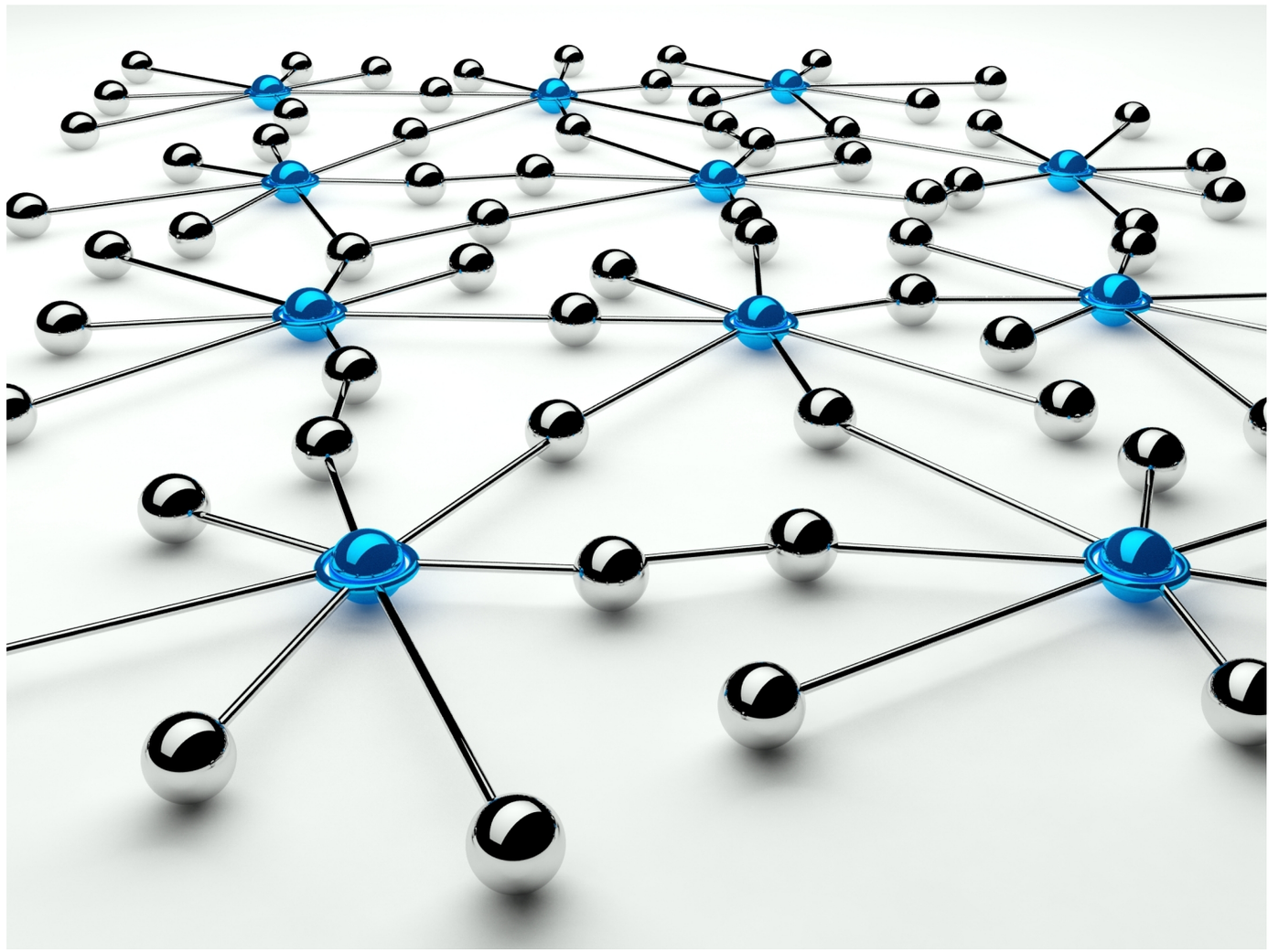


13e rencontre de l'Arcsi : BNF

La confiance dans notre monde numérique peut-elle renaître ?

Les blockchains : outils pour une meilleure confiance ou pour de nouvelles fraudes et des dangers aggravés !

26 novembre 2019

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

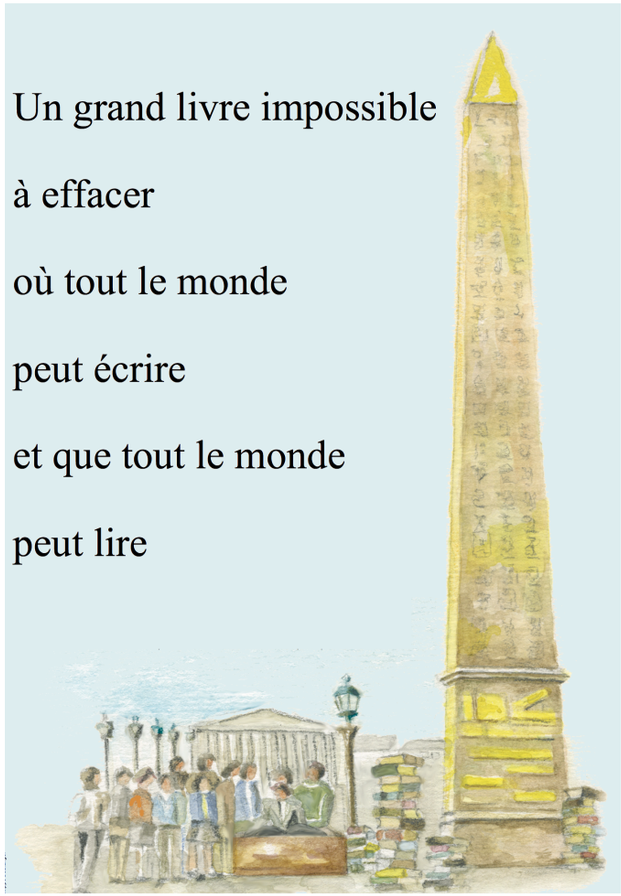
• 31 octobre 2008

Satoshi Nakamoto dépose « ***Bitcoin: A Peer-to-Peer Electronic Cash System***. »

• 3 janvier 2009

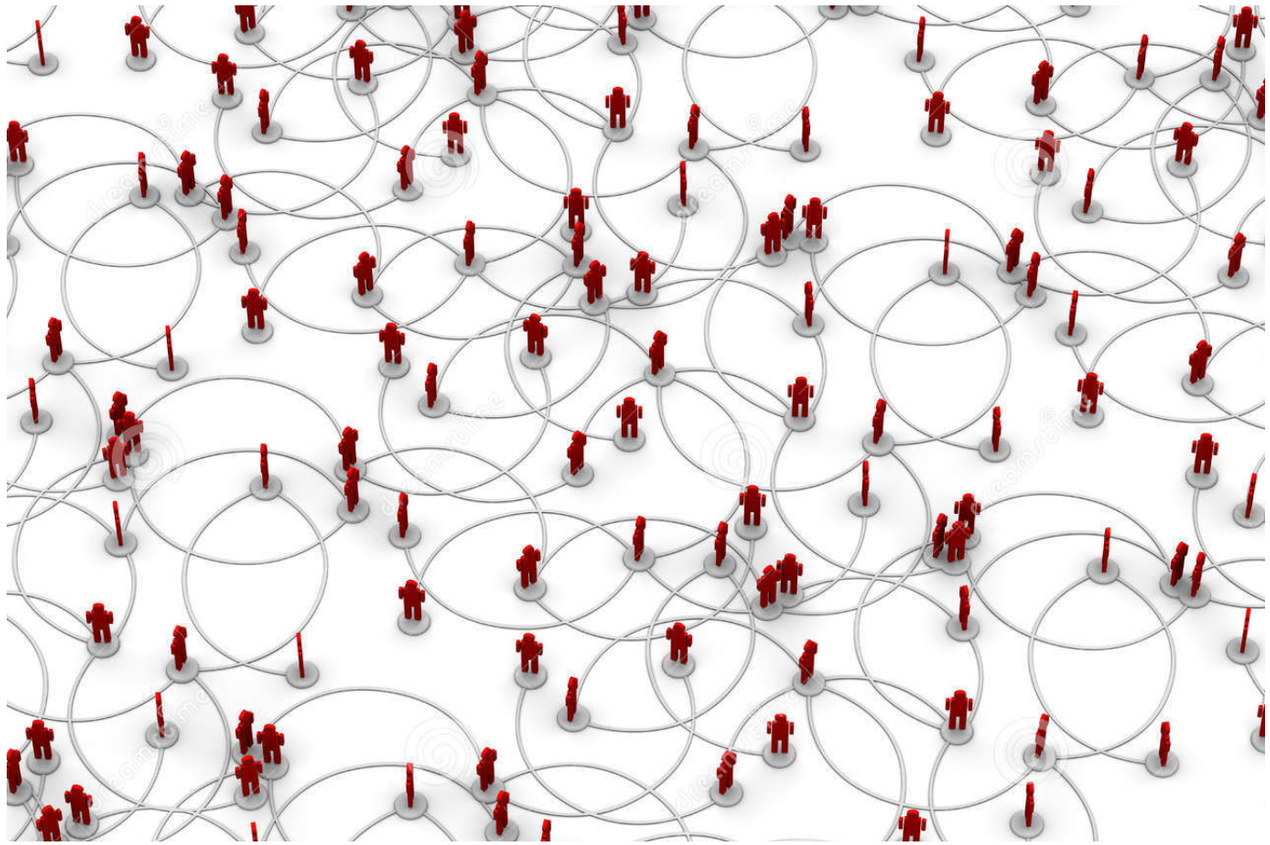
Mise en fonctionnement du réseau ; création des premiers Bitcoin

Créateur Bitcoin : Satoshi Nakamoto



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

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



Moyen pour **partager et s'accorder** sur des informations.

Pas de tiers de confiance.

La sécurité est assurée par la cryptographie

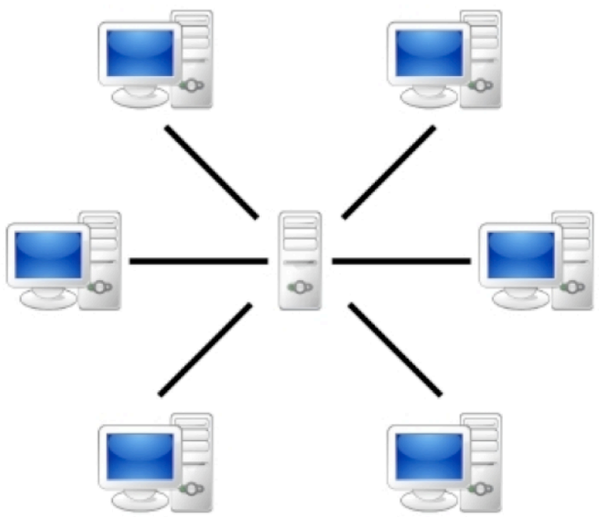
Sécurité assurée aussi car chaque nœud contrôle chaque opération et chaque page.

Consensus. Confiance.

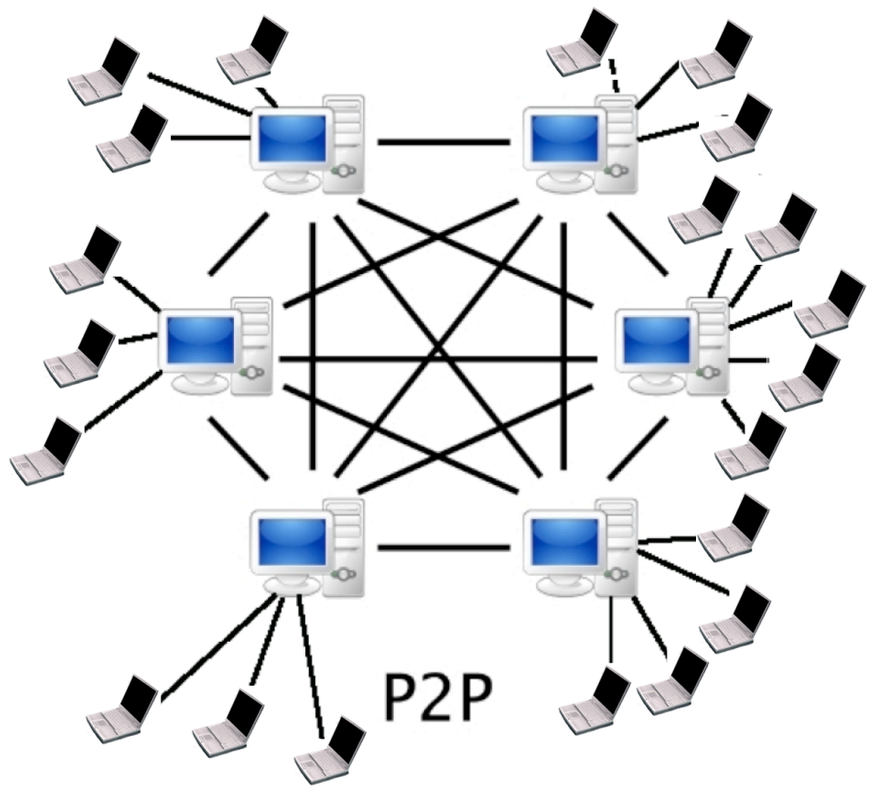
Définition d'une blockchain :

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.

- **Fichier blockchain : ouvert en écriture / ouvert en lecture / semi-ouvert ;**
- **Identité des utilisateurs : masquée (pseudonymat, anonymat) / déclarée (KYC) ;**
- **Chiffrement des données : oui / non / partiel ;**
- **Réseau P2P (qui peut être un nœud ?) : tout le monde / "permissioned"/ … ;**
- **Choix validateur (consensus) : POW / POS / DPOS / Timbre / Cycle / Proba / … ;**
- **Smart-contract : Oui / Non ;**
- **Stabilisé : Oui / Non (réserve, collatéral, ...).**



Centralisé



Les **monnaies cryptographiques** sont des cas particuliers.

Plus de 4000 en novembre 2019 (Coinmarket)

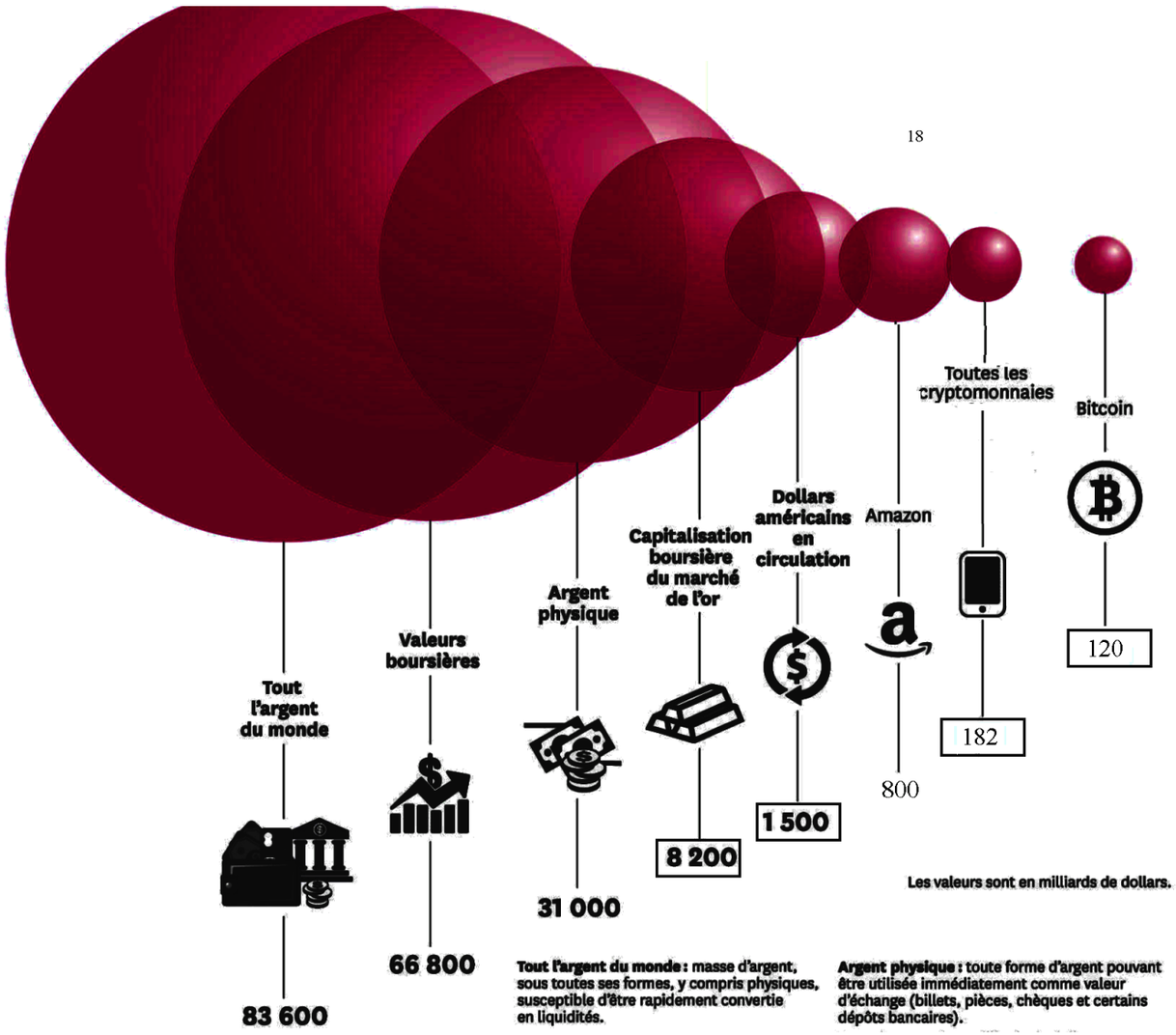
Blockchain : cahier de compte

Cryptocurrencies: 4855 • Markets: 20861 • Market Cap: $182 703 114 215 • 24h Vol: $116 856 654 718 • BTC Dominance: 66.1%

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)
1	Bitcoin	$120 831 512 123	$6 688,13	$44 433 755 513	18 066 562 BTC	-8,01%
2	Ethereum	$14 742 077 073	$135,64	$9 128 993 609	108 685 033 ETH	-10,20%
3	XRP	$9 206 081 600	$0,212612	$10 078 754 434	43 299 885 509 XRP *	-7,93%
4	Tether	$4 117 115 314	$1,00	$30 363 721 879	4 108 044 456 USDT *	-0,75%
5	Bitcoin Cash	$3 582 658 129	$197,59	$2 261 391 557	18 131 538 BCH	-6,97%
6	Litecoin	$2 789 000 004	$43,78	$3 039 216 570	63 703 788 LTC	-8,18%
7	Binance Coin	$2 262 866 921	$14,55	$214 965 613	155 536 713 BNB *	-10,57%
8	EOS	$2 258 244 494	$2,40	$3 773 833 166	941 618 341 EOS *	-10,01%
9	Bitcoin SV	$1 751 568 914	$96,94	$637 377 672	18 068 415 BSV	-7,81%
10	Stellar	$1 107 236 266	$0,055211	$1 045 454 731	20 054 779 554 XLM *	-7,42%

25-11-2019 à 8h : 120 milliards de dollars en bitcoins en circulation

Depuis 1-1-2017 : 1000 $ ➔ 20 000 $ ➔ 3 400 $ ➔ 13 000 $ ➔ 6 700 $


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
800
Toutes les cryptomonnaies
182
Bitcoin
120
Les valeurs sont en milliards de dollars.
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).

Discussions et remarques sur les choix à faire pour une blockchain (principalement de crypto-monnaie)

avec en vue la question

« La confiance dans notre monde numérique peut-elle renaître ? »

On verra que l'intérêt des blockchains dépend de ce qu'on recherche.
Cela change selon qu'on se place du point de vue de l'individu, de l'État, etc.

Rien n'est simple. Les pronostics sont difficiles.

L'exercice est utile pour comprendre le présent et ... ce qui va venir.

A Le problème de la centralisation

Option : Centralisé (on ne peut pas parler de blockchain)

Avantages :

- plus simple, plus rapide ;
- acteur central connu (la banque, l'administration, ...) :
  - il cherche à préserver sa réputation ;
  - on peut s'adresser à lui en cas de problème ;
- possibilités de lutte anti-blanchiment, et contre les trafics et les fraudes.

Inconvénients :

- contrôle unique ;
- censurable ;
- « planche à billets » et donc inflation.

Option : Décentralisé (on peut parler de blockchain)

Les espèces sont décentralisées !
Monnaies cryptographiques de type Bitcoin.

Le but : ne pas tout mettre dans les mains d'un tiers de confiance,
Retirer la monnaie des mains de l'Etat (ce que souhaitait Friedrich Hayek).

Avantages :

- contrôles multiples et croisés (redondance) ;
- non censurables ;
- émissions monétaires sont fixées par le protocole : pas de « planche à billets ».

Le protocole (algorithmique) fixe les règles de manière claire.
Personne ne peut jouer avec les règles écrites et programmées.

Inconvénients :

- c'est plus complexe, moins rapide (c'est encore un problème aujourd'hui) ;
- possibilités de blanchiment et de trafics ;

...***Ce point est peut-être considéré par certains comme un avantage !***

Attention à la décentralisation illusoire !

Exemple : Le Bitcoin. Il y a plus de 5000 nœuds, mais 60% de la puissance de calcul est en Chine

> *Christopher Bendiksen, Samuel Gibbons,* ***CoinShares Research*** The Bitcoin Mining Network Trends, Composition, Average Creation Cost, Electricity Consumption & Sources*,* 5-2019

Or la puissance de calcul du réseau détermine qui gagne les nouveaux bitcoins,
et qui a le pouvoir sur l'évolution du protocole ; beaucoup de puissance permet de perturber le réseau et même de le faire tomber.

Que penser d'une décentralisation contrôlée (réseau "permissioned") ?

EOS : 21 nœuds
XRP
Libra : 100 nœuds validateurs (donc décentralisé)
etc.

1000 transactions par seconde est assez facile.

On perd en pureté.
On gagne en efficacité.

Décentralisation contrôlée : le coût du fonctionnement.

Principe économique élémentaire **:**
il faut payer ceux qui font marcher le réseau, et ce sont les utilisateurs qui paient.

• Donc beaucoup de nœuds validateurs => plus cher.

• Dans le cas de la preuve de travail (POW) une part de l'argent donné aux validateurs est dépensée par eux en équipements de minage et électricité **et ne leur reste pas**.

• **Cas du Bitcoin.**
Pour que les pages puissent circuler assez rapidement,
on limite la taille des pages (donc le nombre de transactions par seconde).
En cas de surchauffe cela conduit à des frais élevés : 55 $ / transaction le 22-12-2017.

Pour la protection de la vie privée :

- décentralisé c'est a priori **moins bien**, puisque les informations sont recopiées un plus grand nombre de fois.

Pour les risques de disfonctionnement, c'est compliqué :

- décentralisé c'est **mieux :**

moins de risque de fausse monnaie (recopie de la blockchain),
moins de risque d'inflation incontrôlée (émission fixée par le protocole),
moins de risque d'erreur (redondance) ;

mais

- nouveaux risques liés au consensus ou au fonctionnement du réseau qui est plus complexe.

Qu'est-ce qui crée la meilleure confiance : centralisé ou décentralisé ?

Pas simple !

Tout dépend des détails du protocole.

Tout dépend de ce qu'on considère comme **prioritaire** et qui on est :

- sécurité des opérations ?
- le contrôle des émissions monétaires (inflation) ?
- lutte contre le blanchiment et les usages frauduleux ?

Tout dépend aussi de l'idée que vous avez des tiers de confiance !

B Le problème de l'anonymat

Anonymat (ou pseudonymat)

Avantages :

- meilleure protection de la vie privée.

Inconvénients :

- facilité à mener des trafics en tout genre.

Il faut distinguer au moins deux anonymats :

anonymat des utilisateurs **et** anonymat des nœuds validateurs.

- **Anonymat des utilisateurs**
  - défendable pour les petites sommes (c'est la protection de la vie privée) ;
  - moins défendable pour les grosses sommes (possibilité de blanchiment et de fraudes).

- **Anonymat des nœuds validateurs**
  - Conduirait mieux à un réseau incensurable ? C'est une illusion (Bitcoin-Chine) :

Il vaut sans doute mieux savoir que le pouvoir de censurer est aux mains d'acteurs indépendants (et concurrents) que de ne pas savoir qui détient le pouvoir.

  - Le contrôle des nœuds validateurs (POS, "permissioned", timbres, etc.) permet :

d'exiger des nœuds d'avoir un minimum de capacité technique ;
de limiter leur nombre ce qui est important pour l'efficacité.

C Le problème des smart-contracts

Les prévoir ?

Avantages :

- Nouveaux types d'applications possibles (finance décentralisée, ICO, STO, etc.)

Inconvénients :

- complexité, nouvelles fragilités.

D Le problème des méthodes de consensus

La preuve de travail (POW) ?

Avantages :

- Augmente le coût d'une attaque 51%, donc consolide le réseau.

Inconvénients :

- Rend coûteux la désignation du nœud validateur, alors qu'il peut ne rien coûter (POS, etc.).
  Bitcoin : au moins 50 TWh/an (pour le Bitcoin) = 6 réacteurs nucléaires.
  POW est un handicap économique dans un contexte de compétition entre réseaux.

- Sur le moyen terme engendre de la centralisation (Chine, Bitmain)

- Incite à un type de fraude spécifique (impossible pour le POS, etc.) : **le crypto-jacking.**

E Le problème de la stabilisation des cours
Stablecoin ?

Avantages :

• Pas de spéculation. Garantie de valeur. Commerce facilité.

Inconvénients :

• Le plus souvent : introduction d'un acteur central qui peut **tricher avec la réserve** (Tether).
- même avec un acteur central assurant la valeur d'échange, **il reste de la décentralisation**.
- il existe des stablecoins décentralisés (DAI).

• Une réserve en fiat est soumise à l'inflation : **perte de l'avantage de l'émission algorithmique**.

• Dans le cas de mécanismes décentralisés de stabilisation : risque de défaillance du système en cas de variation brusque de la demande.

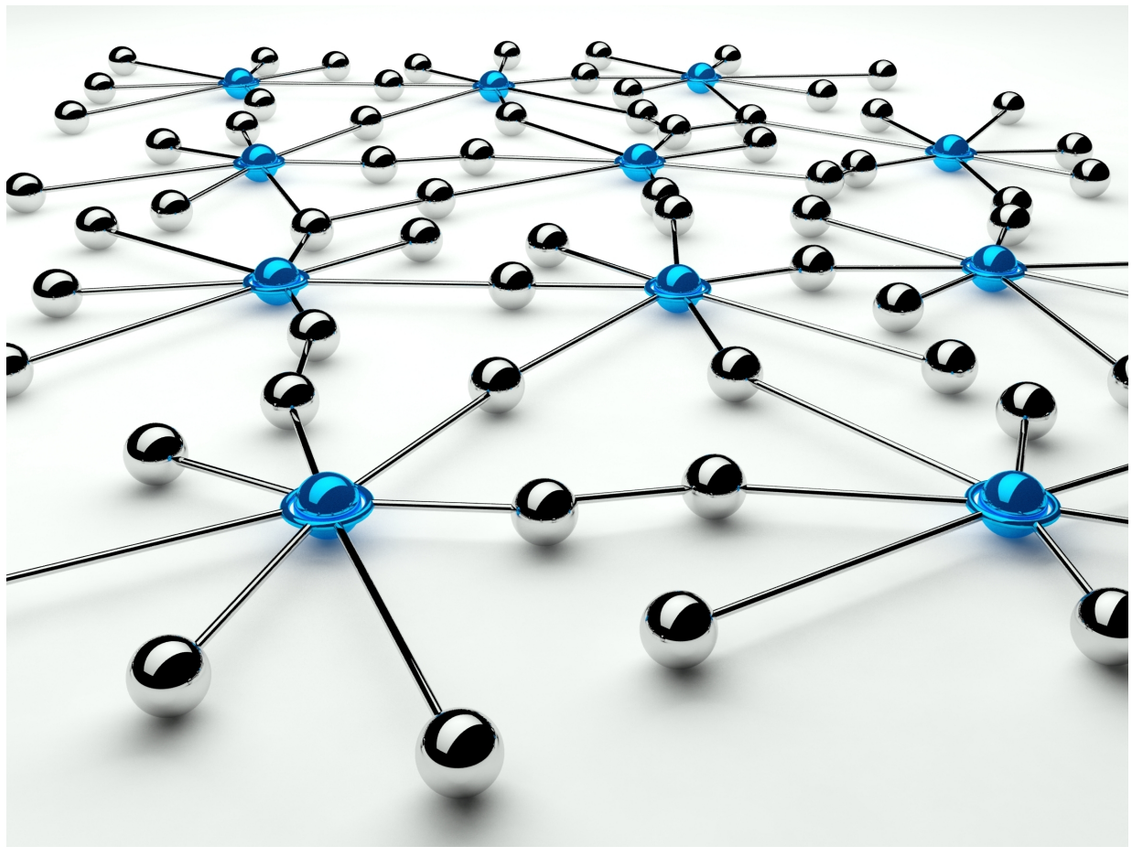
Conclusions.

Les blockchains sont une nouvelle technologie qui permet de développer un nouveau type de partage d'informations et un nouveau type d'applications, dont en particulier les monnaies cryptographiques.

Les nouvelles applications peuvent *créer de la confiance* là où c'était impossible et en se dispensant de tiers de confiance (par exemple sur le contenu des comptes dans le cas d'une crypto-monnaie).
Avec les smart-contracts, on a un outil pour développer facilement des applications décentralisées.

Les risques liés à l'anonymat, aux erreurs (car c'est plus complexe à faire fonctionner), sont à peser pour choisir la bonne configuration de blockchain à mettre en place.

Maintenant que Libra a réveillé les *Banques centrales*, c'est sans doute cette réflexion dans les termes que je viens de présenter qu'elles mènent.
La Chine ne produira probablement pas la même solution que la Fed ou le BCE ... si elles se décident.



Quelques informations

Quantum supremacy
Quantum supremacy : Google l'annonce (novembre 2019), IBM conteste.
En réalité il y a bien un pas de franchi (Aaronson). Il concerne des problèmes très particuliers. L'usage du mot "suprématie" est abusif.

Risque des attaques quantiques ? NON, pas de danger immédiat.

Rapport *National Academies of Sciences, Engineering, and Medicine. Quantum computing: progress and prospects. National Academies Press, 2019.*

La cryptographie post-quantique permet d'envisager un monde où des ordinateurs quantiques universels existeraient.

***

***

Libra

Réactions hostiles.
Paypal, Visa, Ebay, Mastercard s'en vont, mais 1600 attendent.
Prise de conscience que ce sont les *stablecoins* qui sont dangereux et pas seulement Libra.
Les Banques centrales se réveillent.
Une monnaie universelle ?

***

La Chine

L'intérêt déclaré de la Chine pour les blockchains non monétaires.
Xi Jinping parlent des blockchains !
Le minage toléré définitivement ?
Une crypto-monnaie chinoise ?

***

***

Les fausses blockchains

La dénonciation des "fausses applications blockchain en Chine" devrait s'appliquer ailleurs.
Les blockchains de "traçabilités" (supply chain) semblent procéder d'opérations de com.

Si on ne peut pas avoir d'information sur
"qui sont les nœuds du réseau P2P ?", c'est une fausse blockchain.

***

L'évolution des outils de minage ;
L'évolution du hashrate ;
L'évolution de la dépense électrique.

***

***

Bug Bitcoin il y a un an

https://cointelegraph.com/news/the-anatomy-of-bitcoin-cores-recent-bug

***

Les assurances décentralisées

***

L'évolution de la dominance

***

Ethereum va bientôt passer au POS ?

***

Tether plus utilisé que Bitcoin.

***

Le halving de mai 2020

***

https://cryptonaute.fr/banque-france-systeme-reglement-blockchain-europe/

Le 21 novembre 2019, Denis Beau, premier sous-gouverneur de la **banque centrale française** :

“La tokénisation d’actifs financiers, associée à des solutions basées sur la blockchain et à des technologies plus largement distribuées de DLT pour stocker et transférer ces actifs, pourrait aider à répondre aux demandes du marché.

Aussi, cela pourrait contribuer à remédier aux limites actuelles des infrastructures existantes des marchés de gros en explorant de nouvelles pistes.

La mise en œuvre de ces innovations pourrait avoir un impact important sur le secteur financier”.