

Bitcoins et chaînes de blocs

par Michel Gagné
2019-09

Plan de la présentation

- Pourquoi toute cette folie!
- Qu'est-ce qu'une cryptomonnaie
- Qu'est-ce qu'une chaîne de blocs
- Quelques concepts informatiques
- La chaîne de blocs en détail
- Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin

Pourquoi toute cette folie!

En 1439, Gutenberg a inventé l'imprimerie, ce qui a réduit le coût de production d'un document par un facteur de 100

- ▶ journaux - démocratie
- ▶ instruction - science, technologie, richesse, puissance

Pourquoi toute cette folie!

En 1989, Tim Berners-Lee a inventé le Web, ce qui a réduit le coût de production d'un document à presque rien

- ▶ essor d'Internet, disponibilité de l'information, transformation des industries (commerce, journaux, musique, courrier, taxi, etc.)
- ▶ mais, si le Web peut distribuer l'information, il ne peut pas transférer une valeur

Pourquoi toute cette folie!

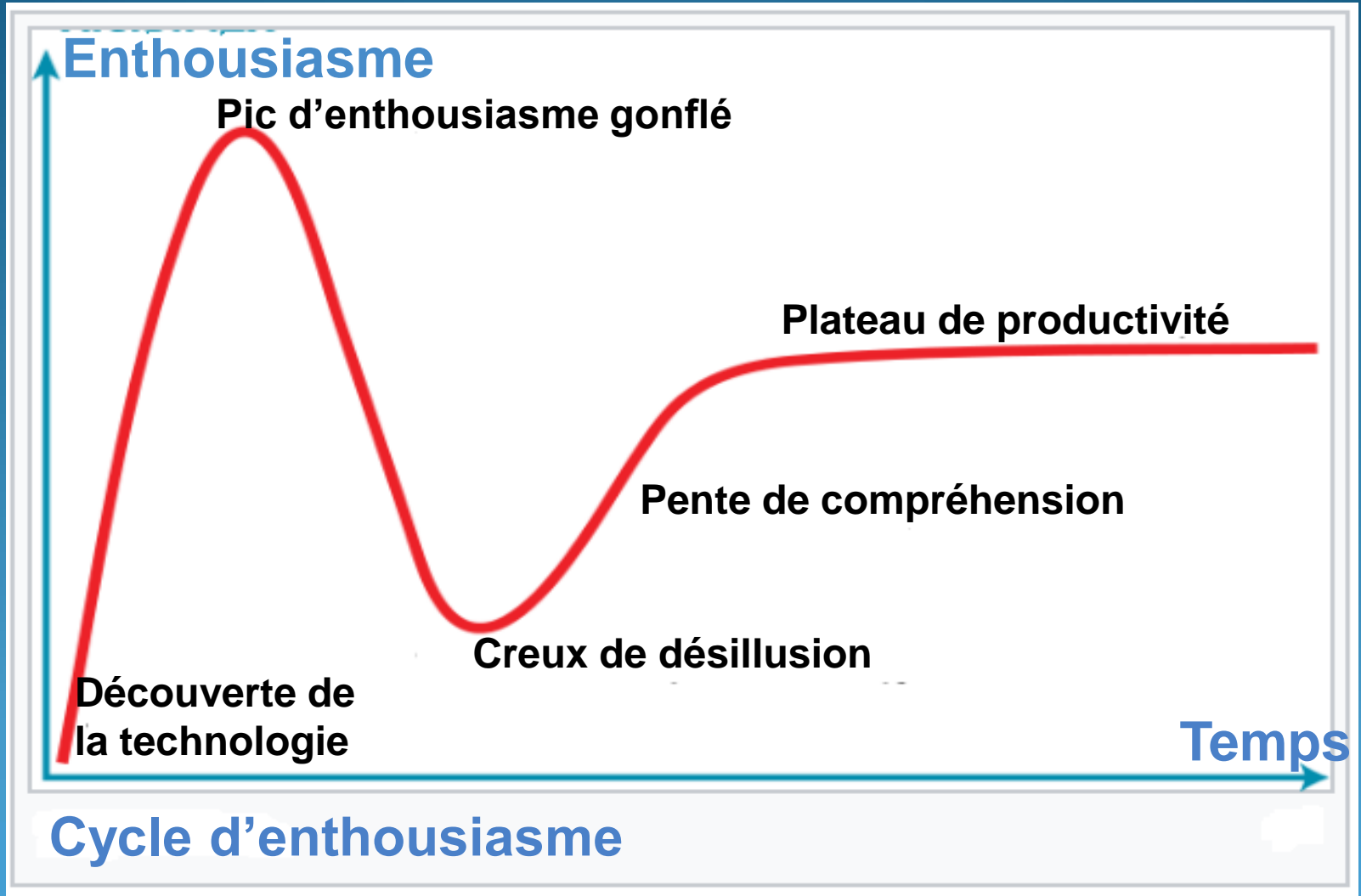
En 2009, Satoshi Nakamoto a créé un outil qui permet

- de transférer une valeur sur Internet
 - de créer une monnaie indépendante d'un gouvernement.
- Certains y ont vu une grande révolution.

Impact

- Eric Schmidt, CEO de Google : Le bitcoin est une réalisation cryptographique remarquable et la création de quelque chose qui ne peut pas être dupliqué dans le monde digital aura des répercussions énormes.
- John McAfee : Vous ne pouvez stopper une chose comme le bitcoin. Il sera partout et le monde devra s'y adapter. Les gouvernements du monde entier devront s'y adapter.

Cycle d'enthousiasme



Plan de la présentation

- Pourquoi toute cette folie!
- ➔ • Qu'est-ce qu'une cryptomonnaie
- Qu'est-ce qu'une chaîne de blocs
- Quelques concepts informatiques
- La chaîne de blocs en détail
- Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin

Définition de monnaie

Une monnaie est un outil financier qui possède trois fonctions :

1. Mesurer la valeur d'une chose
2. Permettre l'acquisition d'une chose
3. Permettre l'accumulation de valeur (pour usage futur)

Définition de cryptomonnaie

Une cryptomonnaie est

- une monnaie
- stockée sur un support électronique (habituellement Internet)
- basée sur des techniques de cryptographie

Historique

- 1998 : Wei Dai décrit le concept de cryptomonnaie
- 1998 à 2009 : plusieurs échecs de cryptomonnaies
- 2009 : Satoshi Nakamoto lance le bitcoin qui deviendra la première cryptomonnaie fonctionnelle
- Depuis 2011 : + de 2800 cryptomonnaies plus ou moins basées sur le bitcoin
(<https://coinmarketcap.com/fr/>)

Historique

Qui est Satoshi Nakamoto?

On ne le sait pas. C'est probablement un groupe de personnes spécialisées dans divers domaines.

Satoshi Nakamoto ou le groupe derrière ce nom ne contrôle pas le bitcoin.

Avantages des cryptomonnaies

- Indépendantes des gouvernements.
- Absence d'intermédiaires : frais de transfert presque nuls et transferts rapides.
- Pas de frais d'échange de devises.

Désavantages des cryptomonnaies

- Faible acceptation.
- Volatilité.
- Consommation d'énergie.

Plan de la présentation

- Pourquoi toute cette folie!
- Qu'est-ce qu'une cryptomonnaie
- ➔ • Qu'est-ce qu'une chaîne de blocs
- Quelques concepts informatiques
- La chaîne de blocs en détail
- Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin

Définition de registre

Un registre est une base de données dans laquelle sont consignés des nombres, des noms ou des faits dont on doit garder trace :

- votre relevé bancaire;
- vos placements chez votre courtier;
- le cadastre du Québec;
- les testaments enregistrés auprès des notaires.

Définition de chaîne de blocs

Un registre doit être protégé

- de la perte;
- de la falsification.

Définition de chaîne de blocs

- Un registre
- numérique et distribué sur un réseau
- sans organe de contrôle
- avec informations à conserver groupées en blocs chaînés
- sécurisé par des techniques cryptographiques

Plan de la présentation

- Pourquoi toute cette folie!
- Qu'est-ce qu'une cryptomonnaie
- Qu'est-ce qu'une chaîne de blocs
- ➔ • Quelques concepts informatiques
- La chaîne de blocs en détail
- Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin

Fonction de hachage cryptographique



Caractéristiques d'une fonction de hachage :

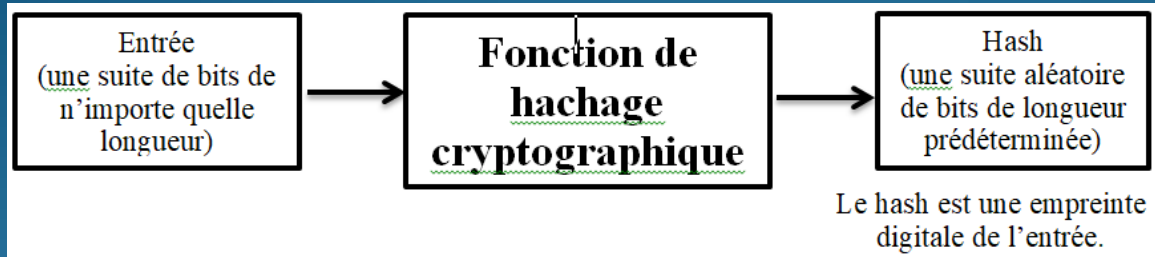
- la fonction s'exécute rapidement, c'est-à-dire qu'on peut calculer rapidement la sortie pour une entrée donnée;
- il est impossible d'inverser la fonction, c'est-à-dire qu'on ne peut pas calculer une entrée pour une sortie donnée.

Preuve de travail

Une preuve de travail est :

- une démonstration;
- que quelqu'un a fait un travail, par exemple, un grand nombre de calculs mathématiques.

Preuve de travail



On peut obtenir une preuve de travail en demandant de trouver une entrée dont le hash commence par un certain nombre de zéros :

- un hash de la forme $0xxx...xxx$ requiert 2 exécutions de la fonction;
- un hash de la forme $00xxx...xxx$ requiert 4 exécutions;
- un hash de la forme $000xxx...xxx$ requiert 8 exécutions;
- un hash de la forme $0..(10)..0xxx...xxx$ requiert 1000 exécutions;
- un hash de la forme $0..(20)..0xxx...xxx$ requiert 1 million d'exécutions;
- un hash de la forme $0..(30)..0xxx...xxx$ requiert en 1 milliard d'exécutions.

Signature à deux clés

Jusqu'en 1978, l'expéditeur et le destinataire d'un message devaient posséder une *clé secrète* pour chiffrer ou déchiffrer un message.

En 1978, une grande découverte a été faite en Californie : le couple *clé privé / clé publique*.

Signature à deux clés

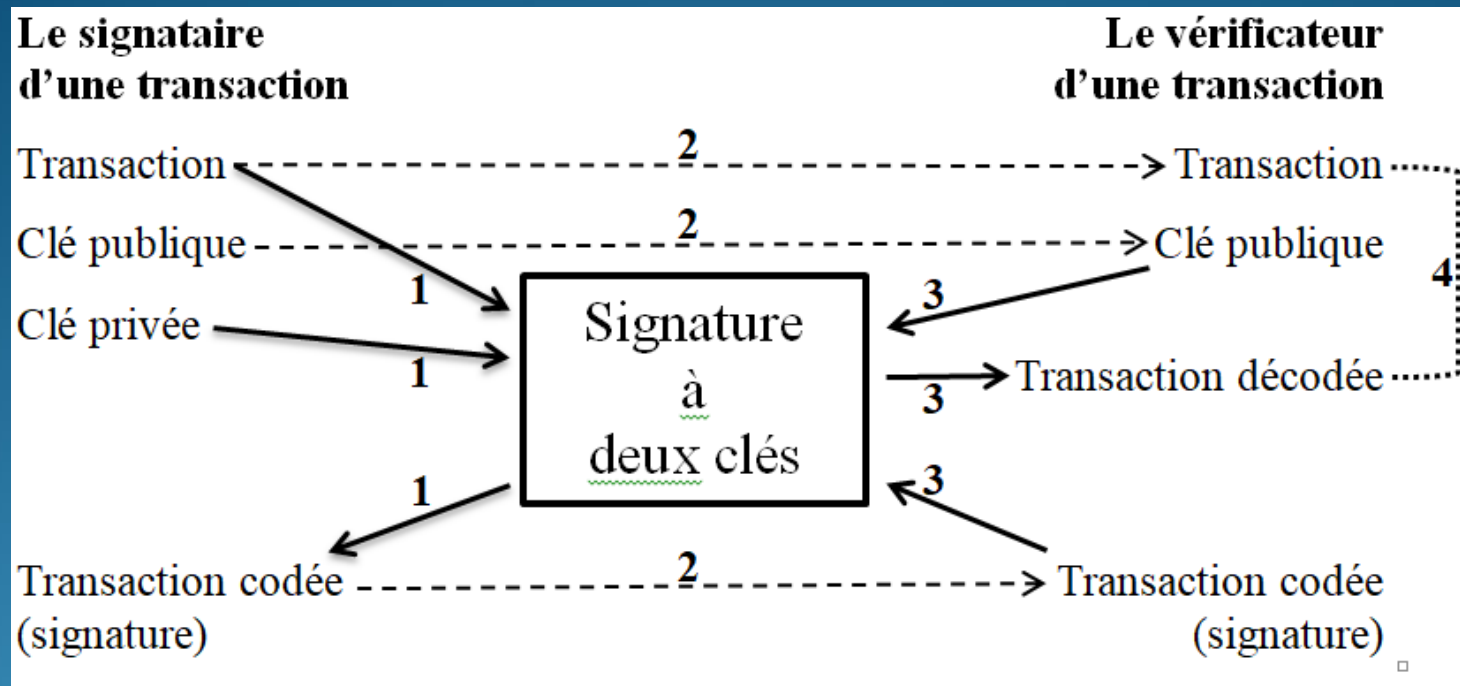
Un couple *clé privée / clé publique* est un couple de nombres qui permet de chiffrer et de signer des transactions. Dans un tel couple,

- la clé privée est uniquement connue de son propriétaire
- et la clé publique est connue de tout le monde.

Un couple *clé privée / clé publique* possède les caractéristiques suivantes :

- un message chiffré avec la clé privée peut être déchiffré avec la clé publique;
- un message déchiffrable avec la clé publique a nécessairement été chiffré avec la clé privée.

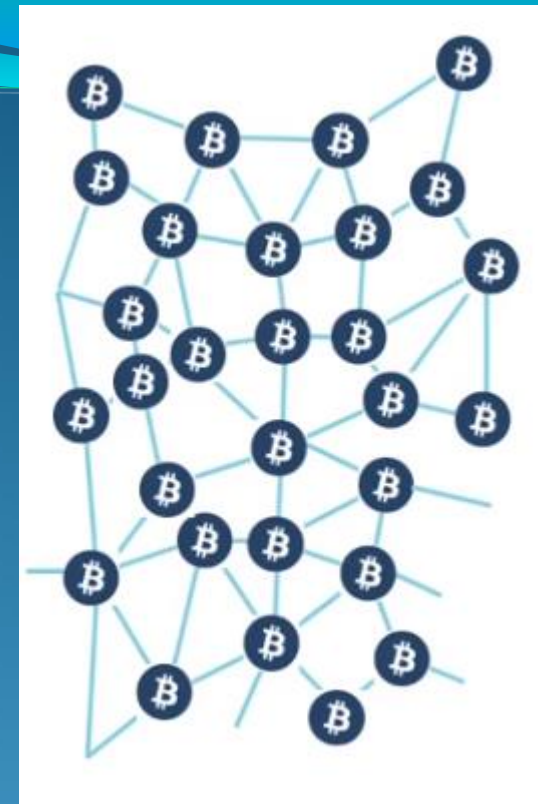
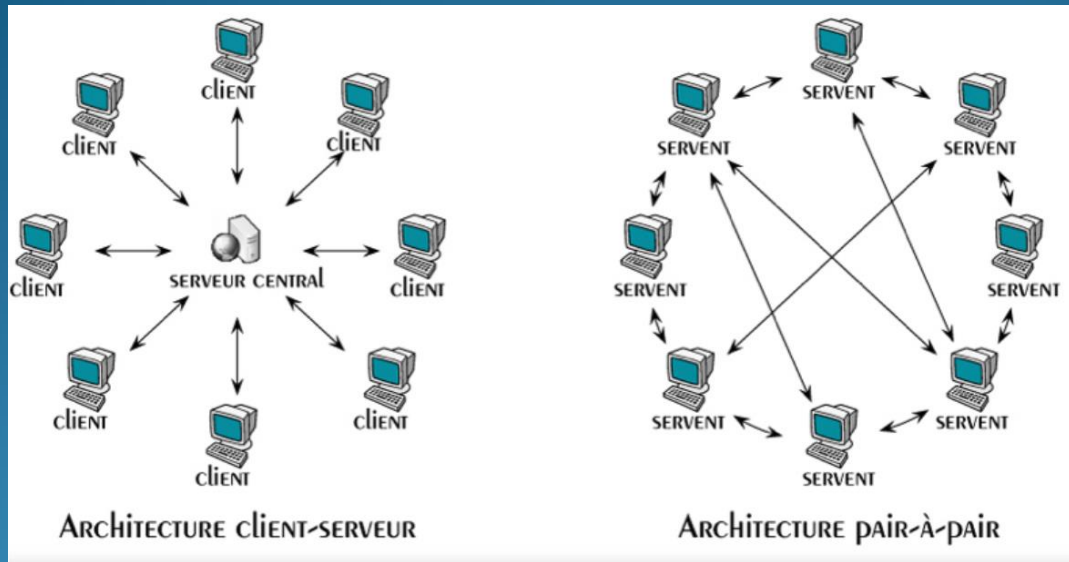
Signature à deux clés



Caractéristiques d'une signature à deux clés :

- le programme de signature à deux clés peut reconstruire la transaction originale au moyen de la clé publique;
- il est impossible de produire la transaction codée qui sera décodée par la clé publique sans avoir la clé privée.

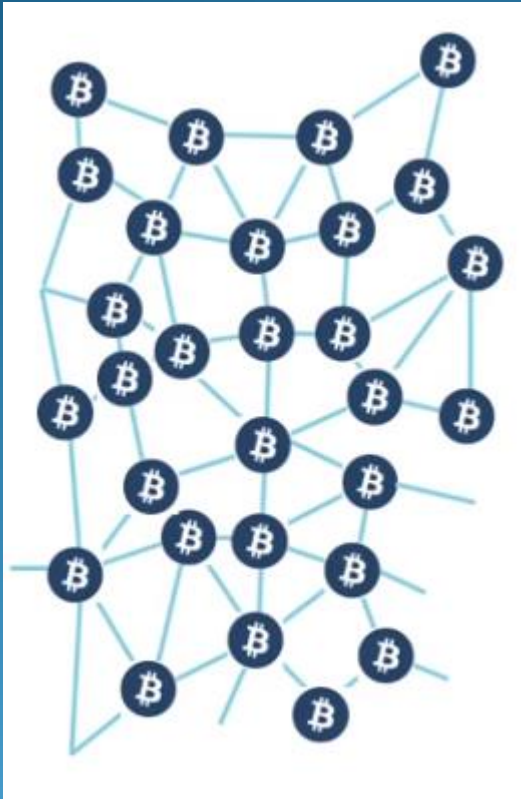
Réseau pair-à-pair



L'architecture client-serveur est vulnérable à la défaillance du serveur central.

L'architecture pair-à-pair est résistante à la perte d'un ou de plusieurs serveurs. De plus, elle permet l'addition ou le retrait dynamique de serveurs.

Réseau pair-à-pair Bitcoin



En 2019, le réseau bitcoin contient :

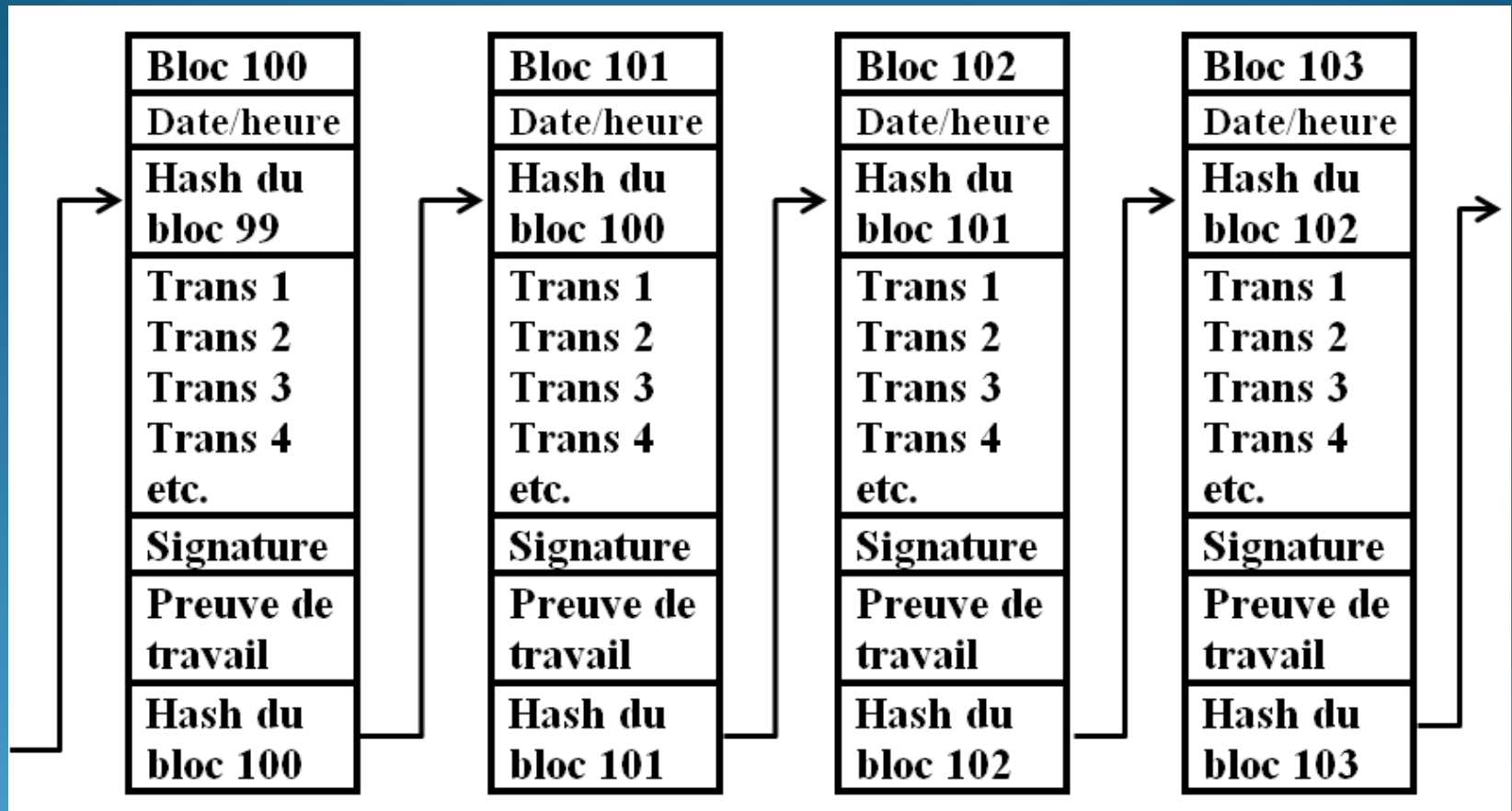
- plus de 100 000 nœuds
- avec une capacité de calcul 100 000 fois plus grande que les 500 plus gros supercalculateurs réunis.

Plan de la présentation

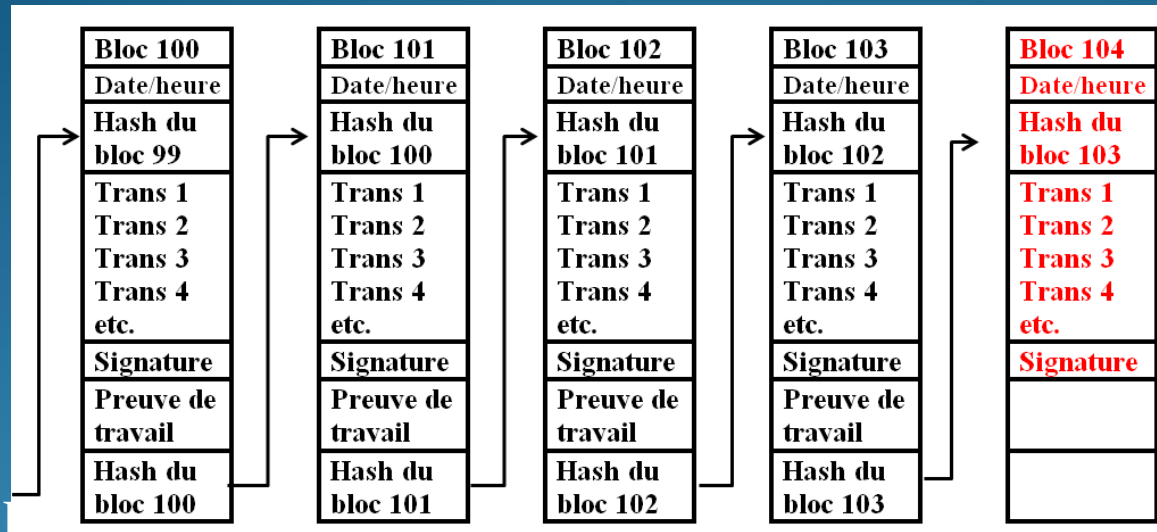
- Pourquoi toute cette folie!
- Qu'est-ce qu'une cryptomonnaie
- Qu'est-ce qu'une chaîne de blocs
- Quelques concepts informatiques
- La chaîne de blocs en détail
- Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin



La chaîne de blocs



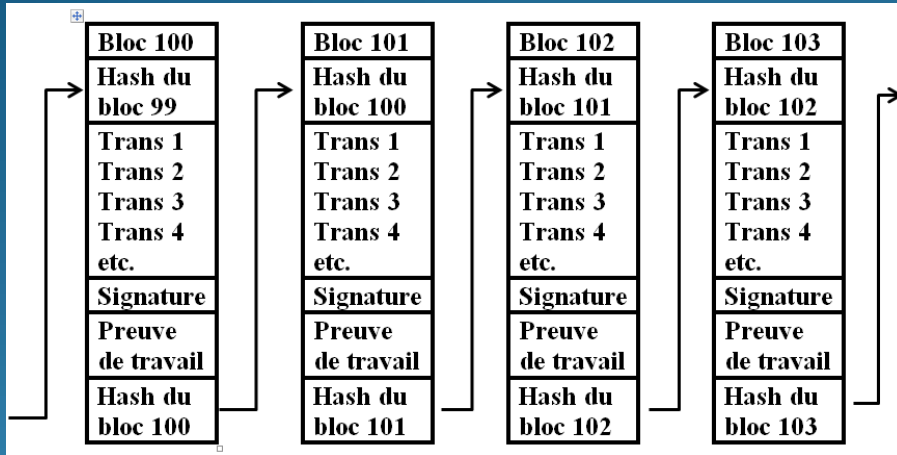
La chaîne de blocs – les mineurs



- il écrit les champs Bloc 104, Hash du bloc 103, Trans, Signature;
- ensuite, il doit trouver une preuve de travail telle que le hash de tout le bloc (incluant la preuve de travail commence par 30 zéros (ou un autre nombre de zéro défini pour que le temps de travail de la communauté soit d'environ 10 minutes)).

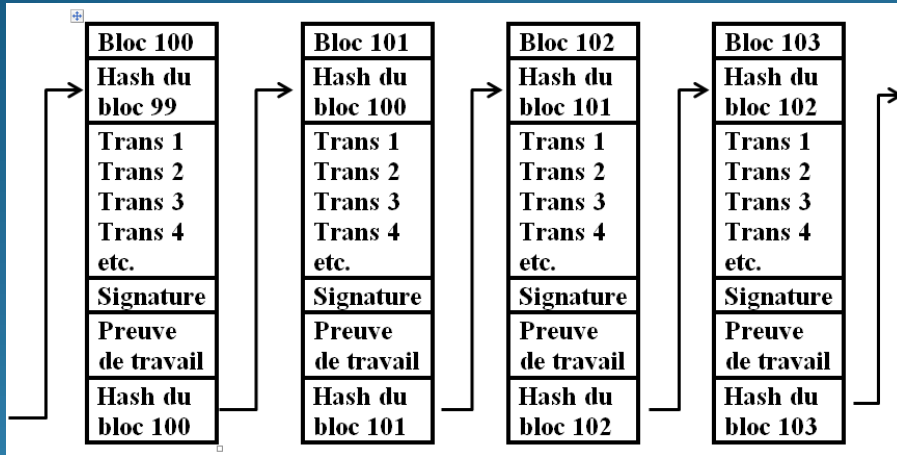
Lorsqu'un mineur a trouvé une bonne preuve de travail, il complète la construction du bloc et le communique aux autres mineurs qui l'ajoutent à la chaîne.

La chaîne de blocs – la sauvegarde



La sauvegarde est assurée par l'architecture pair-à-pair du système.


La chaîne de blocs – l'intégrité



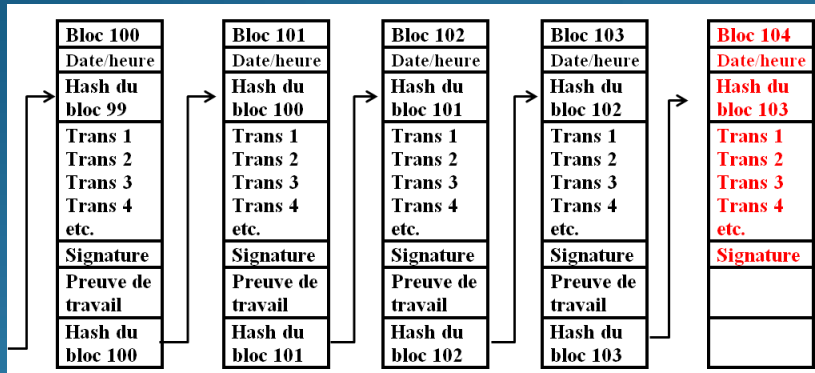
L'intégrité est assurée par les hash et les preuves de travail :

- un pirate qui changerait la Trans 2 du Bloc 101 devrait trouver une nouvelle preuve de travail pour que le Bloc 101 soit valide, ce qui produirait un nouveau hash pour le Bloc 101 et rendrait le Bloc 102 invalide, etc. jusqu'au dernier bloc;
- de plus, toutes les 10 minutes, la chaîne s'allonge d'un nouveau bloc;
- un pirate ne peut avoir assez de force de calcul pour faire cela.

Plan de la présentation

- Pourquoi toute cette folie!
- Qu'est-ce qu'une cryptomonnaie
- Qu'est-ce qu'une chaîne de blocs
- Quelques concepts informatiques
- La chaîne de blocs en détail
-  • Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin

Le bitcoin



Mais qu'est-ce qui motive les mineurs à assembler des blocs?

La récompense lors de l'ajout d'un bloc à la chaîne :

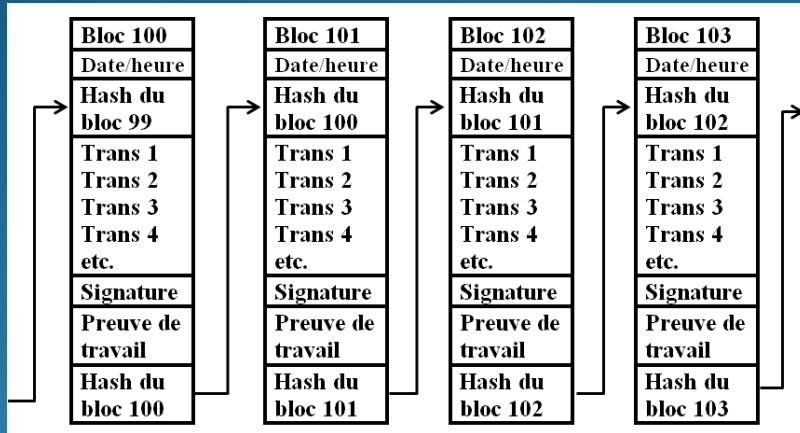
- 12.5 bitcoins donnés par le système Bitcoin.

Plan de la présentation

- Pourquoi toute cette folie!
- Qu'est-ce qu'une cryptomonnaie
- Qu'est-ce qu'une chaîne de blocs
- Quelques concepts informatiques
- La chaîne de blocs en détail
- Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin



Applications sur la chaîne de blocs



On a vu que la chaîne de blocs du bitcoin est un registre infalsifiable.

En plus d'y enregistrer des transferts de bitcoins, on pourrait y enregistrer d'autres informations qui doivent être conservées sécuritairement, par exemple;

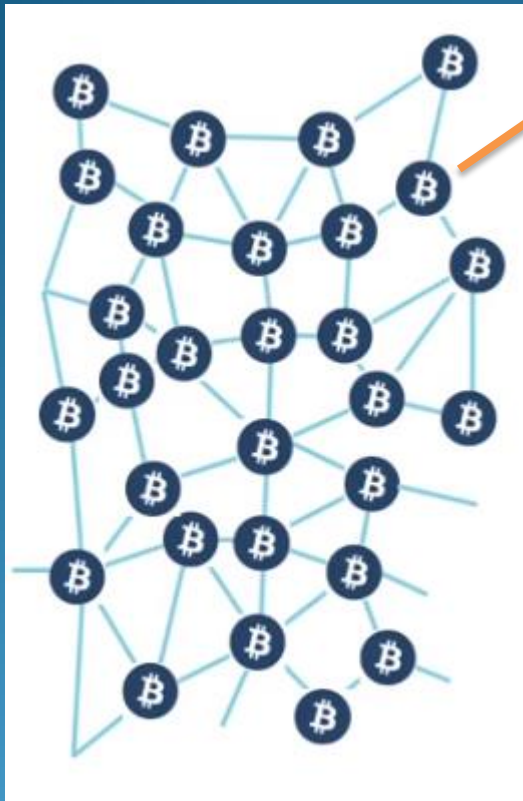
- les diplômes d'une université;
- les signatures de contrats;
- les signatures de testaments;
- la traçabilité des aliments;
- les billets d'un spectacle.

Plan de la présentation

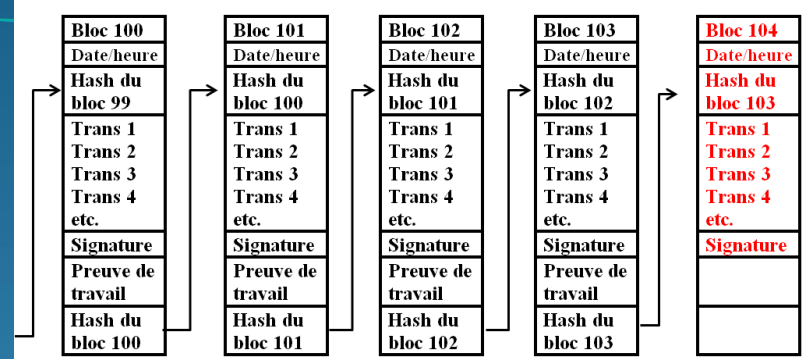
- Pourquoi toute cette folie!
- Qu'est-ce qu'une cryptomonnaie
- Qu'est-ce qu'une chaîne de blocs
- Quelques concepts informatiques
- La chaîne de blocs en détail
- Le bitcoin
- Applications de la chaîne de blocs
- Que pouvez-vous faire avec le bitcoin



Devenez mineur



Vous

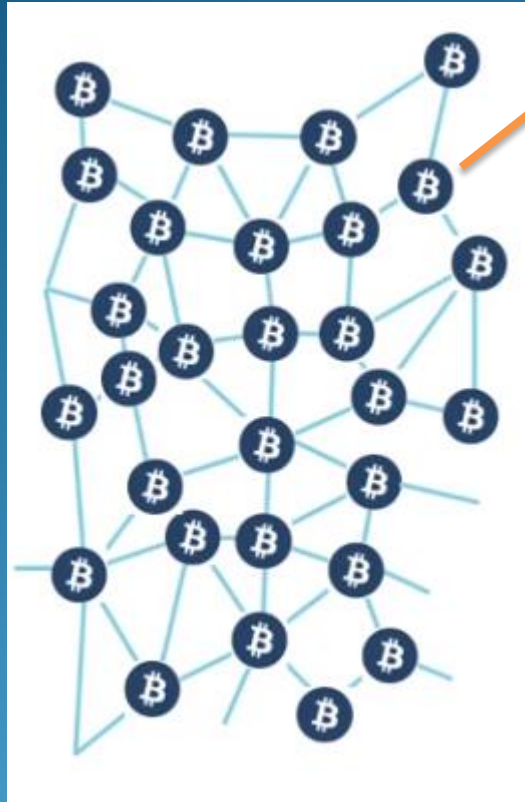


Devenez mineur ou membre d'un club de minage.

Site pour devenir membre :
nicehash.com

Vous pourrez ainsi accumuler des bitcoins en échange du travail que fournira votre ordinateur.

Devenez spéculateur



Place de
marché

Vous



Portefeuille
personnel

Devenez spéculateur en achetant des bitcoins avec des dollars sur une place de marché.

Vous devrez alors décider

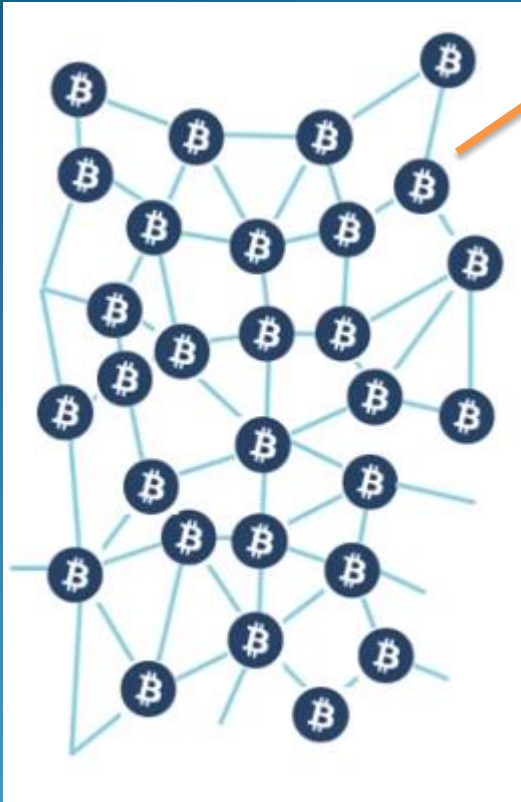
- si vous laissez vos bitcoins dans la place de marché
- ou si vous les conservez dans votre portefeuille personnel

Achetez des produits avec vos bitcoins

Vous



Site marchand
acceptant les
bitcoins



- Sur un site marchand affichant un bouton indiquant que les paiements en bitcoins sont acceptés,
- cliquez sur le bouton indiquant un paiement en bitcoins;
 - faites votre paiement comme pour une carte de crédit.

Payez une rançon à un pirate



Si vous avez déjà des bitcoins, vous pouvez payer avec votre portefeuille.

Si vous n'avez pas de bitcoins, vous pouvez en acheter sur une place de marché et payer le pirate.

Mais le mieux c'est de ne pas payer le pirate, de réinstaller Windows et de copier vos fichiers à partir de votre sauvegarde.

Bibliographie (YouTube)

1. *Comment fonctionne un blockchain - Expliqué simplement*, 1 vidéo de 6 minutes,
https://www.youtube.com/watch?v=SSo_EIwHSd4
2. *Conférence TED, How the blockchain is changing money and business*, 1 vidéo de 19 minutes,
<https://www.youtube.com/watch?v=Pl8OlkkwRpc>
3. *Blockchain : Comment ça marche ?*, 1 vidéo de 35 minutes,
<https://www.youtube.com/watch?v=SccvFbyDaUI>
4. *Blockchain Révolution : comprendre le phénomène Blockchain*, 7 vidéos totalisant 6 heures 52 minutes,
https://www.youtube.com/watch?v=SM4X7ZlsPf4&list=PL5cpoUO2rGHO8ocqB-_yzQ3PJLo13vtDJ