LA GRANDE AVENTURE DU BITCOIN ET DE LA BLOCKCHAIN

SCÉNARIO
OLIVIER BOSSARD

DESSIN ET COULEUR
MAUD RIVIÈRE

DELCOURT

SOMMAIRE

CHAPITRE 1 – **INTRODUCTION AU BITCOIN**

Du troc au Bitcoin
La publication du *Livre blanc du Bitcoin*
Qui était Satoshi Nakamoto ?
Qui sont les cypherpunks ?
La naissance du premier bitcoin !
Comment les bitcoins sont-ils émis ?
Comment Bitcoin contrôle-t-il son offre ?
Pourquoi est-il encore possible de miner des bitcoins ?
En quoi Bitcoin est-il différent des jetons d'achat comme les Q Coins ?
Deux pizzas à plus de 100 millions de dollars !
Le successeur de Nakamoto, Gavin Andresen
Le « robinet aux bitcoins »
Quelles politiques gouvernementales envers les cryptos ?

CHAPITRE 2 – **LE BITCOIN EN PRATIQUE**

Comment fonctionnent les transactions en bitcoins ?
Que se passe-t-il lors d'une transaction Bitcoin ?
Quels frais pour les transactions Bitcoin ?
Qu'est-ce qu'un nœud Bitcoin ?
La signature numérique Bitcoin
Quelques précisions sur l'envoi de bitcoins

CHAPITRE 3 – **LE PROCESSUS DE MINAGE**

Le minage en pratique
Qui sont les mineurs ?
Qu'est-ce qu'une *mining rig* ?
L'évolution des plateformes de minage Bitcoin
À quoi ressemble une ferme de minage ?
Qu'est-ce qu'un *pool* de minage ?
Qu'est-ce que la capacité de hachage ?
Qu'est-ce que la comptabilité concurrentielle ?

CHAPITRE 4 – **LE BITCOIN COMME VÉHICULE D'INVESTISSEMENT**

Quels outils pour investir dans les crypto-actifs ?
Comment utiliser une plateforme d'échange ?
Comment fonctionne le trading de gré à gré ?
Qu'est-ce que le trading quantitatif ?
Qu'est-ce qu'une plateforme d'échange décentralisée ?
Pourquoi utiliser un portefeuille Bitcoin ?
Cold wallet et *hot wallet*
Les nœuds complets et les portefeuilles en ligne
Puis-je utiliser des jetons bitcoin comme moyen de paiement ?
Comment échanger des crypto-monnaies entre elles ?

CHAPITRE 5 – **LA TECHNOLOGIE BLOCKCHAIN**
L'histoire de la technologie *blockchain*
Blockchain, « la machine de confiance »
Comment fonctionne la *blockchain* ?
Qu'est-ce qu'un horodatage ?
Comment la *blockchain* fait-elle consensus ?
Comment catégorise-t-on les *blockchains* ?

CHAPITRE 6 – **MÉCANISMES DE CONSENSUS ET BIFURCATIONS**
Qu'est-ce que le mécanisme de consensus par « preuve de travail » ?
Qu'est-ce que le mécanisme de consensus par « preuve d'enjeu » ?
Qu'est-ce que la « preuve d'enjeu déléguée » ?
Qu'est-ce que la « preuve à divulgation nulle de connaissance » ?
Qu'est-ce que l'algorithme de hachage ?
Qu'est-ce que la cryptographie asymétrique ?
Pourquoi Bitcoin doit-il se mettre à l'échelle ?
Qu'est-ce qu'une bifurcation de *blockchain* ?
Quelle différence entre une bifurcation mineure et une bifurcation majeure ?
Qu'est-ce qu'une attaque par relecture ?
La bifurcation entre Ethereum et Ethereum Classic

CHAPITRE 7 – **APPLICATIONS DE LA BLOCKCHAIN : LES CRYPTO-MONNAIES**
Qu'est-ce qu'une crypto-monnaie ?
Caractéristique #1 : la transnationalité
Caractéristique #2 : l'anonymat
Caractéristique #3 : le registre distribué
Caractéristique #4 : la non-réplicabilité
Qu'est-ce que le Litecoin ?
Qu'est-ce que le NEM ?
Qu'est-ce que le Dash ?
Qu'est-ce que le Monero ?
Qu'est-ce que le Zcash ?

CHAPITRE 8 – **APPLICATIONS DE LA BLOCKCHAIN : PLATEFORMES, TOKENISATION**
Qu'est-ce qu'une plateforme ?
Qu'est-ce que Ethereum ?
Qu'est-ce que EOS ?
Les jetons utilitaires
Qu'est-ce que le jeton utilitaire Augur ?
Qu'est-ce que le jeton utilitaire Golem ?
Les jetons d'actifs
Qu'est-ce que le jeton d'actifs Digix ?
Qu'est-ce que le jeton d'actifs USDT ?

CHAPITRE 9 – **POTENTIEL DE LA BLOCKCHAIN**
La *blockchain* peut-elle changer le monde comme Internet l'a fait ?
Quels sont les inconvénients de la *blockchain* ?
Les grandes organisations autour de la *blockchain*

CHAPITRE 1

INTRODUCTION AU BITCOIN

DU TROC AU BITCOIN

Autrefois, on utilisait en tant que monnaie d'échange des objets tels que des coquillages ou des pierres précieuses.

Leur rareté permettait d'en assurer la valeur.

On utilisa ensuite...

KÉKCÉSSA ?

DES BILLETS, HONORABLE MARCO POLO !

AUSSI APPELÉS PAPIERS-MONNAIES, ILS ONT L'AVANTAGE D'AVOIR UN COÛT DE PRODUCTION TRÈS FAIBLE PAR RAPPORT À LA VALEUR DES BIENS CONTRE LESQUELS ILS PEUVENT ÊTRE ÉCHANGÉS.

CEPENDANT, LEUR VALEUR D'ÉCHANGE EST GARANTIE PAR UN GOUVERNEMENT.

C'EST UNE MONNAIE DITE FIDUCIAIRE, C'EST-À-DIRE BASÉE SUR LA CONFIANCE EN SON ÉMETTEUR.

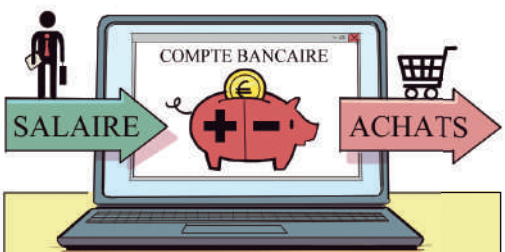
Autre bouleversement de la monnaie...

VIVE LA RÉVOLUTION NUMÉRIQUE !!

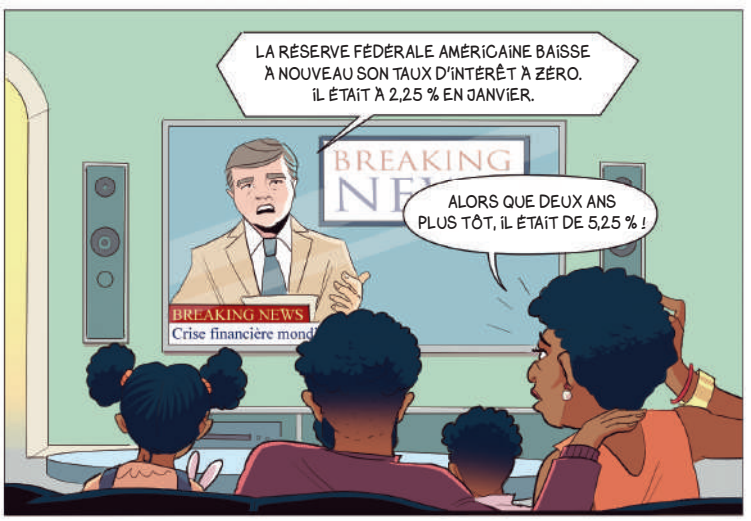
FOLLOW US !

BLOG

Avec Internet, nous sommes passés des billets de banque à des comptes dématérialisés...

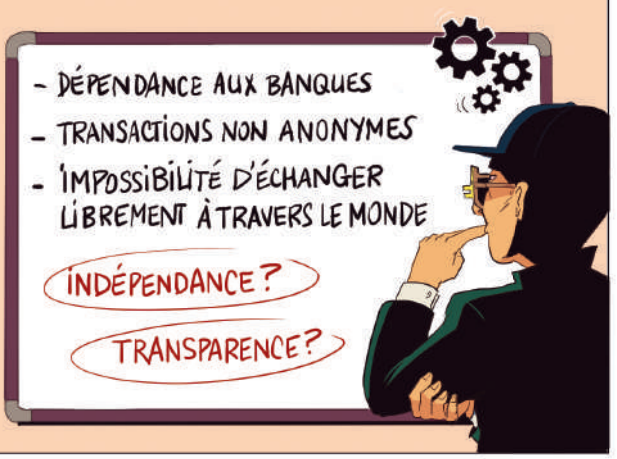


... administrés UNIQUEMENT par les banques.



Un inconnu, caché sous le pseudonyme de Satoshi NAKAMOTO, refusa de subir cette dépendance aux banques centrales.

Il se mit à chercher un nouveau système de paiement qui répondrait aux problématiques soulevées par cette crise.



LA PUBLICATION DU LIVRE BLANC DU BITCOIN

En réponse à cette crise financière de 2008, ce mystérieux Satoshi NAKAMOTO publia un article en ligne intitulé...

« BITCOIN : UN SYSTÈME DE PAIEMENT ÉLECTRONIQUE ENTRE PARTICULIERS »*

Il y décrivait avec une précision redoutable le nouveau système de paiement électronique qu'il venait d'imaginer...

LE SYSTÈME BITCOIN.

INDÉPENDANCE DU CONTRÔLE DE L'OFFRE DE MONNAIE
=
SYSTÈME MONÉTAIRE VIRTUEL POUVANT CONTRÔLER L'OFFRE ET L'ÉMISSION DES JETONS SANS AVOIR BESOIN D'AUCUNE AUTORITÉ CENTRALE.

DROIT ADMINISTRATIF POUR TOUS
=
SYSTÈME DE MONNAIE NUMÉRIQUE *PEER-TO-PEER* (DE PARTICULIER À PARTICULIER) ET DÉCENTRALISÉ.

... ÉMISSION DE JETONS APPELÉS DES BITCOINS.

POSSIBILITÉ DE TRANSFÉRER LES JETONS BITCOIN À N'IMPORTE QUI DANS LE MONDE À TRAVERS CE RÉSEAU.

TRANSPARENCE DE L'ENREGISTREMENT DES OPÉRATIONS
=
TRANSFERT SÉCURISÉ, CHAQUE TRANSACTION EST ENREGISTRÉE.

Bitcoin est donc à la fois le nom du système, de la technologie, et celui des jetons qui circulent dans ce système.

Véritable GENÈSE DU BITCOIN, ce *Livre blanc* marqua par sa publication la naissance de la technologie sous-jacente au Bitcoin...

LA FAMEUSE *BLOCKCHAIN*.

* Le texte original du *Livre blanc du Bitcoin* (11 pages en français) peut être téléchargé librement sur https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf. Il y est même traduit en 40 langues !

QUI ÉTAIT SATOSHI NAKAMOTO ?

Satoshi NAKAMOTO est le créateur et le développeur du système Bitcoin.

Il publia le *Livre blanc du Bitcoin* le 1er novembre 2008 et mina le tout premier jeton bitcoin le 3 janvier 2009.

Il devint ainsi la première personne capable d'utiliser ces jetons bitcoin, minés dans le fameux...

Je vous expliquerai bientôt en détail ce mécanisme de minage et de création des bitcoins.

MAIS QUI ÉTAIT RÉELLEMENT CE SATOSHI NAKAMOTO ?

Beaucoup de gens ont prétendu être cette personne.

2013

Certains émettent l'hypothèse que Satoshi NAKAMOTO est Shinichi MOCHIZUKI, un mathématicien de renommée mondiale.

JE SUIS BIEN SPÉCIALISTE DE LA THÉORIE DES NOMBRES. J'AI NOTAMMENT INTRODUIT LES FROBENIOÏDES, DÉVELOPPÉ LA THÉORIE DE TEICHMÜLLER INTER-UNIVERSELLE, ET AUSSI TENTÉ DE DÉMONTRER LA FAMEUSE CONJECTURE ABC...

... NÉANMOINS, JE NE SUIS PAS SATOSHI NAKAMOTO !

2014

Des pirates informatiques accèdent à l'adresse de messagerie de Satoshi NAKAMOTO et pensent découvrir que le propriétaire de ce compte est l'ingénieur Dorian NAKAMOTO.

MAIS PUISQUE JE VOUS DIS QUE C'EST UNE ERREUR !! J'AI OBTENU L'ACCÈS À CETTE ADRESSE ÉLECTRONIQUE ET SON MOT DE PASSE PAR HASARD !

2016

L'informaticien australien Craig WRIGHT crée un mauvais buzz en prétendant être le véritable Satoshi NAKAMOTO.

OUI, C'EST MOI ! ET JE PEUX LE PROUVER EN VOUS FOURNISSANT SA CLÉ PRIVÉE DE CRYPTAGE.

Cependant, WRIGHT dut retirer sa déclaration, n'étant même pas capable de répondre à tous les doutes exprimés.

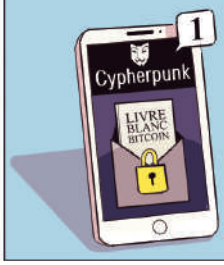
Aujourd'hui, nous ne savons toujours pas qui est le réel Satoshi NAKAMOTO.

Il continue de cacher sa véritable identité, sans doute terrifié de l'impact que son invention pourrait avoir sur sa vie privée et sur sa sécurité.

ALLEZ, SI VOUS VOULEZ MON AVIS, JE PARIERAIS QU'IL S'AGIT EN FAIT D'UN GROUPE DE CYPHERPUNKS DE GÉNIE, PARMI LESQUELS...

QUI SONT LES CYPHERPUNKS?

Le *Livre blanc du Bitcoin* fut publié pour la première fois sur un réseau de messagerie chiffré appellé Cypherpunk.



CYPHER, EN ANGLAIS, DÉSIGNE UN MESSAGE CODÉ ET FAIT RÉFÉRENCE À CETTE BRANCHE DES MATHÉMATIQUES APPELÉE LA CRYPTOGRAPHIE.

VOUS SAVEZ, LE CODAGE ET LE DÉCODAGE SÉCURISÉ DE MESSAGES SECRETS.

Par extension, les utilisateurs de cette messagerie codée se font appeler les « cypherpunks ».

OUAIP ! ON EST LES « PUNKS DE LA CRYPTOGRAPHIE ».

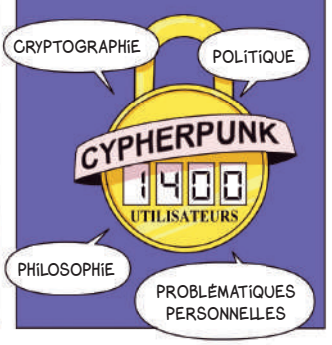
DES « VOYOUS » !

1992 Tim MAY, un grand scientifique travaillant chez Intel, lance la *mailing list* cryptée « Cypherpunk ».

1993 Eric HUGHES écrit un livre intitulé...

C'est la première fois que le mot « cypherpunk » apparaît publiquement.

De nombreux sujets y sont abordés par les utilisateurs.



Les membres d'origine du réseau Cypherpunk sont des célébrités de l'industrie des technologies de l'information, comme...

AVANT LA NAISSANCE DU BITCOIN, LA COMMUNAUTÉ CYPHERPUNK AVAIT DÉJÀ INVENTÉ PLUS DE DIX SYSTÈMES DIFFÉRENTS DE MONNAIES NUMÉRIQUES ET DE SYSTÈMES DE PAIEMENT...

B-MONEY
BIT GOLD
HASHCASH
...

... MAIS AUCUN N'AVAIT VRAIMENT PERCÉ.

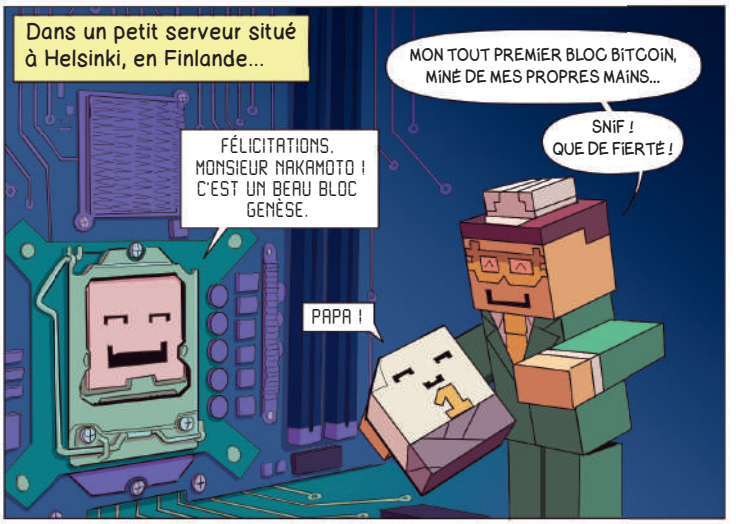
Et c'est là, avec ce fameux Bitcoin, que commence véritablement

L'AVENTURE DE LA *BLOCKCHAIN*.

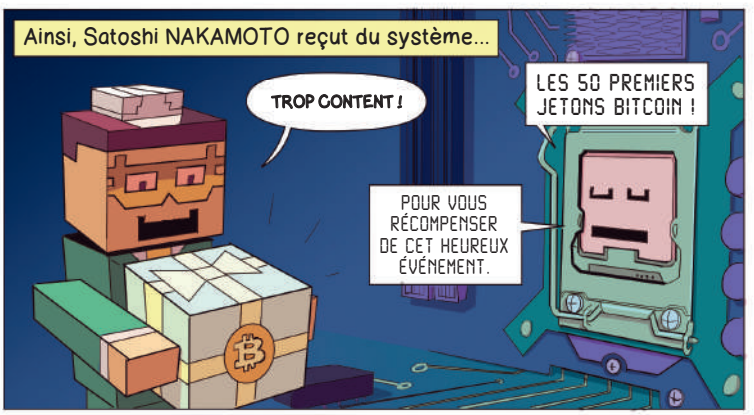
LA NAISSANCE DU PREMIER BITCOIN !

Trois mois après la publication du *Livre blanc du Bitcoin*, le grand jour arriva...

Dans un petit serveur situé à Helsinki, en Finlande...

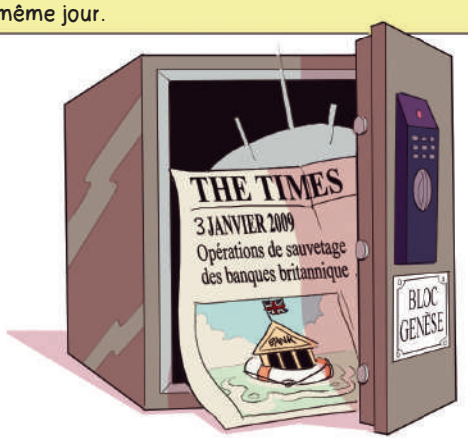


Ainsi, Satoshi NAKAMOTO reçut du système...



LE BITCOIN (BTC) ÉTAIT NÉ !

Pour commémorer cette naissance du Bitcoin, Satoshi NAKAMOTO inséra dans le code de ce premier bloc un article du *Times* daté du même jour.



COMMENT LES BITCOINS SONT-ILS ÉMIS ?

Tout d'abord, QU'EST-CE QUE LE BITCOIN ?

Il s'agit d'une monnaie numérique de particulier à particulier et décentralisée.

BITCOIN ZONE

COMMENT ÇA, VOUS N'AVEZ PAS BESOIN DE MOI ? VOUS SAVEZ QUI JE SUIS ?

LAISSE TOMBER ! ICI C'EST *PEER-TO-PEER*.

NO BANK

BANK

LE SYSTÈME QUI PERMET D'ÉMETTRE CES BITCOINS EST ÉQUIVALENT À UN GRAND REGISTRE.

Il n'a pas d'émetteur spécifique et repose seulement sur un système de distribution décentralisé.

La tenue de ce registre est réalisée par des informaticiens appelés des « mineurs ».

SALUT !

NO BANK

FREE

REGISTRE

Toutes les dix minutes, les mineurs se font concurrence pour être les premiers à trouver la solution à un problème mathématique complexe leur permettant d'obtenir le droit d'enregistrer sur ce grand registre une nouvelle page appelée « bloc ».

MINUTES

BLOC

VOUS AVEZ GAGNÉ !

50 BITCOINS

Pour chaque bloc enregistré, le mineur obtient une certaine quantité de bitcoins en récompense. Ces jetons bitcoin sont émis progressivement par le système.

C'est donc ainsi que ce processus de « minage » permet l'émission de nouveaux bitcoins.

COMMENT BITCOIN CONTRÔLE-T-IL SON OFFRE ?

Le Bitcoin est une monnaie virtuelle qui a été mise en place avec une offre limitée.

Le nombre total de bitcoins émis n'excédera pas...

21 MILLIONS DE JETONS

Lors de la conception du Bitcoin, NAKAMOTO définit pour chaque jeton bitcoin une limite de divisibilité à 1 centième de millionnième.

TOUT COMME 1 EURO PEUT ÊTRE DIVISÉ EN 100 CENTIMES D'EURO, LE BITCOIN PEUT ÊTRE DIVISÉ EN UNITÉS PLUS PETITES APPELÉES SATOSHIS.

100 000 000 SATOSHIS POUR ÊTRE PRÉCIS.

0,00000001
1 unité = 1 satoshi

En pratique, cette divisibilité permet en cas de hausse du bitcoin de le rendre accessible à tous et utilisable comme monnaie quotidienne.

VOUS POUVEZ MÊME ACHETER UN ORDINATEUR DE *GAMING* ALIENWARE EN UTILISANT DES BITCOINS !

PAF! PIF!

MAIS POURQUOI CETTE OFFRE PRÉPROGRAMMÉE ?

Cette limite fut fixée par Satoshi NAKAMOTO selon **DEUX RÈGLES** ...

Règle n° 1 :

1 bloc = 10 min.

210 000 blocs = 4 ans

Règle n° 2 : La récompense en bitcoins pour le minage d'un bloc est divisée successivement par 2 tous les 210 000 blocs.

JACKPOT !

?! GRAT GRAT

GLOUPS !

ARGH !

Vers l'an **2045**, **99,95 %** des bitcoins seront émis

LE TOUT DERNIER JETON. SNIF !

2009	2012	2016	14 MAI 2020	2140
50 JETONS	25 JETONS	12,5 JETONS	6,5 JETONS	
0 à 210 000 blocs	211 000 à 420 000 blocs	421 000 à 630 000 blocs	631 000 à 840 000 blocs	20 790 000 à 21 000 000 blocs

Cette offre préprogrammée du Bitcoin provoqua tout un débat parmi les économistes.

CE SYSTÈME APPORTE UNE SOLIDITÉ INTRINSÈQUE !

MAIS POURQUOI EN LIMITER LA QUANTITÉ ?!

ON IMITE AINSI LES RÉSERVES D'OR !

BLA BLA BLA BLA BLA BLA BLA BLA BLA BLA

Ce mécanisme eut pour effet d'encourager les mineurs à commencer au plus vite leur activité.

... ET QUI DIT PLUS DE MINEURS, DIT PLUS DE PUISSANCE DE TRAITEMENT DES TRANSACTIONS...

... MAIS AUSSI PLUS DE SÉCURITÉ AU RÉSEAU, CAR CHAQUE MINEUR POSSÈDE UNE COPIE DU REGISTRE BITCOIN, OÙ LES BLOCS SONT RELIÉS ENTRE EUX.

POURQUOI EST-IL ENCORE POSSIBLE DE MINER DES BITCOINS ?

Le système Bitcoin ajuste sa difficulté de minage pour perdurer dans le temps.

BON, LES GARS, COMME VOUS LE SAVEZ DÉJÀ, ON A DIX MINUTES POUR CREUSER ET RÉSOUDRE LE PROBLÈME... À LA CLÉ, UN BLOC À CRÉER ET DES JETONS BITCOIN EN RÉCOMPENSE POUR LE VAINQUEUR.

MIN. 10 20 30 40 50 60 FACILE DIFFICILE

ATTENTION, LE NIVEAU DE DIFFICULTÉ A DE NOUVEAU AUGMENTÉ !

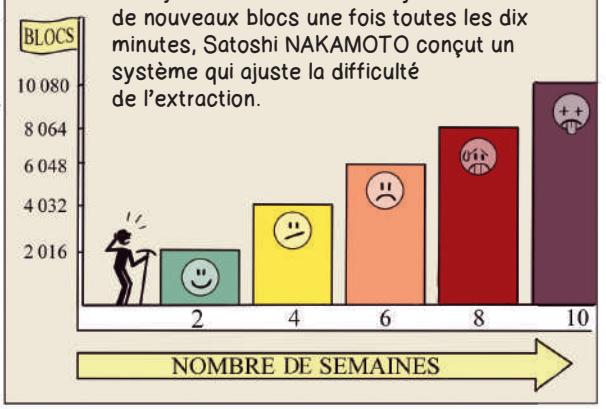
ENCORE ??
MAIS ON N'Y ARRIVERA JAMAIS !!

ALORS TOUS À VOS POSTES ET QUE LE PLUS RAPIDE GAGNE !

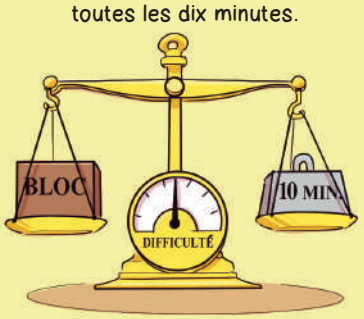
Imaginez si la puissance de calcul du réseau Bitcoin ne cessait d'augmenter....

HEY, LES GARS, AVEC MA NOUVELLE BÉCANE, ON VA MINER TOUS LES JETONS BITCOIN EN UN RIEN DE TEMPS !

Pour justement maintenir le rythme de création de nouveaux blocs une fois toutes les dix minutes, Satoshi NAKAMOTO conçut un système qui ajuste la difficulté de l'extraction.



Ainsi, cette difficulté ajustée permet de maintenir le rythme de génération des nouveaux blocs à un seul bloc toutes les dix minutes.



À l'heure actuelle...

DIFFICULTÉ = 480PH/S (OU PÉTA-HASH PAR SECONDE)

SOIT ENVIRON 68 MILLIARDS DE FOIS PLUS DIFFICILE QUE L'EXPLOITATION DU BLOC GENÈSE.

RENDEZ-VOUS COMPTE... CELA SIGNIFIE QUE, SUR LA BASE DE LA PUISSANCE DE CALCUL ACTUELLE, TOUS LES MINEURS DOIVENT EFFECTUER **300 SEXTILLIONS DE *HASHS**** (SOIT 3×10^{23} *HASHS*) AFIN DE RÉSOUDRE LE PROBLÈME CRYPTOGRAPHIQUE LEUR PERMETTANT DE GAGNER L'EXPLOITATION DU NOUVEAU BLOC.

* *Hash* = algorithme ou série d'opérations mathématiques effectuées par un ordinateur.

EN QUOI BITCOIN EST-IL DIFFÉRENT DES JETONS D'ACHAT COMME LES Q COINS ?

T'ES QUI, TOI ?

UN Q COIN. JE FAIS PARTIE DE LA FAMILLE DES JETONS D'ACHAT. NOUS SOMMES ÉMIS PAR DES ENTREPRISES PRIVÉES.

LA MIENNE S'APPELLE TENCENT.

ET TOI ?

VS

ON M'APPELLE BITCOIN. JE SUIS UN ACTIF NUMÉRIQUE QUI, CONTRAIREMENT À TOI, EST ENTIÈREMENT DÉCENTRALISÉ.

AUCUNE ENTITÉ NE ME CONTRÔLE !

JE SUIS CERTES ÉMIS PAR UNE INSTITUTION CENTRALISÉE, MAIS C'EST GRÂCE À LA CONFIANCE QUE LES GENS ONT EN L'ENTREPRISE TENCENT QUE JE SUIS LARGEMENT ACCEPTÉ DANS LE MONDE.

IL A RAISON ! CEPENDANT, LEUR UTILISATION EST ÉGALEMENT LIMITÉE AUX JEUX ET SERVICES DE TENCENT. LA VALEUR DE TELS JETONS D'ACHAT DÉPEND DONC ENTIÈREMENT DE CETTE CONFIANCE QUE L'ON PEUT AVOIR ENVERS SON ENTREPRISE ÉMETTRICE.

SI JE COMPRENDS BIEN, C'EST PAS VRAIMENT UNE MONNAIE, MAIS PLUTÔT DES JETONS D'ÉCHANGE POUR UN MARCHÉ PRÉCIS ?

EN TOUT CAS, **MOI**, JE N'AI PAS BESOIN DE M'APPUYER SUR LA MOINDRE AUTORITÉ CENTRALE POUR ÊTRE ADOPTÉ DANS LE MONDE ENTIER !

JE DISPOSE D'UNE SUPER TECHNOLOGIE INALTÉRABLE !

Cette fameuse technologie réside dans la capacité innée du Bitcoin à créer la confiance...

AUCUNE AUTORITÉ CENTRALE

INDÉPENDANCE ET LIBERTÉ D'AGIR

ÉMISSION ET CIRCULATION DES BITCOINS ENREGISTRÉES DANS LA *BLOCKCHAIN*

TRANSPARENCE ET SÉCURITÉ DES TRANSACTIONS

Elle forme une chaîne solide et solidaire qui garantit que personne ne puisse altérer le registre.