Bitcoin : crypto-monnaie décentralisée ouverte et libre

Mathématiques, algorithmes et méthode de confiance

David Tsang Hin Sun
tsang@univ-tlse3.fr
UPS/DSI/ Ingénieur informaticien

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université de Toulouse

Sommaire

- Qu'est ce que le bitcoin ?: une crypto devise virtuelle , un protocole, un réseau , une technologie ouverte et libre.
- Comment ça marche: une démonstration (wallet / adresse bitcoin)
- Les outils mathématiques :
    - Clés privées/ clés publiques [Courbes elliptiques+Corps fini (ou de Galois)]
    - Le blockchain : un livre de compte ouvert et décentralisé
      (consensus + règles mathématiques = la vraie invention du bitcoin)
    - Minage / Proof of work (pb des Généraux Byzantins)
- Quelques graphiques (cours du bitcoin, puissance de calcul)
- Les alt-coins : késako ?
- Comment se procurer des bitcoins ?
- Le bitcoin se démocratise: Dell, expedia, Microsoft, Wikipedia …
- M-PESA → Bit-Pesa: le Kenya laboratoire du futur !
- Questions ?
- Références

Bitcoin, bitcoin

Une invention, une technologie : une monnaie numérique, un réseau, un protocole, un logiciel libre.

PC : Personal Computer

INTERNET

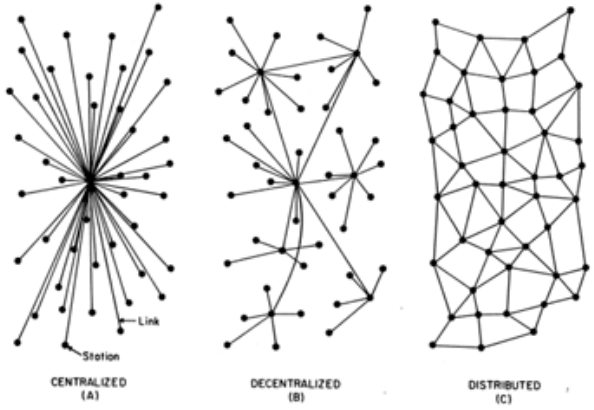


FIG. 1 — Centralized, Decentralized and Distributed Networks

Network Routing Configurations. (1964) Source: Introduction to Distributed Communications Networks, Paul Baran

Logiciels libres

FREE SOFTWARE FOUNDATION

BITCOIN

Le bitcoin , bien plus qu'une crypto devise virtuelle : un protocole, un réseau , une technologie ouverte , neutre et libre.

Bitcoin, bitcoin

Une invention, une technologie : une monnaie numérique, un réseau, un protocole, un logiciel libre.

La monnaie : Unité de compte + Réserve de Valeur + Instrument d'échange

Mais le bitcoin est bien plus qu'une **monnaie**: c'est avant tout **un réseau**, **un protocole, une technologie disruptive , ouverte, libre, neutre , basée sur une confiance décentralisée, orchestrée par les règles mathématiques.**

Source: @AlineRollin https://twitter.com/AlineRollin/status/540830463355797505/photo/1

Bitcoin, bitcoin

Les origines

Le 1er novembre 2008, en pleine crise financière mondiale , un inconnu « Satoshi Nakamoto » poste un message sur une liste de diffusion de cryptographie :

Bitcoin: A Peer-to-Peer Electronic Cash System

- Le 3 janvier 2009, « genesis block » la création ou minage des 50 premiers bitcoins par « Satoshi Nakamoto »

cf http://blockexplorer.com/b/0

- Le 9 janvier 2009, Message posté par « Satoshi Nakamoto » sur mailing liste crypto :

Logiciel libre « Bitcoin v0.1 released »
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Ref:
http://www.bitcoin.org/bitcoin.pdf
http://satoshi.nakamotoinstitute.org/

Bitcoin, bitcoin

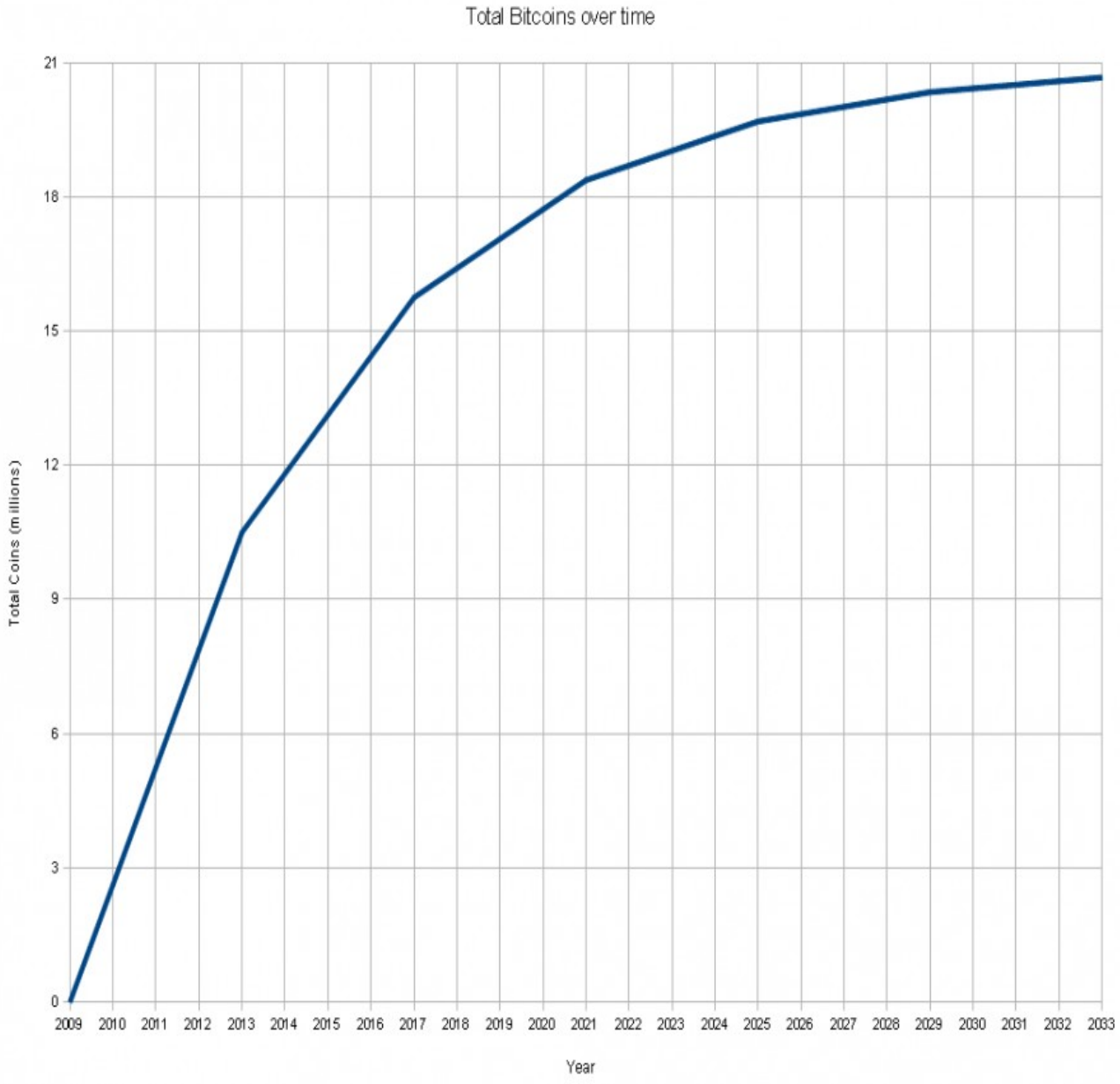
Les origines ?: l'identité de « Satoshi Nakamoto » reste inconnue

Not Me !
Dorian S Nakamoto (CA, USA)

Source:http://techcrunch.com/2014/03/06/satoshi-dorian/

Bitcoin, bitcoin

Les origines et quelques données



- 1 bitcoin = 10^8 satoshis
- 1 satoshi = 0.00000001 bitcoins
- Quantité limitée de bitcoin :
21 millions de bitcoins au maximum d'ici 2140.

- au 05/02/2015 :

~ 13 802 500 bitcoins générés
1 Bitcoin ~ 228 USD

Network Hashrate (Pflops): 3840492.75

256 fois plus rapide que l'ensemble du top 500 des super ordinateurs (Forbes 2013 cf Références)

Bitcoin, bitcoin

Un réseau p2p : https://getaddr.bitnodes.io/

BITNODES

Bitnodes is currently being developed to estimate the size of the Bitcoin network by finding all the reachable nodes in the network.

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Jan 24 2015 10:53:45 GMT+0100 (CET).

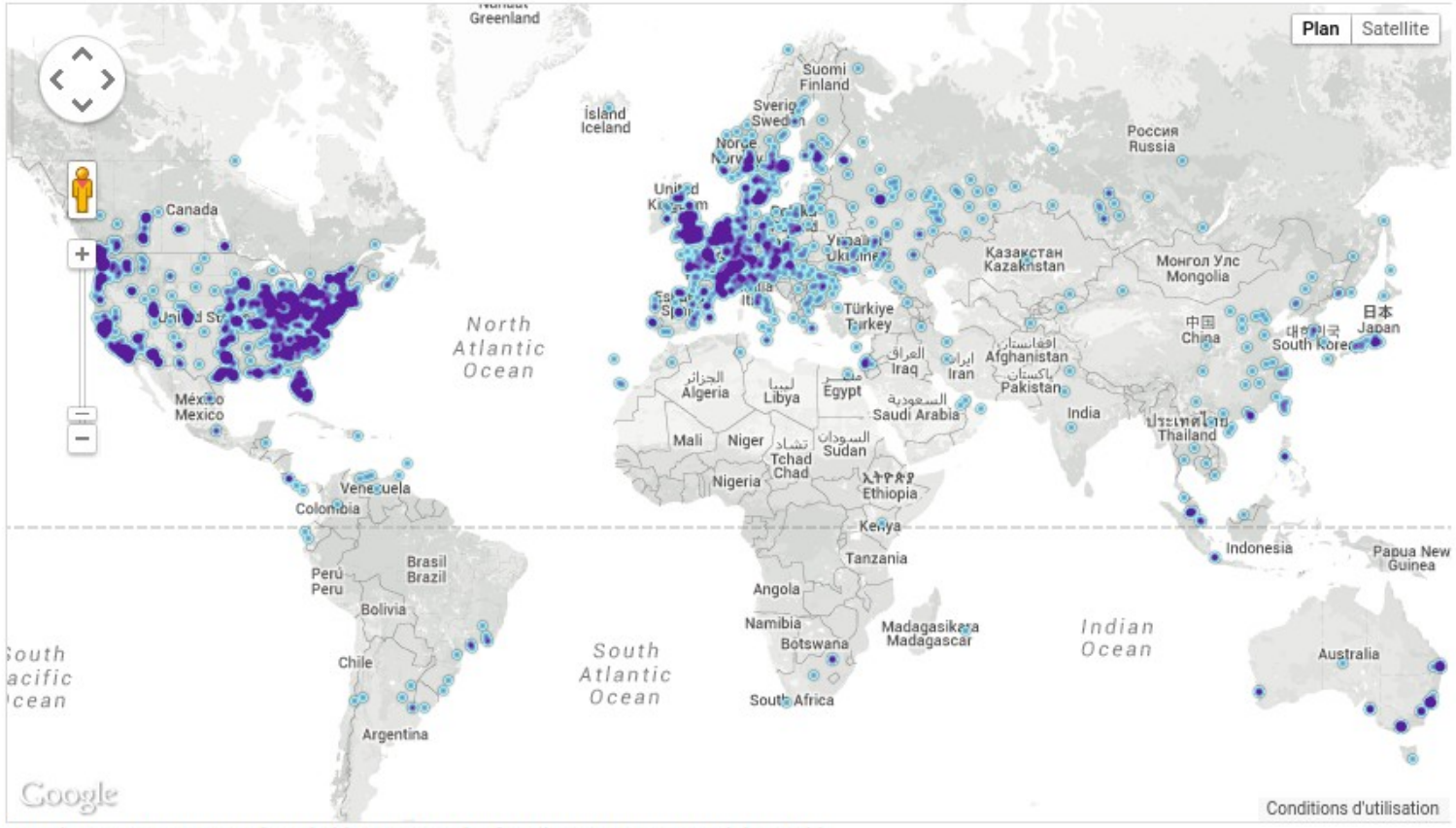
6548 nodes

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2500 (38.18%)
2	Germany	568 (8.67%)
3	France	428 (6.54%)
4	United Kingdom	371 (5.67%)
5	Canada	343 (5.24%)
6	Netherlands	291 (4.44%)
7	Russian Federation	276 (4.22%)
8	China	160 (2.44%)
9	Australia	130 (1.99%)
10	Sweden	123 (1.88%)

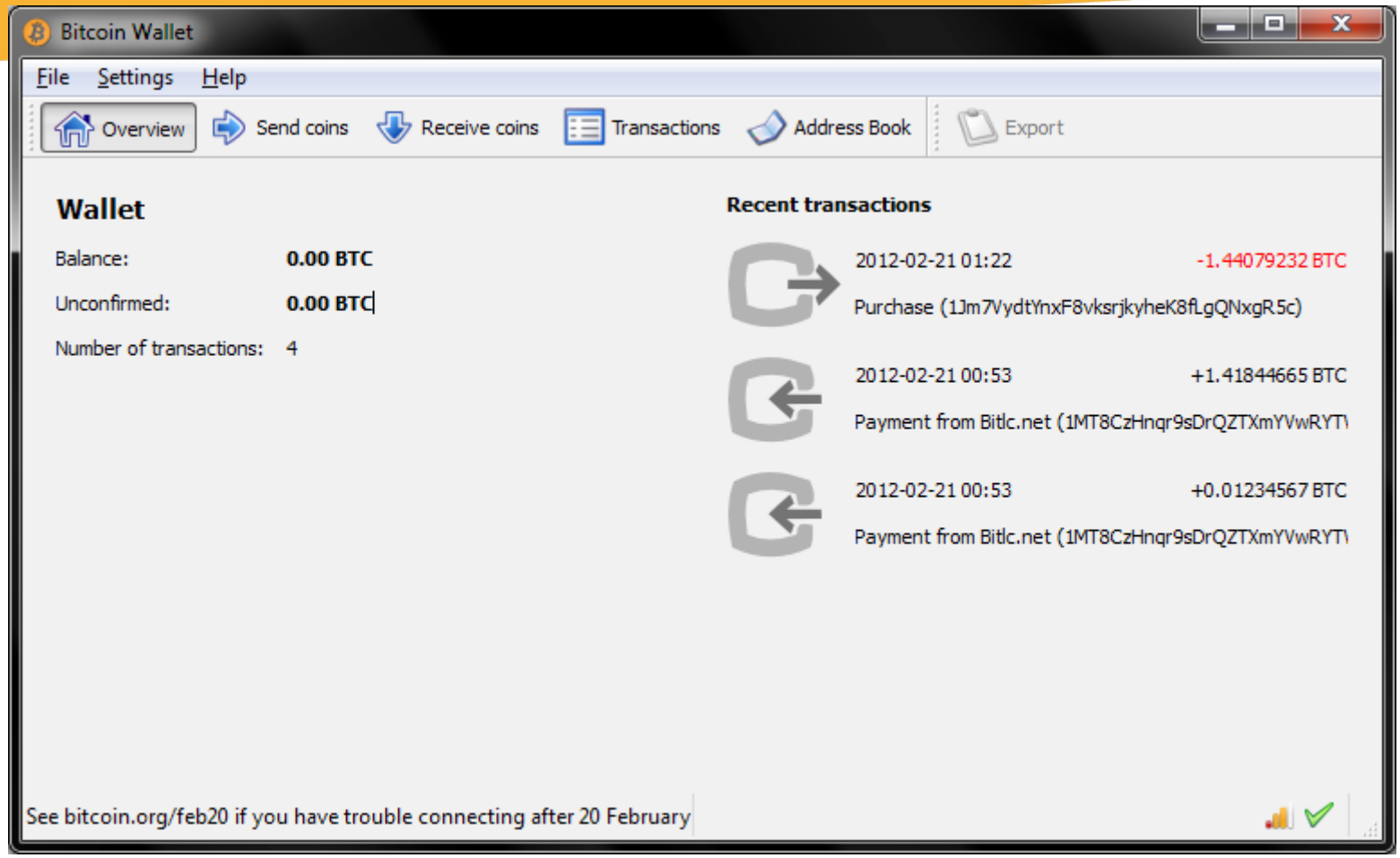
More (87) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

Bitcoin, bitcoin

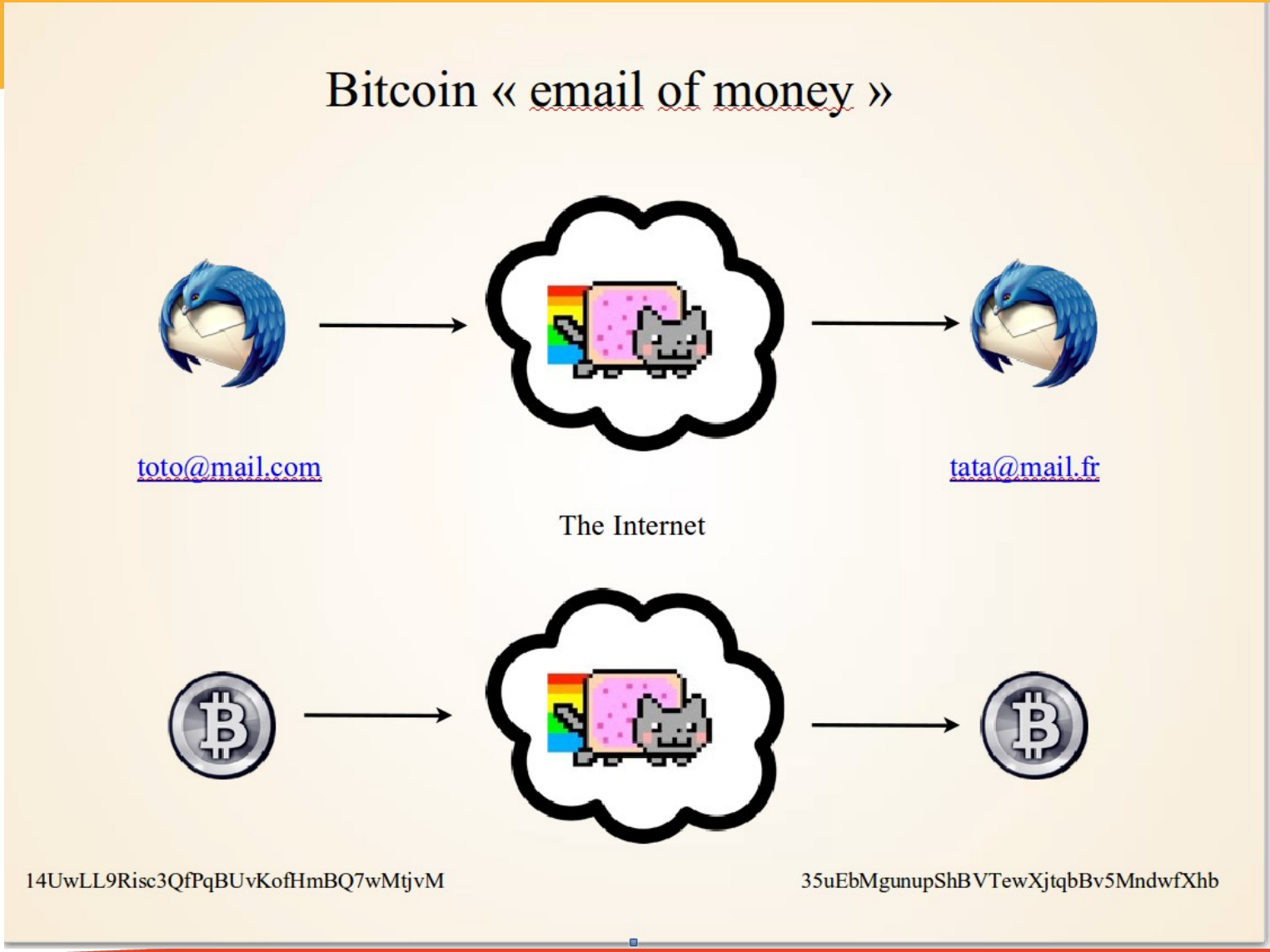
Un logiciel libre , un protocole



https://github.com/bitcoin/bitcoin

Bitcoin, bitcoin

Comment ça marche ? : démonstration



Bitcoin, bitcoin

Comment ça marche ? : il faut un logiciel ou wallet (portefeuille)

Un portefeuille ou wallet, **ne contient pas de bitcoin** (les transactions sont disponibles dans la blockchain). Il **contient uniquement les clés privée et publique** correspondantes à l'adresse bitcoin.

Le terme « porte clés » serait donc plus juste que « portefeuille » !

Adresse(publique) bitcoin de 34 caractères (commencent par 1 ou 3 = multisignature) :

14UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM

https://bitcoin.org/fr/choisir-votre-porte-monnaie

Pour générer des adresses bitcoins: https://www.bitaddress.org

Bitcoin, bitcoin
Une innovation disruptive ?

HALLMARKS OF DISRUPTIVE INNOVATORS

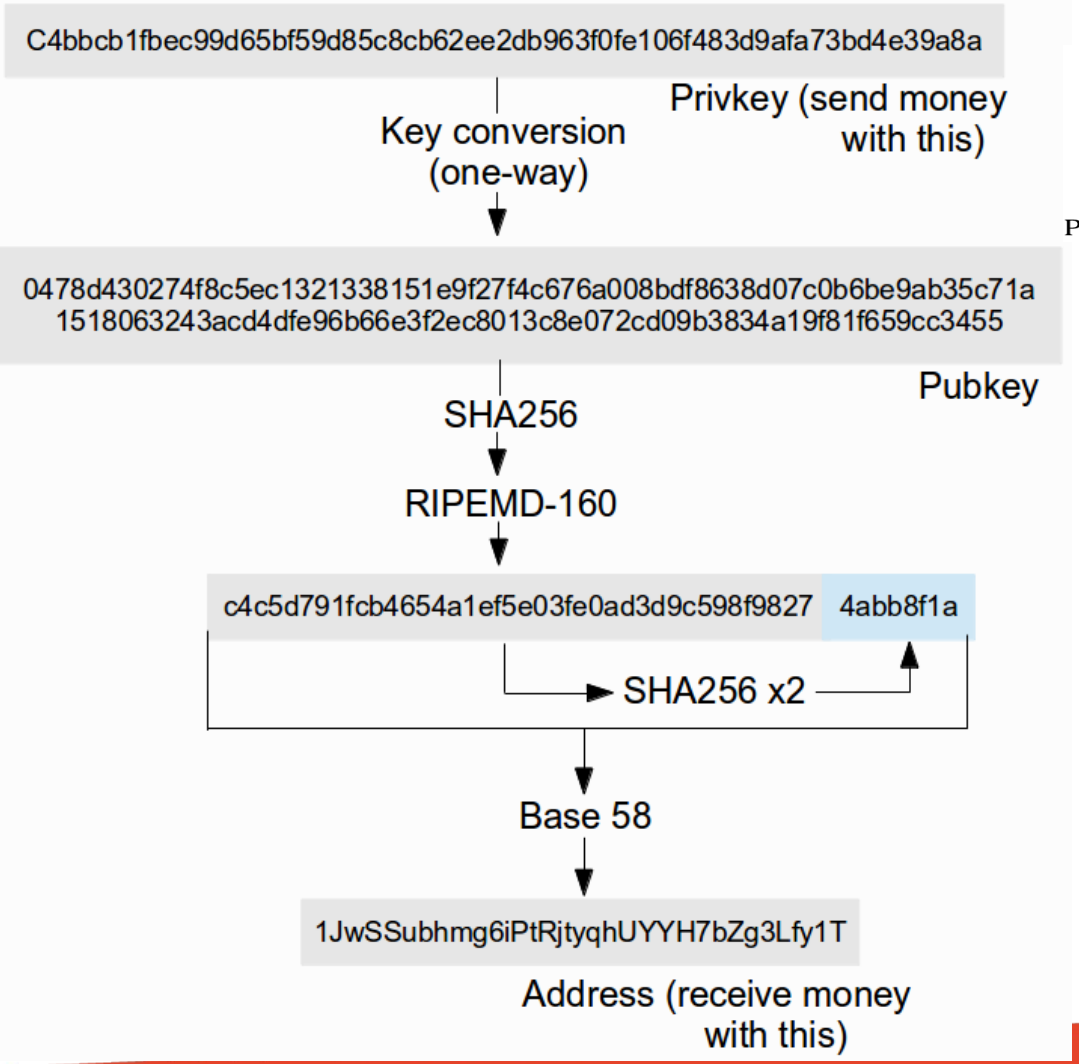
- Introduced by an "outsider"
- Less expensive than existing products
- Targeting underserved or new markets
- Initially inferior to existing products
- Advanced by an enabling technology

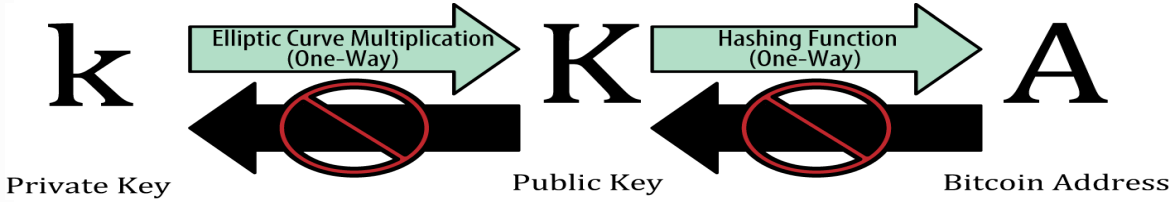
Source:https://twitter.com/tikhon/status/524001742048878593

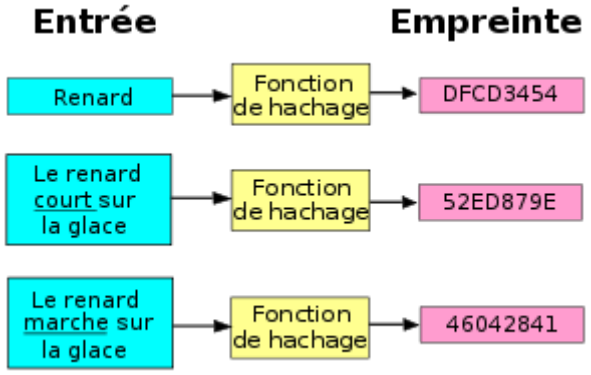
Bitcoin, bitcoin

Les outils mathématiques ?

- Clé privée/Clé publique, Adresse bitcoin , courbes elliptiques + corps fini (ou de galois) , secp256k1, sha256, ripemd-160



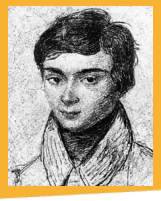




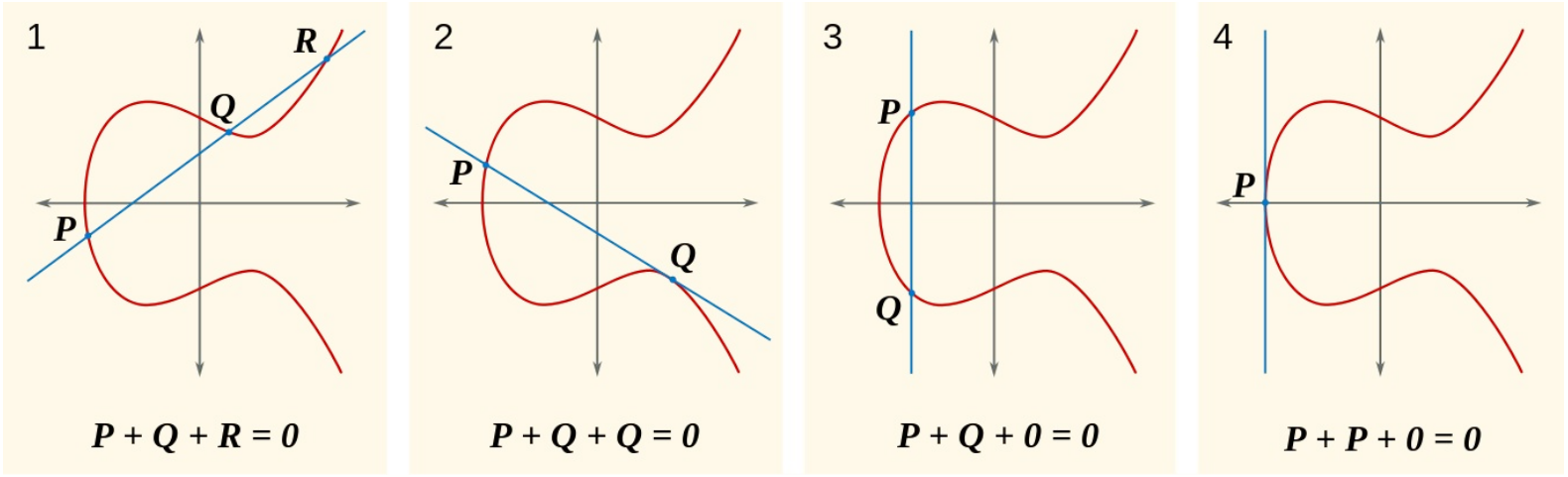
Ref:
https://en.bitcoin.it/wiki/Technical_background_of_Bitcoin_addresses
http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf
http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_introduction

Bitcoin, bitcoin

Mathématique appliquée, cryptographie: $y^2 = x^3 + ax + b$



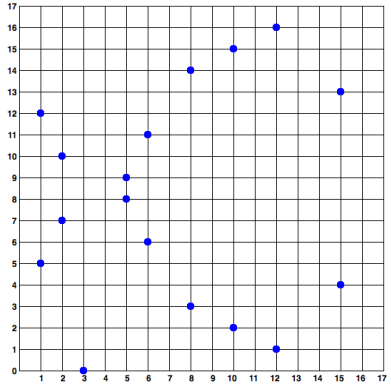
- Clé privée/Clé publique, Adresse bitcoin , courbes elliptiques + corps fini (ou de galois) , secp256k1, sha256, ripemd-160



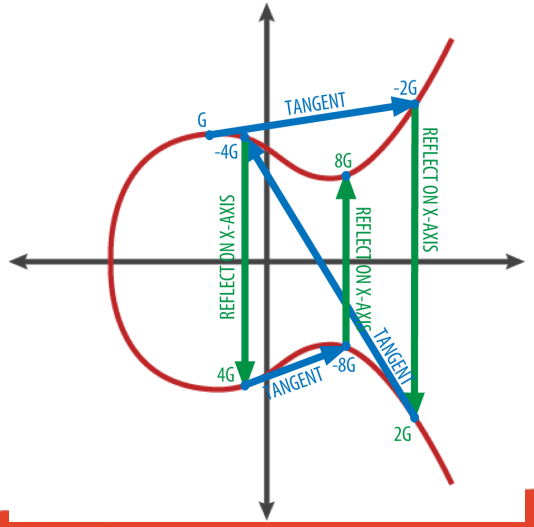
SECP256K1 (NIST) :
$y^2 = x^3+7$ over (Fp)
or
$y^2 \bmod p = (x^3+7) \bmod p$

P = 2^256 – 2^32 – 2^9 – 2^8 – 2^7 – 2^6 – 2^4 – 1

Ref:
http://www.secg.org/collateral/sec2_final.pdf
https://en.bitcoin.it/wiki/Secp256k1



y^^2 mod p = (x3+7) mod p (p=17)



$K = k * G$ (« multiplication » au sens « courbe elliptique »)

K= public key (point sur la courbe elliptique secp256k1)
G= generator point(point sur la courbe elliptique secp256k1)
The size of k = bitcoin's private key space, 2^256 is an unfathomably large number. It is approximately 10^77 in decimal. The visible universe is estimated to contain 10^80 atoms.

Ref:
http://www.coindesk.com/math-behind-bitcoin/
http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#elliptic_curve

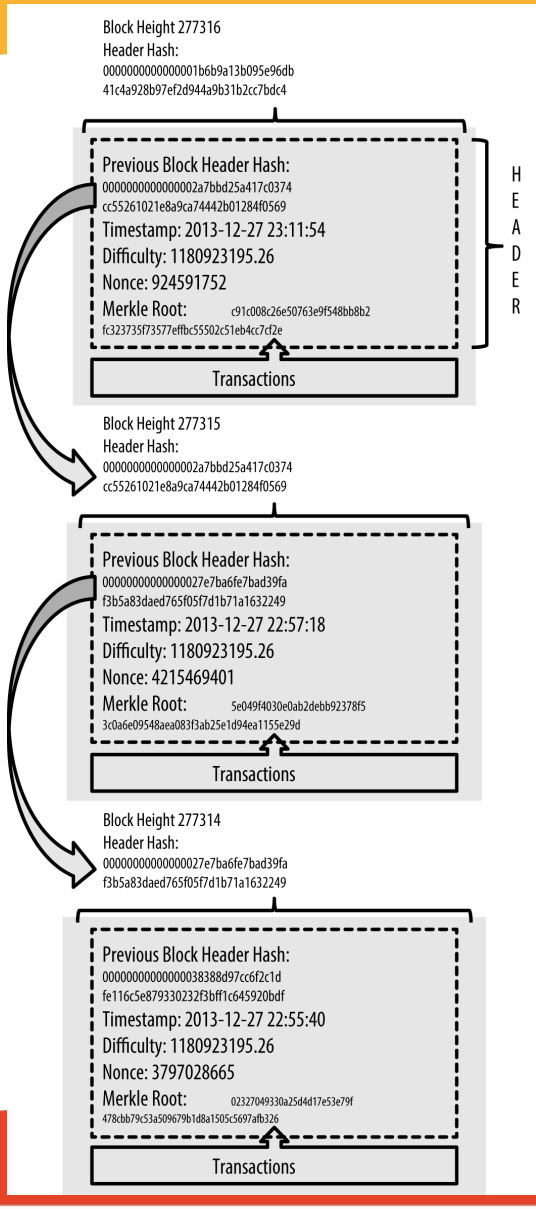
Bitcoin, bitcoin

Le blockchain : c'est la véritable invention du bitcoin !

C'est un registre ou livre de compte à double entrée,ouvert et public contenant tous les blocs (regroupant les transactions signées cryptographiquement).
Les blocs sont minés (validés) environ toutes le 10 minutes sur la base d'un consensus des nœuds du réseau décentralisé, consensus garanti par des algorithmes mathématiques !
Taille de la blockchain =~ 28Go au 5/2/2015

Luca Pacioli 1495 – Comptabilité à partie double
Ref :http://fr.wikipedia.org/wiki/Luca_Pacioli

Vous pouvez consulter les transactions et blocs :
https://blockchain.info/
http://blockexplorer.com/



Bitcoin, bitcoin

Le minage:

processus de validation des transactions et
processus de création des bitcoins

Le minage est le procédé par lequel les bitcoins sont mis en circulation.
Les mineurs effectuent avec leur **matériel informatique des calculs mathématiques (POW) pour le réseau Bitcoin** afin de **confirmer des transactions et augmenter leur sécurité**. Comme récompense pour leurs services, ils collectent les bitcoins nouvellement créés ainsi que les frais des transactions qu'ils confirment.
Les mineurs (ou les coopératives de mineurs) sont en concurrence et leurs revenus sont proportionnels au nombre de calculs effectués.
Un bloc contenant les transactions signées est miné (validé) environ tous **les 10 minutes**, **cette validation rapporte 25 bitcoins** (récompense divisée par 2 tous les 4 ans)

Bitcoin, bitcoin

Proof of Work (POW): solution originale au problème de consensus dans un système distribué (cf pb des généraux byzantins – Lamport 1982)

POW ou Proof of Work est la **solution originale** préconisée par **Satoshi Nakamoto** pour résoudre le problème de consensus dans le réseau distribué de minage (**Pb des généraux Byzantins** – étude de tolérance à la panne de systèmes distribués).
Cela consiste à **résoudre** environ toutes les **10 minutes un puzzle mathématique aléatoire** dont la **difficulté varie** en fonction de la **puissance de calcul du réseau Bitcoin** . La solution du puzzle est « **difficile à trouver ou à calculer** » , mais « **facile à vérifier** » !

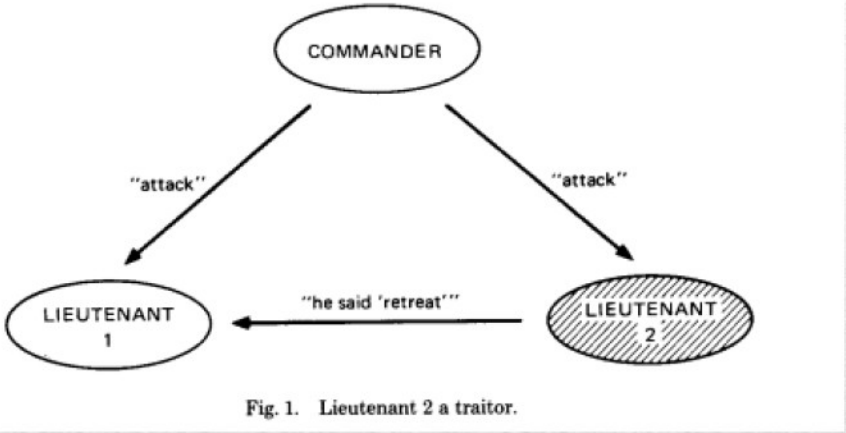


Fig. 1. Lieutenant 2 a traitor.

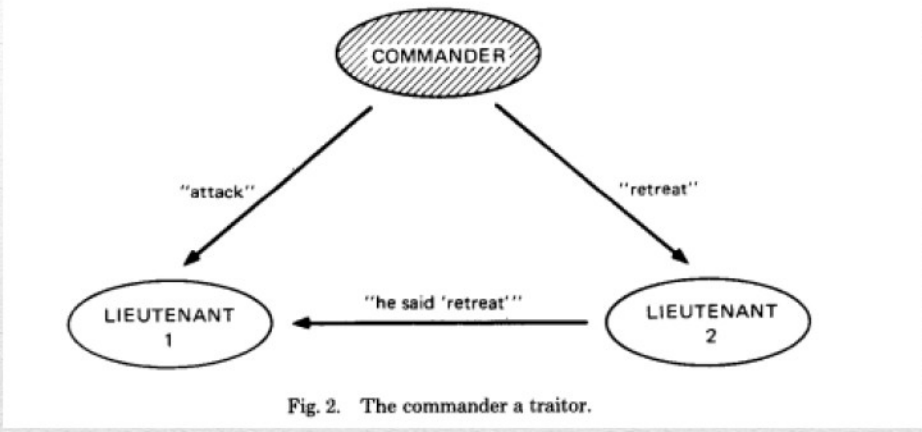


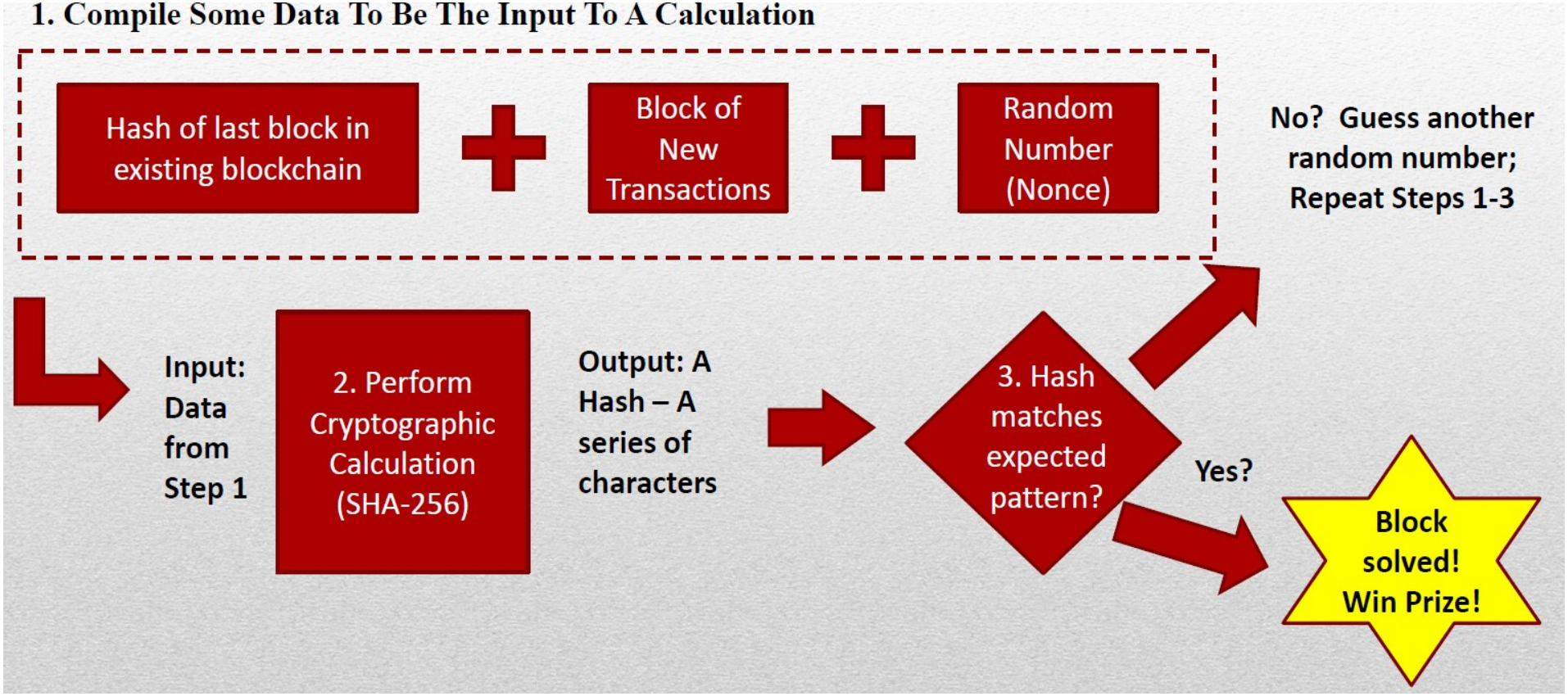
Fig. 2. The commander a traitor.

Le POW fonctionne tant que 51 % des nœuds du réseau Bitcoin sont / restent honnêtes , fiables.

The byzantine generals problem(BGP)
http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf (Leslie Lamport 1982)
Mastering Bitcoin: Mining & Consensus (Andreas Antonopoulos)
http://chimera.labs.oreilly.com/books/1234000001802/ch08.html

Bitcoin, bitcoin

Proof of Work: solution au problème consensus dans un système distribué (pb des généraux byzantins)



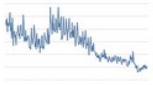
The byzantine generals problem
http://blockexplorer.com/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf
Mastering Bitcoin: Mining & Consensus (Andreas Antonopoulos)
http://chimera.labs.oreilly.com/books/1234000001802/ch08.html

Bitcoin, bitcoin

Quelques graphiques : hashrate , difficulté, cours du bitcoin : https://blockchain.info/fr/charts

Prix du marché (USD)
Un graphique indiquant le prix du marché en USD (Source : Mt.Gox)

% du coût du volume des transactions
Un tableau indiquant les mineurs recettes en pourcentage du volume de transaction.



Coût par transaction
Un tableau indiquant les revenus des mineurs divisé par le nombre de transactions.

Taux de hash
L'estimation du nombre de gigahash par seconde (milliards de hash par seconde) que le réseau bitcoin atteint.

Difficulté
Un tableau montrant l'évolution de la difficulté au fil du temps. La difficulté est une mesure de combien il est difficile de trouver un nouveau bloc par rapport à la simple il ne pourra jamais l'être.

Revenu des mineurs
Graphique historique indiquant le nombre de bitcoins miné par jour + frais de transaction * prix du marché.

Temps moyen de confirmation d'une transaction
Le temps moyen que prennent les transactions pour être acceptées dans un bloc.

Graphiques, statistiques disponibles sur https://blockchain.info/fr/charts

Bitcoin, bitcoin

Les alt-coins: késako ?

Les altcoins sont des dérivés du bitcoin. La majorité sont des copies du code source bitcoin.Chaque altcoin rajoute des fonctionnalités ou modifie la recette de base du bitcoin.

Exemples d'altcoins (+de 700 altcoins):
Primecoin : (calcul de nombre premiers , chaine de cunningham) cf http://primecoin.io/index.php
Ripple : (principe du hawala à la sauve bitcoin)
Litecoin
http://coincreator.net/ vous permets de créer votre propre monnaie alternative ou altcoin.

Mais la technologie du blockchain permets beaucoup d'autres usages que celui de la monnaie :

Ethereum : généralisation du bitcoin au « smart contract » et « Apps »
[bitcoin ~ smtp / ethereum ~ http]
Storj : stockage distribué de type cloud basé sur la technologie blockchain (proof of ressource)
MaidSafe : internet distribué basé sur la technologie blockchain (proof of ressource)
Swarm : plateforme de crowdfunding basée sur la technologie de blockchain et de multisignature

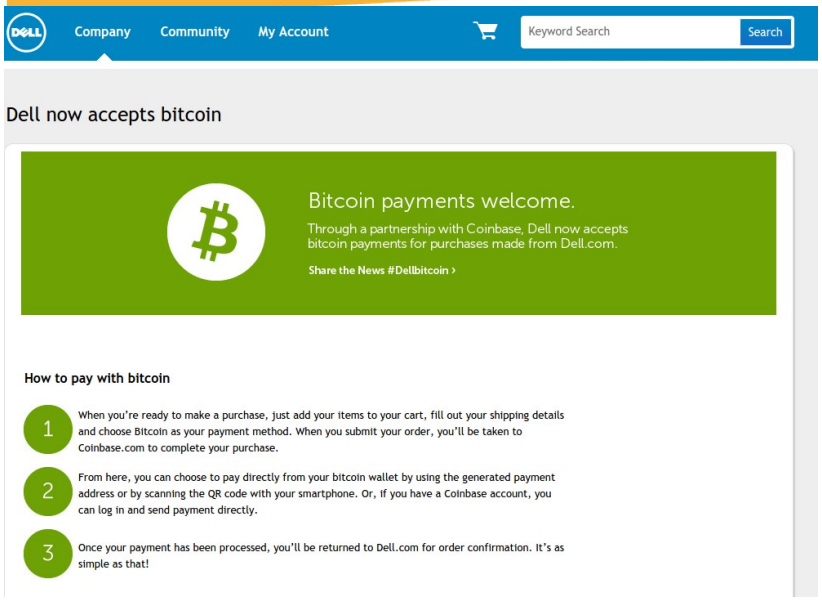
Bitcoin, bitcoin

Comment se procurer des bitcoins ?

1) Vendre des gateaux ou autres spécialités/services pour des bitcoins !
2) Demander à un ami de vous envoyer des bitcoins :-)
3) www.localbitcoins.com (sorte de leboncoin du bitcoin)
4) Place de marché (USD/EUR/BTC) :
kraken.com, coinbase.com , virwox.com, saffelo.com, paymium.com
5) utiliser un distributeur de bitcoin à toulouse : mineoncloud 18 rue de Toul, 31000 Toulouse
http://www.bitcoin.fr/post/Un-distributeur-de-bitcoins-%C3%A0-Toulouse
6) Miner (risqué et ultra compétitif)

Bitcoin, bitcoin

Bitcoin se démocratise : Dell , Expedia, Wikipedia aux USA,



Expedia
To Accept Bitcoin

WIKIMEDIA

donations accepted
bitcoin

Premier Mooc sur les bitcoins par l'Université de Nicosie (par Andréas Antonopoulos : bitcoin guru)
http://digitalcurrency.unic.ac.cy/free-introductory-mooc

Le nombre de publications sur arxiv augmente chaque année :
http://arxiv.org/find/all/1/all:+bitcoin/0/1/0/all/0/1

Apparition de nouveaux services basés sur le blockchain :
Proofofexistence.com :
Service de propriété intellectuelle (sorte d'INPI basé sur le blockchain du bitcoin)
Certificat de mariage dans la blockchain :
https://www.cryptocoinsnews.com/bitcoin-wedding-marriage-on-the-blockchain/

Bitcoin, bitcoin

MPESA → BitPesa : le Kenya un laboratoire pour le futur !

2007, est lancé M-PESA : M=mobile / Pesa= argent en swahili.
Service de paiement par SMS, téléphone mobile (safaricom).
Explosion en 2010, plus de 17 millions de comptes pour 44 millions d'habitants.
Unité de compte = minutes de communication ↔ Shilling Kenyan

2014 : Lancement de Bit-Pesa pour le transfert d'argent via Bitcoin entre le Kenya et l'international ...

2015 …. : Le Kenya est un formidable laboratoire pour comprendre les mécanismes de l'adoption de nouvelles technologies adaptées à un écosystème : le téléphone mobile (non intélligent) , le bitcoin ...

http://www.safaricom.co.ke/personal/m-pesa

BitPesa

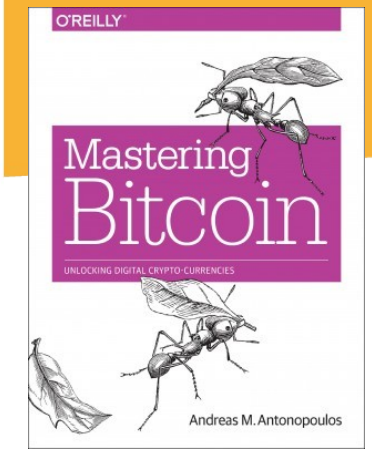
https://www.bitpesa.co/

Bitcoin, bitcoin

Questions ?

Bitcoin, bitcoin

Références :



Bitcoin: A Peer-to-Peer Electronic Cash System par Satoshi Nakamoto (01/11/2008) **:**
https://bitcoin.org/bitcoin.pdf

Mastering Bitcoin par Andréas M. Antonopoulos
Disponible chez amazon ou en libre accès à :
http://chimera.labs.oreilly.com/books/1234000001802/index.html
https://github.com/aantonop/bitcoinbook
Site web de l'auteur :
http://antonopoulos.com/

Le bitcoin par Ken Shirriff :
http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html
http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html
http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html
http://bitcoinstrings.com/ (messages inclus dans le blockchain)

Maths & bitcoin :
http://blog.chain.com/post/95218566791/the-math-behind-bitcoin

« Ce que signifie l'émergence du bitcoin » par Sylvain Fontan, économiste
« Argent valeur vs Argent dette »
http://www.latribune.fr/opinions/tribunes/20141007trib09d1cb928/ce-que-signifie-l-emergence-du-bitcoin.html

Le réseau Bitcoin 256 fois plus puissant que l'ensemble du Top500 des supercomputer
http://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/
http://bitcoincharts.com/bitcoin/
http://www.bitcoinwatch.com/

Quelques liens :
http://bitcoinvanitygen.com/
https://www.bitaddress.org
http://coinmarketcap.com/
http://plus.franceculture.fr/les-mathematiques-et-la-cryptographie-reinventent-la-monnaie-le-bitcoin
http://www.e-ducat.fr/bitcoin-et-les-arbres-de-merkle/
Mooc sur les bitcoins par l'Université de Nicosie (par Andréas Antonopoulos : bitcoin guru)
http://digitalcurrency.unic.ac.cy/free-introductory-mooc