B n B: Bitcoin et Blockchain

Guy Bégin

UQAM

Midi-conf du 30 novembre 2016

Monnaie

Chronologie et mystère

bitcoin

Blockchain

Bitcoin

- Une technologie de l'information
- Un système de paiement décentralisé et sécuritaire
- Un mécanisme pour stocker, vérifier, auditer des informations
- Un système pour représenter numériquement de la valeur
- Un réseau décentralisé

Rôles d'une monnaie

Unité de compte, réserve de valeur et intermédiaire des échanges

- Intermédiaire d'échange : annuler les dettes et les obligations
- Instrument de paiement
- Réserve de valeur
- Unité de compte pour le calcul économique ou la comptabilité
- Une devise
  - Cours légal dans une juridiction
  - Devise : monnaie d'un pays étranger

Caractéristiques essentielles d'une monnaie

- Confiance
- Persistance de la valeur
  - Et l'inflation ?
- Capacité à servir de moyen d'échange
  - Partageable
  - Transportable

Monnaies modernes

Les monnaies modernes sont des monnaies fiduciaires

- Les supports n'ont pas de valeur intrinsèque
- Émises par une banque centrale
- Reposent uniquement sur la confiance du public en l'émetteur
  - Confiance de pouvoir l'échanger, maintenant et dans le futur pour des biens ou des services
- Formes
  - Monnaie fiduciaire corporelle : argent sonnant et trébuchant
  - Monnaie scripturale
  - Support électronique

Bitcoin (grand B)

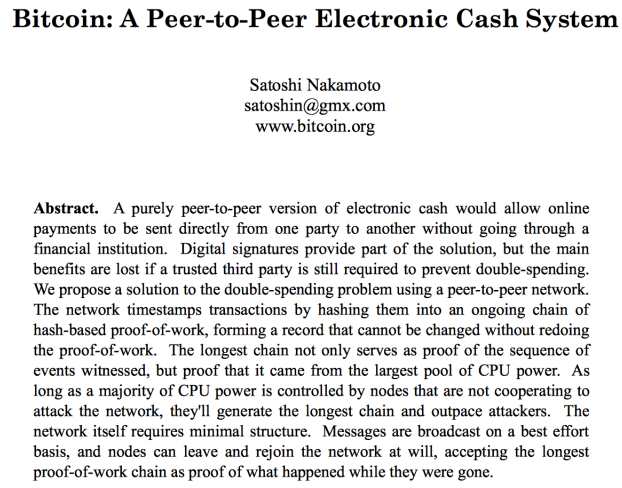
- Un concept
- Un système d'échange de valeurs
- Une application

Caractéristiques de la monnaie Bitcoin

- Une monnaie «déflationaire» : la récompense décroît avec le temps
- Divisible en très petites unités
- Frais de transactions payés au réseau
- Le même coût pour une transaction de $.01 ou de $1 000 000
- Basé sur le consensus : sans autorité centrale
- Difficile à contrefaire
- Processus de création bien défini
- Ne peut se dépenser plusieurs fois

Chronologie

- 18 août 2008 : enregistrement du nom de domaine «bitcoin.org»
- 31 octobre 2008 : publication de l'article fondateur
- 9 novembre 2008 : enregistrement du projet Bitcoin sur SourceForge.net
- 3 janvier 2009 : premier bloc à 18 :15 :05 GMT
- 9 janvier 2009 : lancement de l'application Bitcoin v0.1 (via «mailing list» cryptographique)
- 12 janvier 2009 : première transaction Bitcoin, de Satoshi à Hal Finney, dans le bloc 170



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. 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.

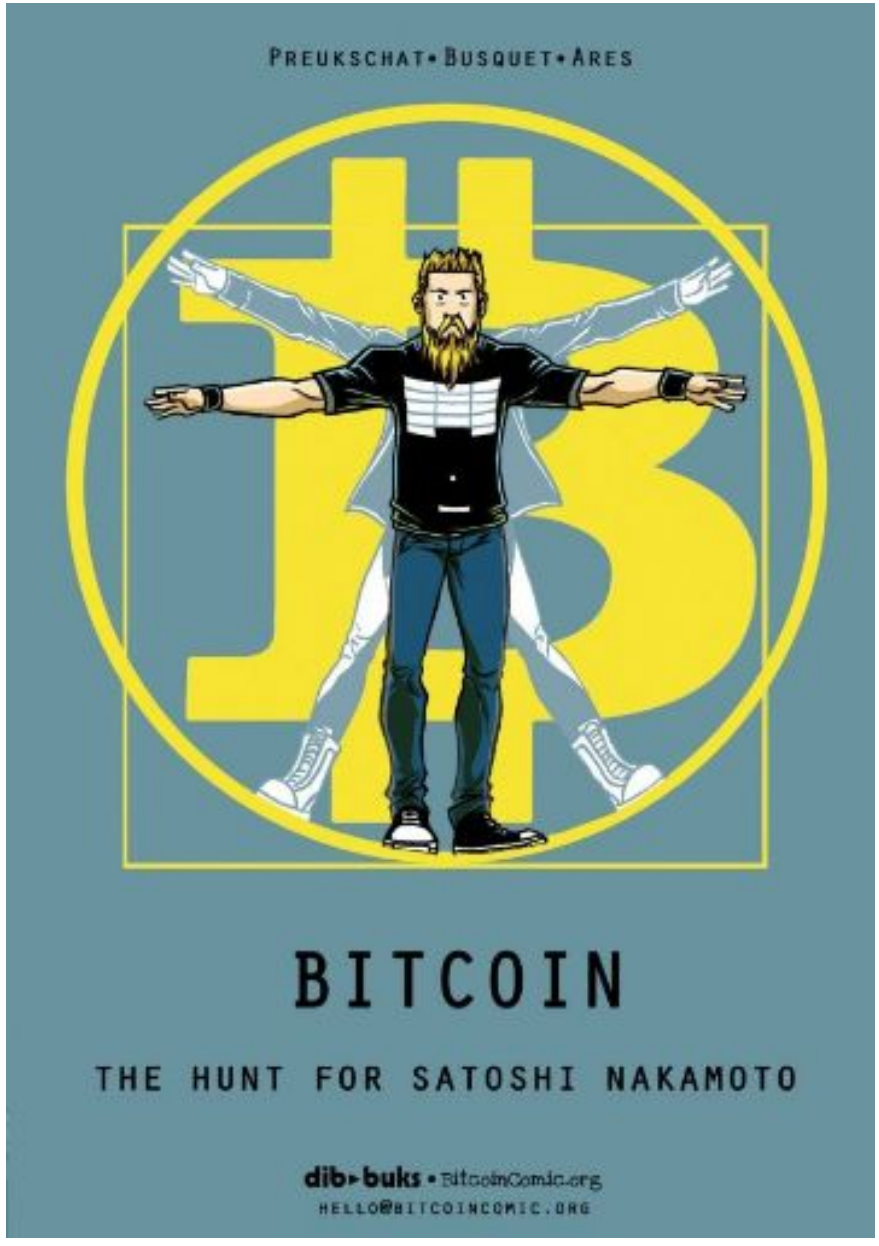
Première «vraie» transaction

La première fois où des bitcoins ont été utilisés pour acheter quelque chose de tangible

- 22 mai 2010 : un programmeur, Laszlo Hanyecz, paye 10 000 BTC à un collègue du forum Bitcoin Talk pour deux pizzas Papa John's
- Selon la valeur actuelle du bitcoin, c'est **9 954 800 $ CAN**

Qui est Satoshi Nakamoto ?

- Il possèderait un million de bitcoins, valeur de plus de 500 millions US$



Hal Finney ?

- Bénéficiaire de la première transaction

Dorian Nakamoto ?

- Selon un article de Newsweek magazine
- Prétend que non

Nick Szabo ?

- Concepteur du «bit gold»

Craig Steven Wright ?

- Entrepreneur Australien
- En mai 2016, prétend être SN
  - Fournit des «preuves» cryptographiques
  - Preuves sont contestées
- Mais plus tard : «I'm Sorry»
- «either invented bitcoin or is a brilliant hoaxer who very badly wants us to believe he did»

Lui ?

?

OK, mais comment ça marche ?

bitcoin (petit b)

- Une unité de valeur intangigle
- La plus petite unité - un satoshi - vaut 1/100 000 000-ième de bitcoin
- La valeur du bitcoin à un moment donné est déterminée par l'usage économique qui en est fait, donc par le marché

Concepts et mécanismes nécessaires

- Le réseau Internet : pour les communications entre les participants
- Un moyen de vérifier la validité des transactions et de les inscrire dans un fichier public sans autorité centrale
  - Une chaîne de signatures électroniques qui certifie les transferts de fonds (transactions)
- Un moyen d'éviter la double utilisation d'un bitcoin
  - Un registre de transactions horodaté

Outils technologiques nécessaires

- Réseau pair-à-pair (P2P)
- Signature électronique
- Hachage cryptographique
- Horodatage
- Mécanisme de preuve de travail

Signature électronique

- Signature avec algorithme connu et clé secrète
  - Opération qui peut ne se faire qu'avec une information secrète
- Vérification avec algorithme connu et clé publique
  - N'importe qui peut vérifier la validité d'une signature
- Elliptic Curve Digital Signature Algorithm

Hachage cryptographique

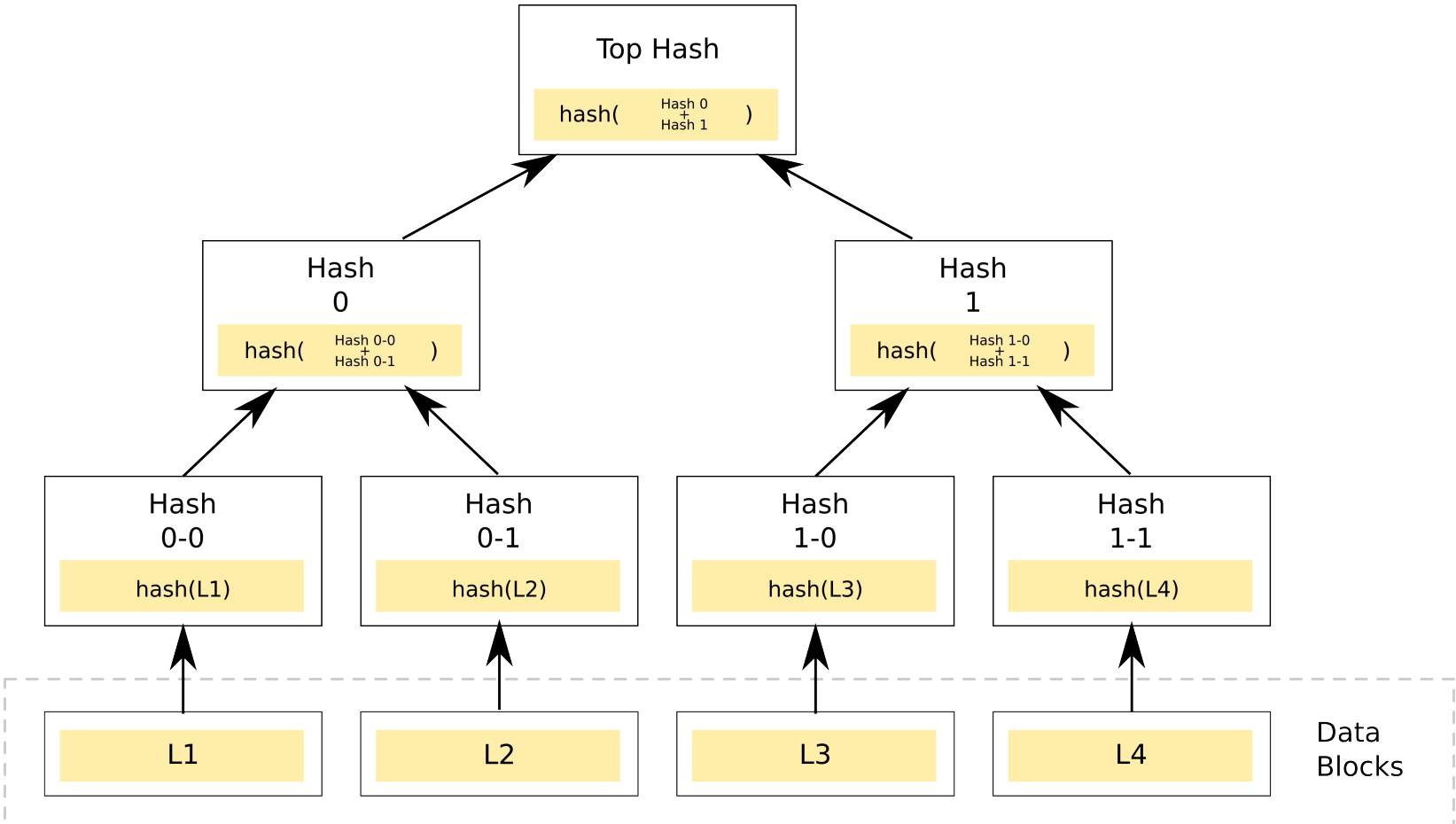
- Un haché est un condensé de message, obtenu par calcul à partir du message
- Message de longueur variable $\rightarrow$ condensé de longueur fixe : $h = H(m)$
- Selon un algorithme public, typiquement standardisé
- Le calcul doit être facile dans le sens direct :
  - Pour un m donné, $h = H(m)$ doit être facile à calculer
- Fonction à sens unique
  - «Impossible» de trouver un message correspondant à un haché donné
  - Faible probabilité de collision
- Fonction de hachage SHA-256

Empreinte d'horodatage (timestamp)

- Une empreinte d'horodatage lie cryptographiquement un contenu à un instant précis
- Permet de situer une action dans le temps
- Un service d'horodatage prend le haché d'un bloc qui contient une valeur de temps et diffuse le résultat publiquement

Arbre de Merkle

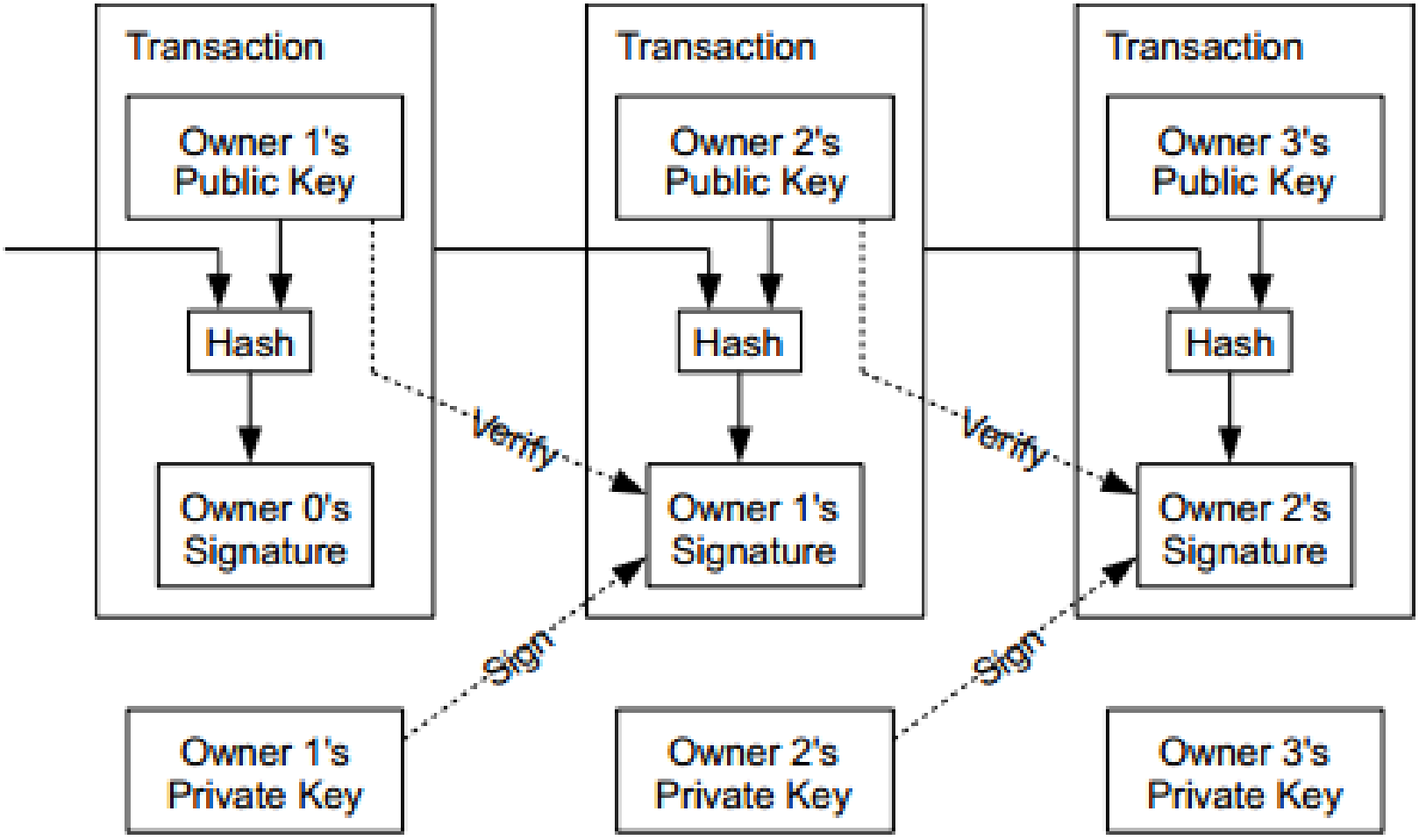
Chaque noeud qui n'est pas une feuille est étiqueté avec le haché des étiquettes (ou valeurs, pour les noeuds feuilles) de ses enfants



Transaction Bitcoin

- Les participants sont identifiés par des pseudonymes
- Un bitcoin est défini par une séquence de transactions signées numériquement, qui débute avec la création du bitcoin
- Celui qui possède le bitcoin le transfère à un autre usager en signant électroniquement le transfert
- Celui qui reçoit le bitcoin peut vérifier sa validité en regardant l'historique de possession du bitcoin
- Une transaction est irréversible

Chaîne de transactions



Source : N. Satoshi

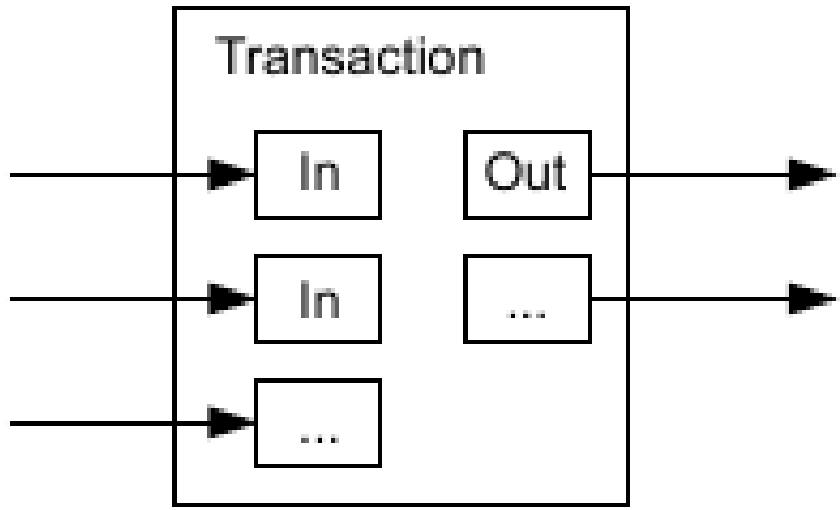
Composition d'une transaction

Débiter certains comptes pour créditer d'autres comptes

- Une transaction est composée d'un certain nombre d'entrées (inputs) et d'un certain nombre de sorties (outputs)
- Un input est une référence à un output d'une transaction antérieure
- Un output comporte un montant et la clé publique de l'adresse créditée

Transaction (2)

- Les transactions peuvent affecter simultanément plusieurs bitcoins
  - Inputs et outputs multiples
  - Les bitcoins peuvent ainsi être partagés ou combinés
- Une transaction peut provenir d'un seul input ou de la combinaison de plusieurs sources, et résulter en un ou deux outputs
  - Un pour le paiement et un pour le «change» retourné au payeur
  - Il peut aussi y avoir des frais de transactions



Transaction : validation

Pour faire la validation, Bitcoin utilise un langage de scriptage minimaliste qui automatise les vérifications. Le langage est non Turing-complet afin d'éviter les boucles infinies

- Lors de la validation d'une transaction, les scripts de chaque input sont exécutés, dans l'ordre : script d'output puis script d'input
- La transaction n'est validée que si le résultat est « vrai » pour tous les inputs

Blockchain

La Blockchain est un moyen d'établir un consensus rapidement et de façon fiable

- C'est un historique complet de toutes les transactions enregistrées
  - On y stocke les empreintes d'horodatage des transactions
- Protégée cryptographiquement contre la modification
- Maintenue et lisible par tous les noeuds du réseau P2P

Propagation par rumeur

Dans le réseau Pair-à-Pair

- Les transactions émises par un noeud sont diffusées à ses voisins
- Les voisins valident les transactions qu'ils reçoivent et les ajoutent progressivement dans un pool local avant de les transmettre à leurs propres voisins
- Les transactions validées sont ainsi diffusées de proche en proche à tous les noeuds du réseau, après avoir été re-vérifiées à chaque fois
- Les noeuds du réseau P2P sont semi-aléatoirement connectés entre eux
- Les informations (transactions, blocs, adresses des pairs, messages d'alerte) finissent pas atteindre tout le réseau

Finalisation de transaction

- Avant d'inscrire une transaction définitivement dans la Blockchain, le réseau effectue vérifie que :
  - les outputs référencées par les inputs existent et n'ont pas déjà été utilisés
  - l'auteur de la transaction est bien titulaire de l'adresse créditée dans ces outputs
  - la somme des montants figurant dans les outputs de la transaction est inférieure à la somme des montants des outputs référencés par les inputs
- Inscrire une transaction dans la Blockchain interdit toute future référence aux outputs désignés par les inputs de cette transaction
- On débite donc les comptes associés à ces outputs des montants de la transaction, et on crédite les comptes désignés par les outputs de la transaction des montants indiqués

Délai de prise en compte

- Une transaction est prise en compte instantanément par le réseau
- Elle est confirmée une première fois au bout de 10 minutes environ
- Chaque nouvelle confirmation renforce un peu plus la validité de la transaction dans le registre des transactions

Minage et preuve de travail

Le minage assure la gestion et la protection de la Blockchain. Il repose sur un mécanisme de preuve de travail

- Pour «fixer» un horodatage, il faut effectuer un calcul très-très lourd
- L'effort moyen requis augmente progressivement, de façon exponentielle
- La vérification est par contre très facile

Travail qui doit être effectué pour gérer la Blockchain

On doit calculer le haché du bloc en hachant deux fois l'ensemble formé de :

- Numéro de version du logiciel
- Haché de l'en-tête du bloc précédent (arbre de Merkle)
- Racine de l'arbre des transactions du bloc (qui est lui-même un haché indirect de l'ensemble des transactions du bloc)
- Horodatage (temps écoulé depuis le 1er janvier 1970 0 h, en secondes)
- Une valeur arbitraire de 32 bits (le *nonce*) qui répond aux exigences de difficulté

La difficulté

Le calcul du haché est rendu difficile en imposant des conditions sur le résultat

- Le *travail* consiste à trouver un bloc qui, haché deux fois avec la fonction de hachage cryptographique SHA-256, commence avec un certain nombre de bits zéro
- En pratique, on incrémente le «nonce» du bloc, encore et encore, jusqu'à trouver une valeur qui, lorsqu'on hache deux fois de suite le bloc, donne le nombre requis de zéros en préfixe
- Même en connaissant les hachés obtenus avec certains nonces, il est impossible de déterminer la valeur du haché avec un nouveau nonce sans ré-exécuter l'algorithme de hachage
- La validité d'un bloc se vérifie facilement : 1) calcul le haché deux fois ; 2) vérifie le nombre de zéros du préfixe

Protection de la Blockchain

- Pour une valeur donnée du nonce, la probabilité de calculer un haché respectant la difficulté est très faible : de nombreuses tentatives doivent être effectuées
- On ne peut donc trouver un nonce approprié que par essais successifs
- Ce système de preuve de travail et de chaînage des blocs par hachage rend toute modification de la Blockchain blocs impossible
- Un attaquant qui veut modifier une transaction dans un bloc donné doit recalculer son haché et celui de tous les blocs suivants
- Le temps nécessaire à une telle modification augmente très rapidement :
  - La *difficulté* (nombre de zéros requis) augmente avec le temps
  - Des nouveaux blocs s'ajoutent à la suite de la transaction

Propagation de la Blockchain

- Quand un noeud a construit un bloc valide (son haché satisfait la condition de difficulté), il le diffuse (rumeur) aux noeuds voisins, qui vérifient aussi sa validité avant de le rediffuser à leur tour
- À partir du nonce inclus dans l'en-tête, il est facile et rapide de vérifier la validité du bloc
- Les blocs valides sont diffusés de proche en proche à tout le réseau, après avoir été vérifiés à chaque fois, mais sans plus pouvoir être modifiés

Évolution de la difficulté

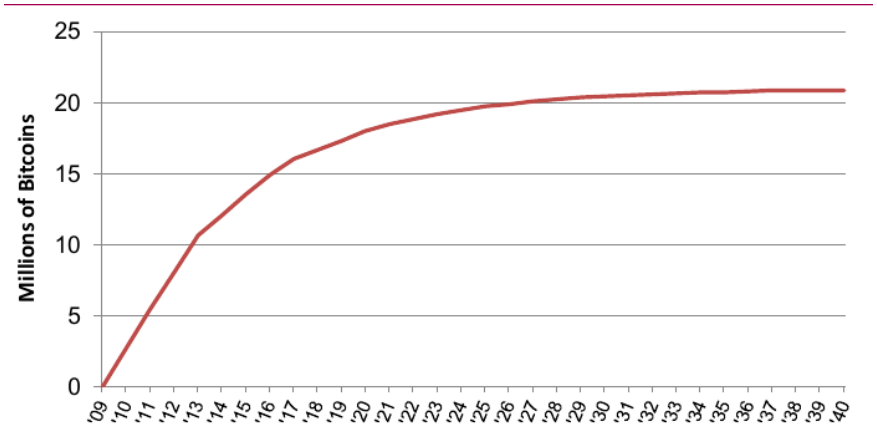
- Entre 2014 et 2016, le nombre moyen de nonces que chaque mineur devait tester entre chaque création de blocs est passé de 1 milliard à 200 milliards
- La difficulté est réajustée tous les 2016 blocs pour tenir compte de la puissance de calcul réelle du réseau et permettre en moyenne d'ajouter un bloc toutes les 10 minutes
  - La durée probable de calcul d'un haché valide est de 10 minutes pour l'ordinateur ou le groupe d'ordinateurs le plus puissant du réseau
  - La difficulté de trouver un haché est ainsi ajustée environ aux deux semaines

Récompenses

- Pour la création d'un nouveau bitcoin
- Pour la gestion de la Blockchain
- Avec le temps, les seules récompenses seront ces dernières

Création de bitcoins (minage)

- La première transaction dans un bloc est une transaction spéciale qui crée un nouveau bitcoin appartenant au créateur du bloc
- Les bitcoins sont émis lentement et régulièrement, de façon dégressive, jusqu'à atteindre un montant plafond de 21 millions dans quelques décennies

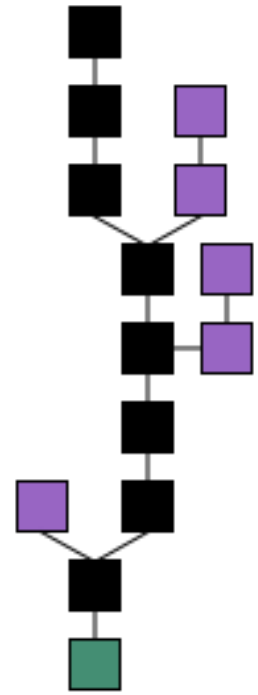


Système de récompense

- Un mineur fournit le travail pour assembler des transactions en « blocs »
- Le mineur inclut dans les blocs une transaction qui lui crédite un certain nombre de bitcoins créés à cet effet - sa récompense, ainsi que de frais de transaction proposés par les émetteurs
- La récompense ne sera effective que si le bloc est définitivement accepté dans la chaîne de blocs par les autres noeuds
- Un bloc peut contenir un nombre quelconque de transactions, typiquement entre 1000 et 2000, mais la taille $<$ 1 megaoctet
- Dans un bloc, les transactions sont stockées sous la forme d'un arbre de Merkle

Consensus

- L'horodatage d'un bloc est fixé par la preuve de travail : le bloc ne peut être changé sans refaire le travail
- Lorsque des blocs ultérieurs sont chaînés, changer le bloc demanderait en plus de refaire le travail pour tous les blocs ultérieurs
- Le consensus majoritaire est la plus longue chaîne, celle qui demande le plus de travail à produire
- Si la majorité de la capacité de traitement est contrôlée par des noeuds honnêtes, la chaîne honnête croîtra le plus rapidement et gagnera contre les chaînes malhonnêtes



Minage en pratique

- Le calcul consiste à effectuer un très grand nombre de fois le même calcul de hachage avec des données différentes, il se prête bien au calcul parallèle
- CPU
- GPU
- FPGA
- Circuit intégré dédié (ASICs)
- Fermes de calcul (par ex., en Islande)
- Estimé en 2016 : 1,46 terawatt-heures par année pour le minage

Pour l'utilisateur

Vous voulez essayer ?

- Accès au réseau Internet
- Une application «open source» pour utiliser les Bitcoin
  - Github : https ://github.com/bitcoin/bitcoin
- Créer son porte-monnaie Bitcoin (qui contient surtout les clés privés)
- Avec l'application, on peut se connecter au réseau Bitcoin et créer des comptes
- On peut effectuer des transactions de nos comptes vers d'autres comptes
- Mais attention : un présumé millionnaire du Bitcoin, Jered Kenna, aurait perdu environ son porte-monnaie et ainsi US$200 000 en 2010 après avoir reformaté un disque dur !

En terminant : je passe le chapeau