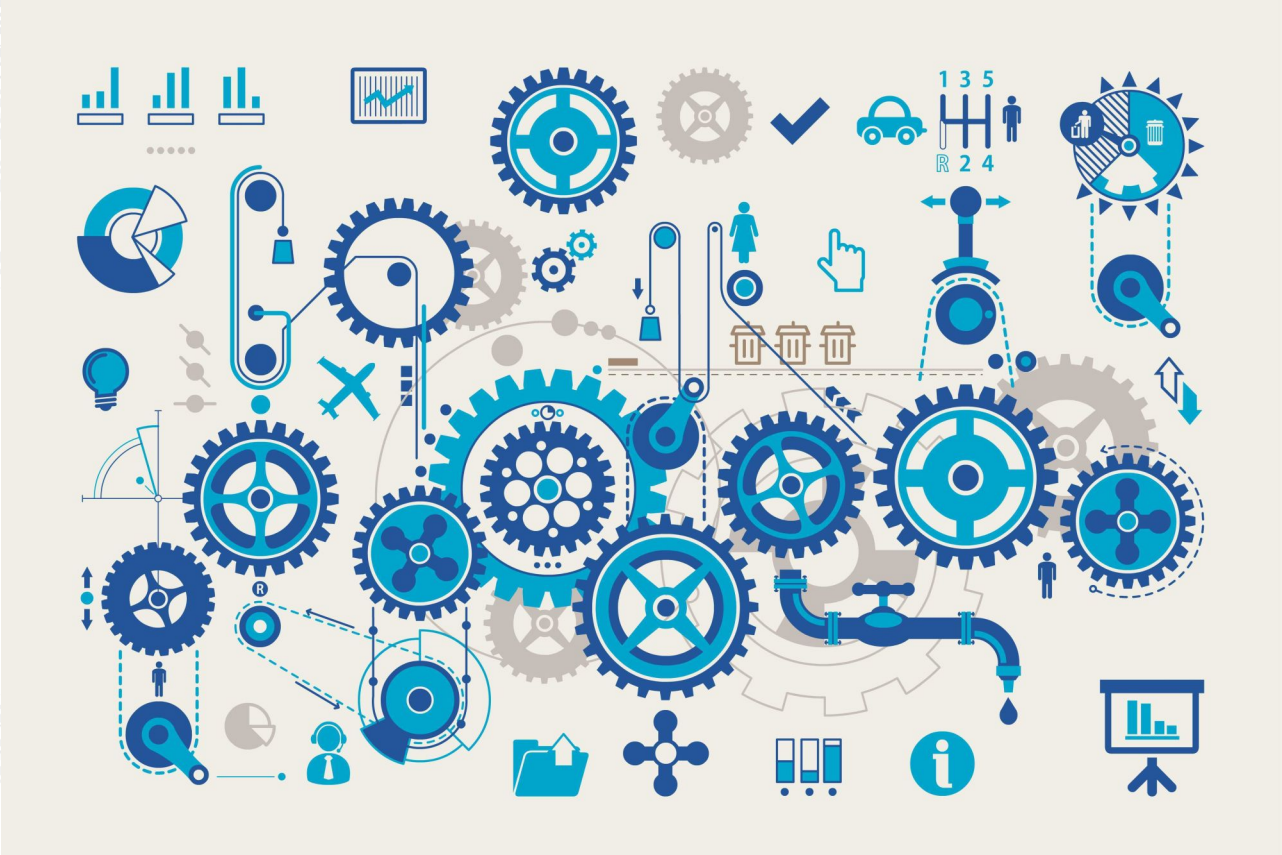
Le bitcoin est un argent **programmable** :

On peut décider qu'une transaction se déroulera le 1 janvier 2020 et qu'elle ne sera valable que si 2 signataires parmi 3 signent, etc.

Cet aspect est révolutionnaire.

Mauvaise réputation ? C'est injustifié.

Depuis presque 10 ans, le protocole Bitcoin fonctionne bien



L'internet a permis la **circulation de l'information de pair à pair**

Les blockchains permettent la **circulation de valeurs de pair à pair**

Cet aspect est révolutionnaire.

Dans le cas du ***Bitcoin*** **:**

blockchain **= liste complète de toutes les transactions**

- Comptes anonymes.
- 21 millions de *bitcoins* en tout.
- Le bicoin est divisible en 100 000 000-ième
- 12,5 nouveaux *bitcoins* toutes les 10 minutes. Division par 2, tous les 4 ans.
- En 2140 plus d'émission.

- **Fonction de hachage** (SHA256) (on parle de hash, d'empreinte, etc.)
- **Signature à double clé** (*Elliptic Curve Digital Signature Algorithm*, ECDSA)
- **Incitation** à surveiller la *blockchain* : "mining" (minage)
- **Preuve de travail** (pour l'attribution des nouveaux ***bitcoins*** créés)

?

Pourquoi en 2009 ?

(a) La puissance de calcul et de mémorisation donnée à tous par les progrès des technologies de l'information (loi de Moore),

(b) la cryptographie mathématique moderne,

(c) la technologie des réseaux pair-à-pair

ont permis de réaliser un partage massif d'informations, collectivement validées, protégées et sans autorité centrale.

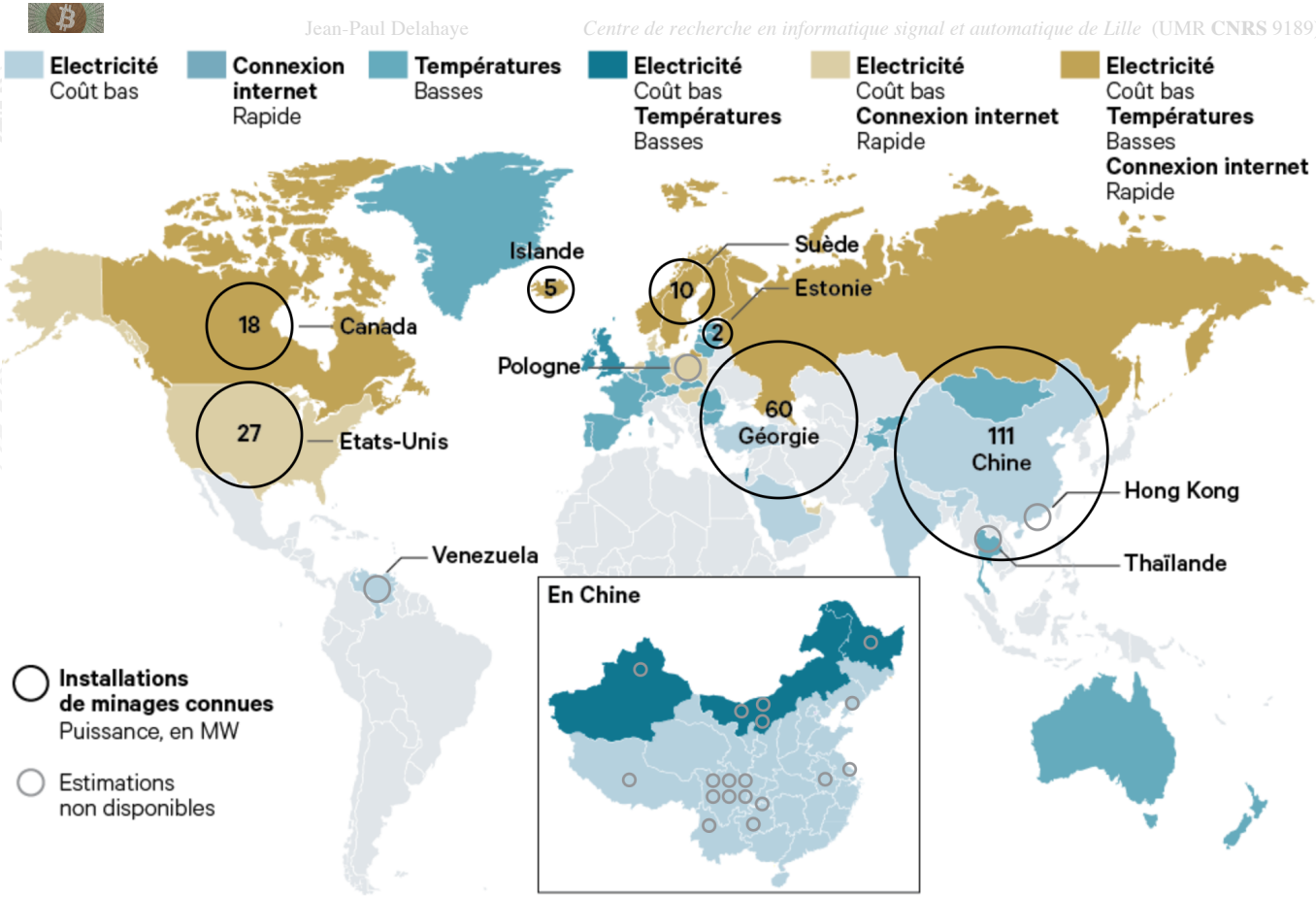
Le problème de l'énergie

La dépense électrique provient des ***preuves de travail*** :

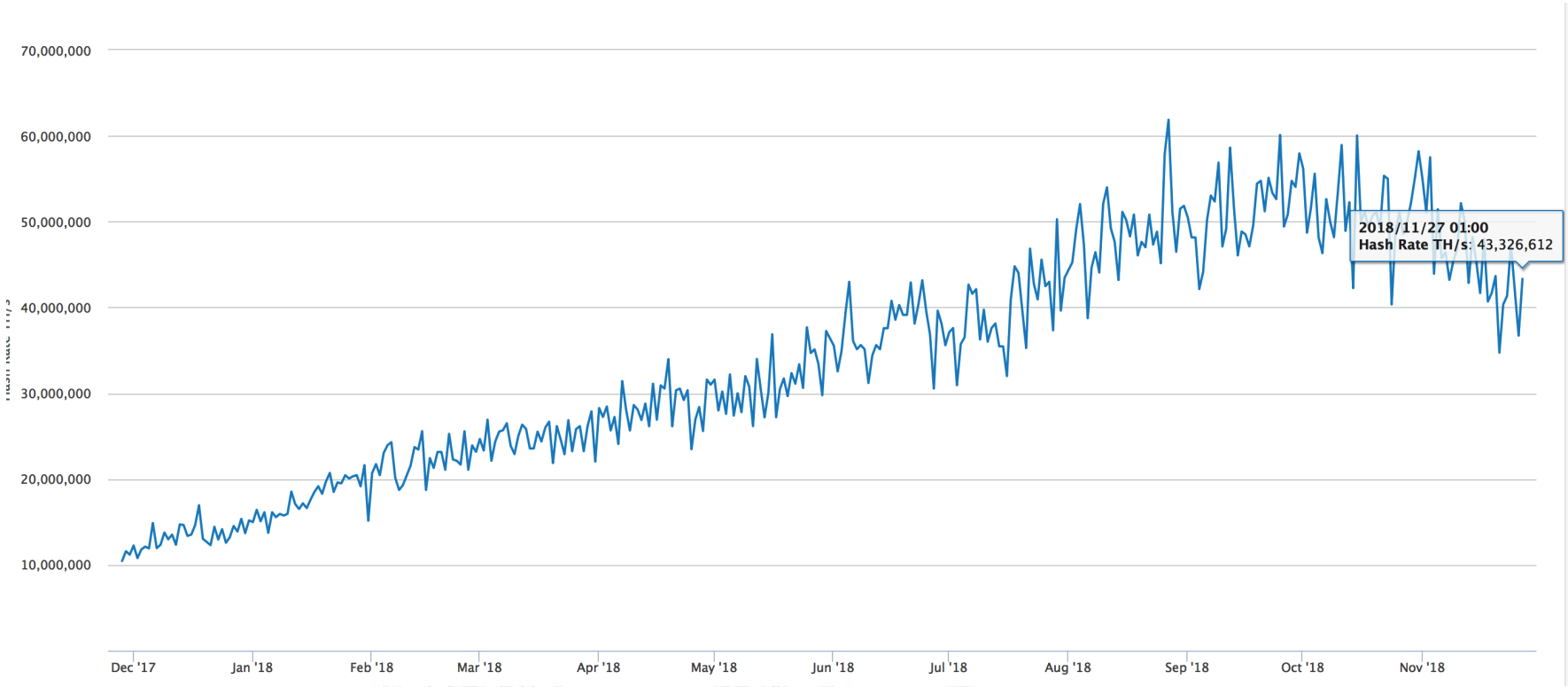
- **incitation** (distribution de nouveaux bitcoins)
- **attribution** par concours

Plus on dispose de capacités à calculer le SHA256, plus on a de chances de gagner les nouveaux bitcoins émis.
Course folle à la puissance.
Rend plus difficile les attaques de type 51%,
mais pas toutes les attaques.

Solutions : preuves d'enjeu, blockchains à validateurs identifiés.



La Chine détient 60 % (environ) de la puissance de minage.



De 7_x10^{18} (1 octobre 2017) à 43_x10^{18} (28 novembre 2018)

Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	52.41
Bitcoin's current minimum annual electricity consumption** (TWh)	46.16
Annualized global mining revenues	$2,621,408,311
Annualized estimated global mining costs	$2,620,421,076
Country closest to Bitcoin in terms of electricity consumption	Romania
Estimated electricity used over the previous day (KWh)	143,584,716
Total Network Hashrate in PH/s (1,000,000 GH/s)	45,642
Number of U.S. households that could be powered by Bitcoin	4,852,632
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.23%

BITMAIN

Newest Model

ANT**MINER** S9 + APW3++ Power Supply

Minorant de la dépense électrique du minage du bitcoin 1-10-2018

Un des outils de minage le plus efficace (énergétiquement)

• **Antminer S9** https://www.bitcoinmining.com/bitcoin-mining-hardware/

Advertised Capacity: 13.5 Th/s **Power Efficiency:** 0.098 W/Gh

Fait de 189 Bitmain's BM1387 chip Prix Amazon **800 dollars**

Il produit **13,5 10^12** hash par s. Consommation électrique 13,5*98 W = 1323 W

(ce qui est beaucoup comparé à un ordinateur qui dépense de 100 à 200 W)

La puissance du réseau le 1-10-2018 est de **58*10^18** hash par seconde

Si tout le minage était fait avec Antminer S9, il faudrait (58*10^18)/(13,5*10^12) =

4 300 000 appareils

Ils coûteraient donc plus de 3 000 000 000 de dollars.

La consommation de ces appareils serait de 4300000*1323 W = 5 700 000 000 W

Annuellement = 49,9 10^12 Wh = **49,9 TWh environ 6 centrales nucléaires**

Digiconomist pour le minimum le 1-10-2018 = **59 TWh (et 73 TWh évaluation)**

Autres chiffres : **Google : 6 TWh** **Toutes les télés en France : 3 TWh**

Pour égaliser l'or (x60) entre 2000 et 4000 TWh (par la méthode du calcul gain=dépense)

Le problème du nombre de transactions

Trop peu de transactions peuvent passser : 6 par seconde pour Bitcoin

Concerne aussi les blockchains sans cryptomonnaie.

Solutions : augmentation de la taille des pages (Bitcoin cash),
Couche au-dessus du réseau de base (Lightning network)
Blockchain à validateurs identifiés et limités (Ripple)
Autres modèles (IOTA)

Christine Lagarde

(septembre 2017, dans une conférence organisée par la *Banque d'Angleterre*)

Les monnaies virtuelles [...] produisent leur propre unité de compte et leur propre système de paiement.

Ces systèmes permettent des transactions de pair à pair, sans chambre de compensation, sans banque centrale.

À l'heure actuelle les monnaies virtuelles comme Bitcoin ne représentent pas encore de menace pour l'ordre existant des monnaies fiduciaires et des banques centrales.

Christine Lagarde

Pourquoi ? *: parce qu'elles sont trop volatiles, trop risquées, trop énergivores, parce que les technologies sous-jacentes ne sont pas suffisamment scalables, que beaucoup d'entres elles sont trop opaques pour les régulateurs et que certaines ont été piratées.*

Mais beaucoup de ces défauts ne sont que des défis technologiques qui pourraient être surmontés avec le temps.

Christine Lagarde

(*13 mars 2018, article du FMI*)

Que la valeur de Bitcoin augmente ou qu'elle diminue, tout le monde se pose la même question : quel est exactement le potentiel des ***crypto-actifs*** *?*

La technologie derrière ces actifs, y compris blockchain, constitue une avancée passionnante qui pourrait aider à révolutionner d'autres domaines que la finance. [...]

Il ne serait pas judicieux de rejeter les ***crypto-actifs*** [...]

Nous pouvons exploiter le potentiel des crypto-actifs tout en veillant à ce qu'ils ne deviennent jamais un refuge pour les activités illégales ou une source de vulnérabilité financière.

Rapport du FMI , 6 juin 2018

Nous ne pouvons exclure la possibilité que certains crypto-actifs soient largement adoptés et remplissent mieux les fonctions de monnaie dans certaines régions ou dans des réseaux d'e-commerce.

Un tel changement aurait pour conséquence une modification de la façon dont l'argent est créé à l'ère numérique *:*

de l'argent du crédit [dette] à l'argent des marchandises [...]

En tant que moyen d'échange, les actifs cryptographiques ont certains avantages.

Robert Ophèle, président *Autorité des marchés financiers* 7 juin 2018

L'essor des crypto-actifs est probablement irrépressible car il traduit des questions légitimes.

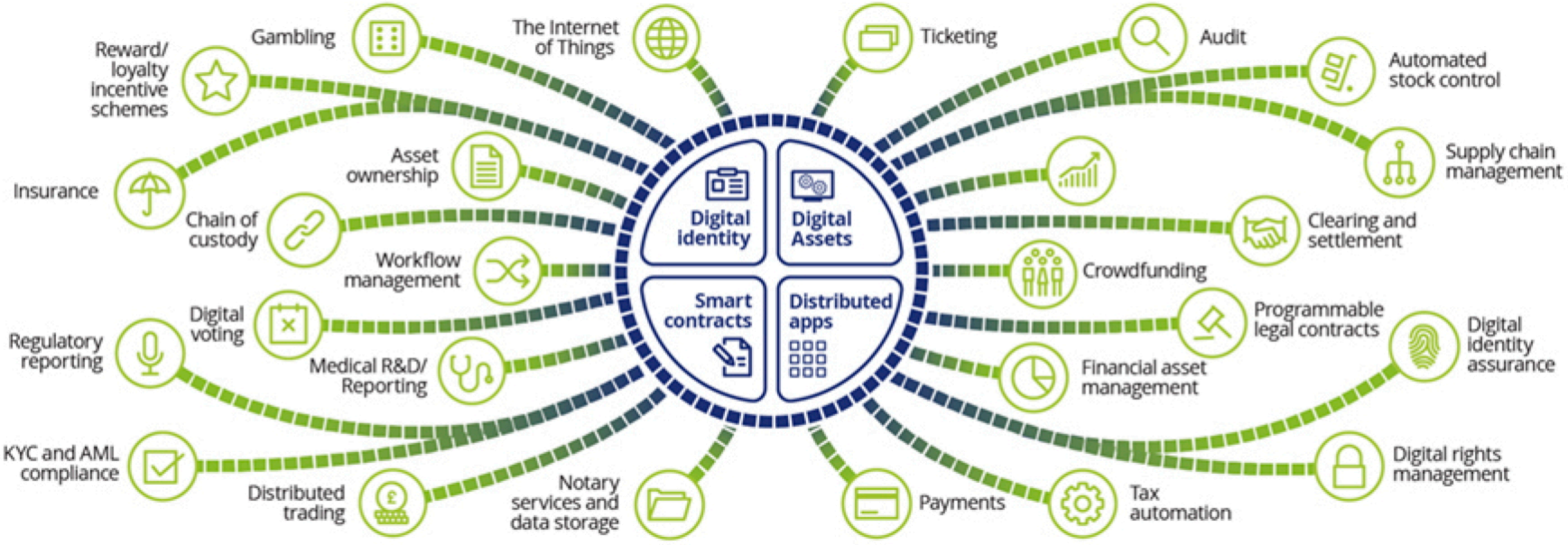
Certes cet essor s'accompagne de dangers.

Mais ces risques traités, les crypto-actifs correspondent à une réponse efficace à des questionnements légitimes et interpellent la finance intermédiée traditionnelle souvent trop lente, trop coûteuse et qui finance mal l'économie.

L'AMF, pour qui le statu quo n'est pas une option, préconise

une approche d'encadrement.

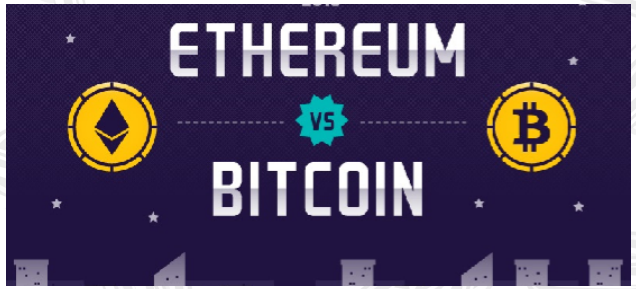
Blockchains privées, semi-privées, de consortium.



Domaines concernés :

- Echanges de titres,
- Horodatages, preuves d'existence (INPI)
- Assurance,
- Suivi d'objets (objets d'art, diamants, etc.)
- Votes,
- "Supply chain" (chaînes logistiques)
- Partage sécurisé d'informations,
- Cadastres, contrats, actions, etc.
- l'internet des objets (iot) - etc.

Smart-contracts = programmes sur une blockchain



EOS etc.

- Garantie de l'exécution (qui se fait en chaque nœud du réseau).

- L'organisateur d'une loterie, de jeux, de paris ou l'organisateurs ne peut pas arrêter le programme.

- Transparence et sureté.

- ICO (initial coin offering) (levée de fonds pour les start up)

Cet aspect est révolutionnaire.

Bruno Le Maire 1 octobre 2018

https://bitcoin.fr/bruno-le-maire-le-projet-de-loi-de-finances-prevoit-un-regime-fiscal-particulierement-favorable-a-la-blockchain/

« Notre objectif est clair :

la France doit être le leader européen de la blockchain [...].

« Le ministre de l'économie et des finances qui est totalement engagé en faveur des nouvelles technologies financières. Il est convaincu quela France peut et va être à la pointe et qu'elle sera un modèle pour beaucoup de pays européens. »

CONCLUSION

Réellement une révolution.

- Dans le domaine monétaire (crypto-actifs).

- Plus généralement pour l'échange d'objets ayant de la valeur :

la blockchain c'est l'internet de la valeur

- Plus généralement encore :

partage d'informations infalsifiables et sécurisées.


digital
network
exchange
cryptocurrency
business
market
money
finance
smart
ledger
technology
data
exchange
business
Blockchain
concept
litecoin
finance
digital
money
bitcoin
currency
technology
money
exchange
network
contract
finance
transaction
virtual
digital
protocol
bitcoin
node
digital
data
cash
ledger
data
node
virtual
cryptocurrency
finance
financial
cash
business
virtual
exchange
coin
electronic
currency
payments
business
data
coin
crypto
node
currency
litecoin
internet
virtual
bitcoin
financial
smart
ledger
coin
currency
internet
network
smart
contract
transaction
business
exchange
cryptocurrency
protocol
market
bitcoin
bitcoin
data
concept
payments
technology
internet
digital
data
node
cash
business
cryptography
cryptocurrency
protocol
Blockchain
internet
crypto
litecoin
cash
cash
electronic
money
coin
smart
crypto
contract
smart
ledger
cash
litecoin
ledger
coin
market
payments
currency
crypto
node
transaction
financial
litecoin
bitcoin
money
market
concept
technology
virtual
financial
virtual
digital
crypto
concept
technology
technology
finance
market
market
coin
coin
finance
contract
bitcoin
transaction
internet
financial
business
money
concept
transaction
electronic
concept
digital
contract
protocol
money
electronic
Blockchain
protocol
internet
currency
electronic
payments
cryptography
litecoin
node
Blockchain
financial
transaction
transaction
network
cryptocurrency
virtual
ledger
electronic
currency
exchange