FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Blockchain, Bitcoin: On vous explique tout !

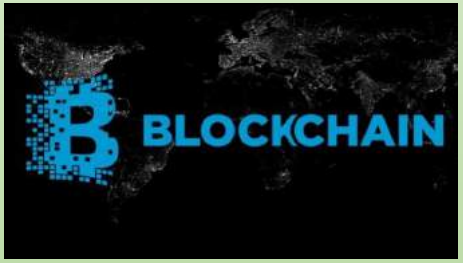
Présenté par : Alain Wagner B. Gest.
10 octobre 2019

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Chaîne de blocs, Bitcoin: On vous explique tout !

La question que tout le monde se pose :

- Faut-il investir dans le Bitcoin ?
- N'est-il pas trop tard ?
- Mais au fait, le Bitcoin qu'est-ce que c'est ?
- Pourquoi l'associe-t-on toujours à la Blockchain ?



FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et Chaîne de blocs

Le problème actuel:

- Pour emprunter de l'argent vous devez passer par un intermédiaire qui va voir que son argent est passé de chez lui chez vous.
- Il existe un lien de confiance.
- Comment se passer de cet intermédiaire ?

Solution:

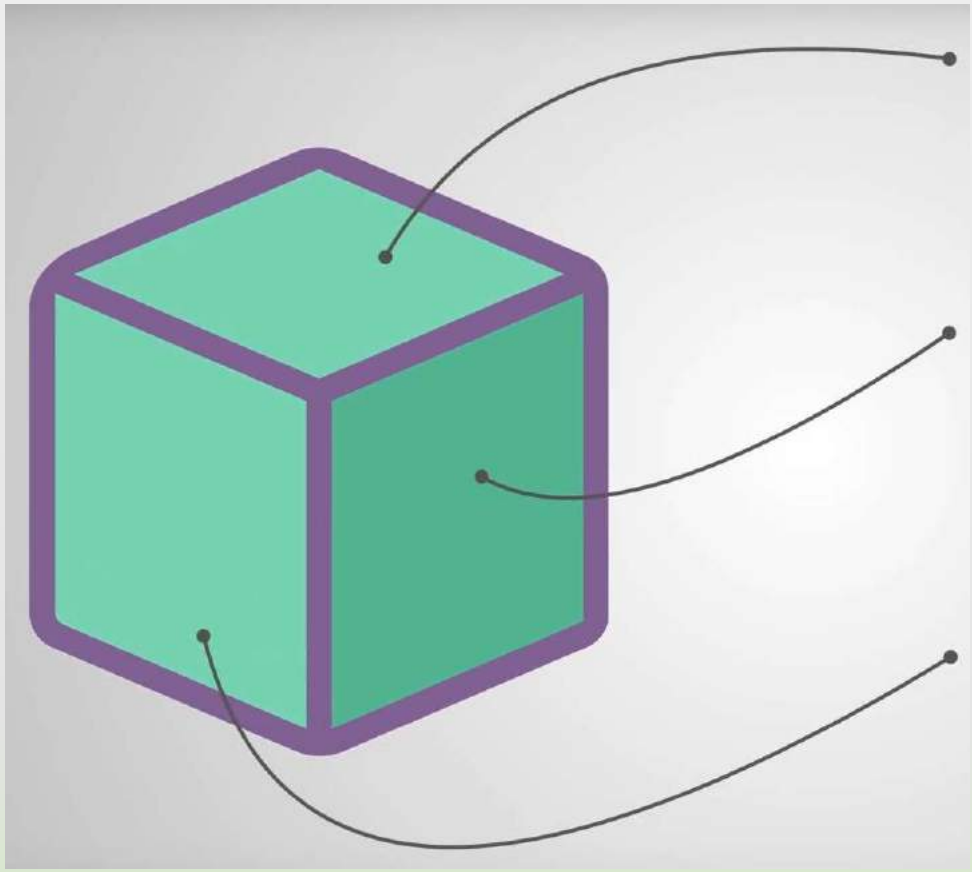
- Se défaire du seul registraire de transaction en faisant en sorte que chaque ordinateur du réseau (des milliers) conserve la trace de la transaction.
- Création de la ***chaîne de blocs***.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Qu’est-ce qu’une chaîne de blocs ?

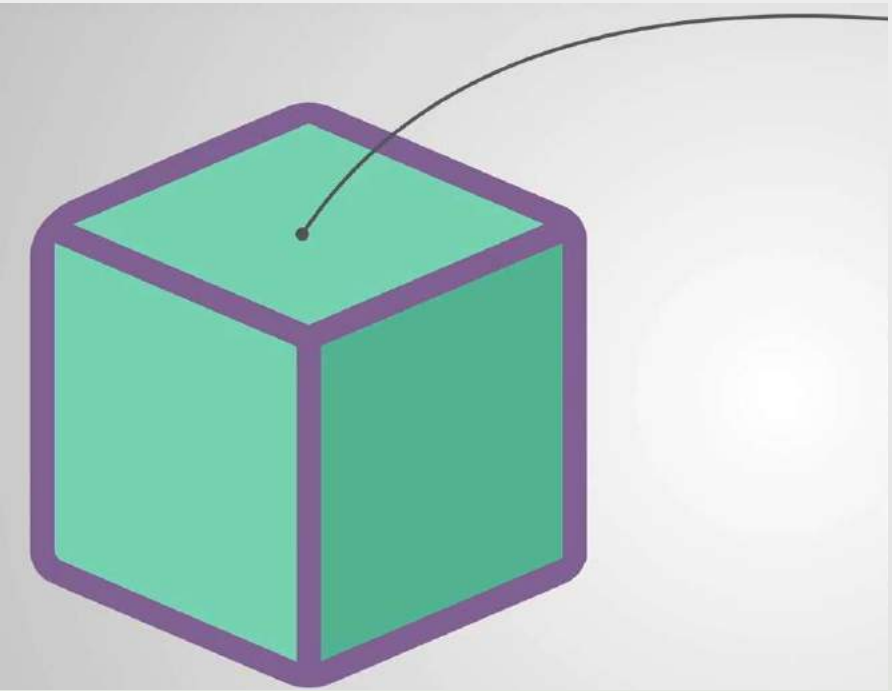
FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Contenu d'un bloc



FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Données dans un bloc



Données

De: 

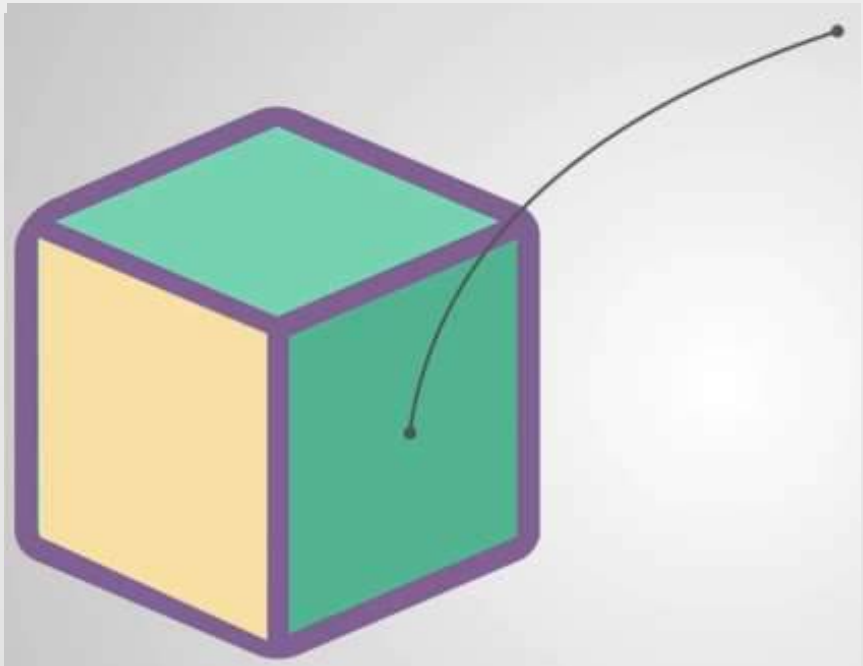
A: 

Montant: 

Exemple de données pour le Bitcoin

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Données dans un bloc



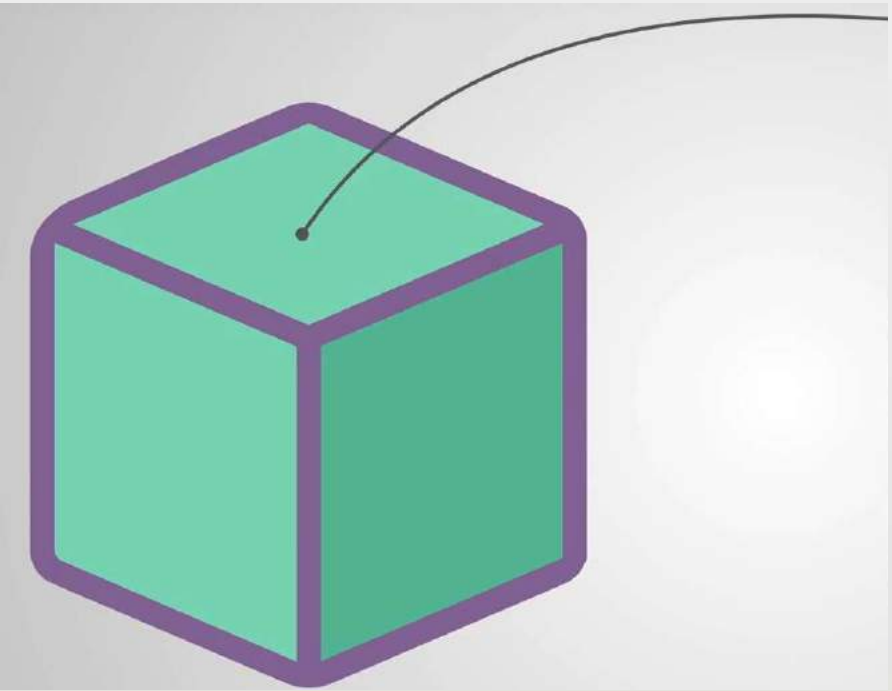
Hash

3602470b25278c5f3ead34cfc6ae607adc111196

Signature digitale

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

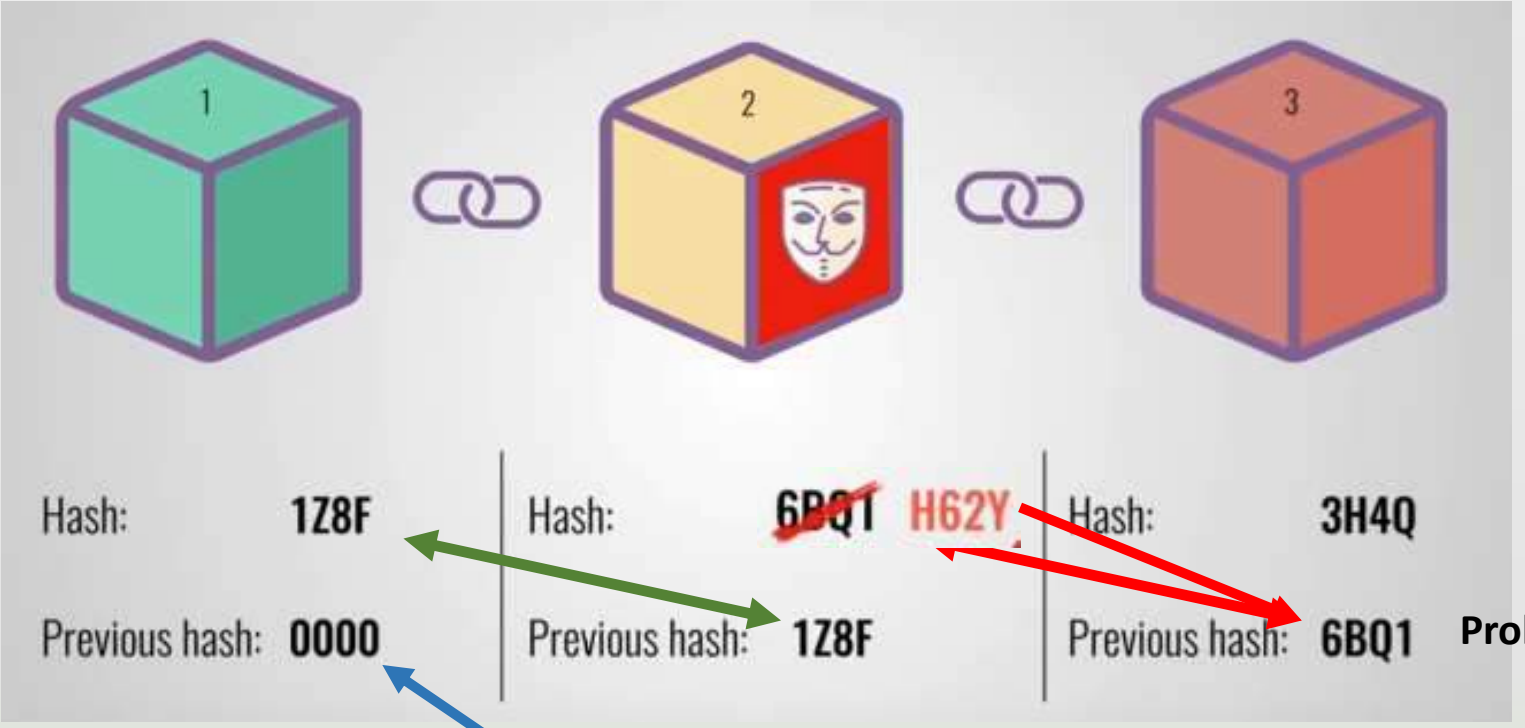
Données dans un bloc



Hash du bloc précédent

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

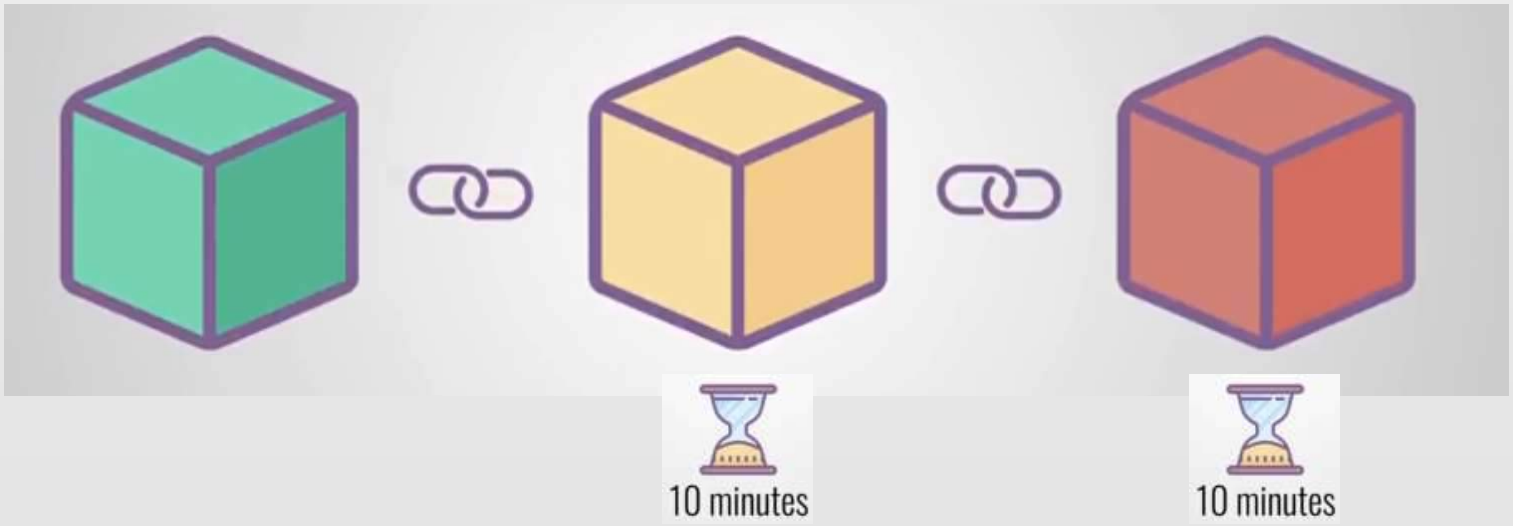
La chaîne de blocs



FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

La chaîne de blocs

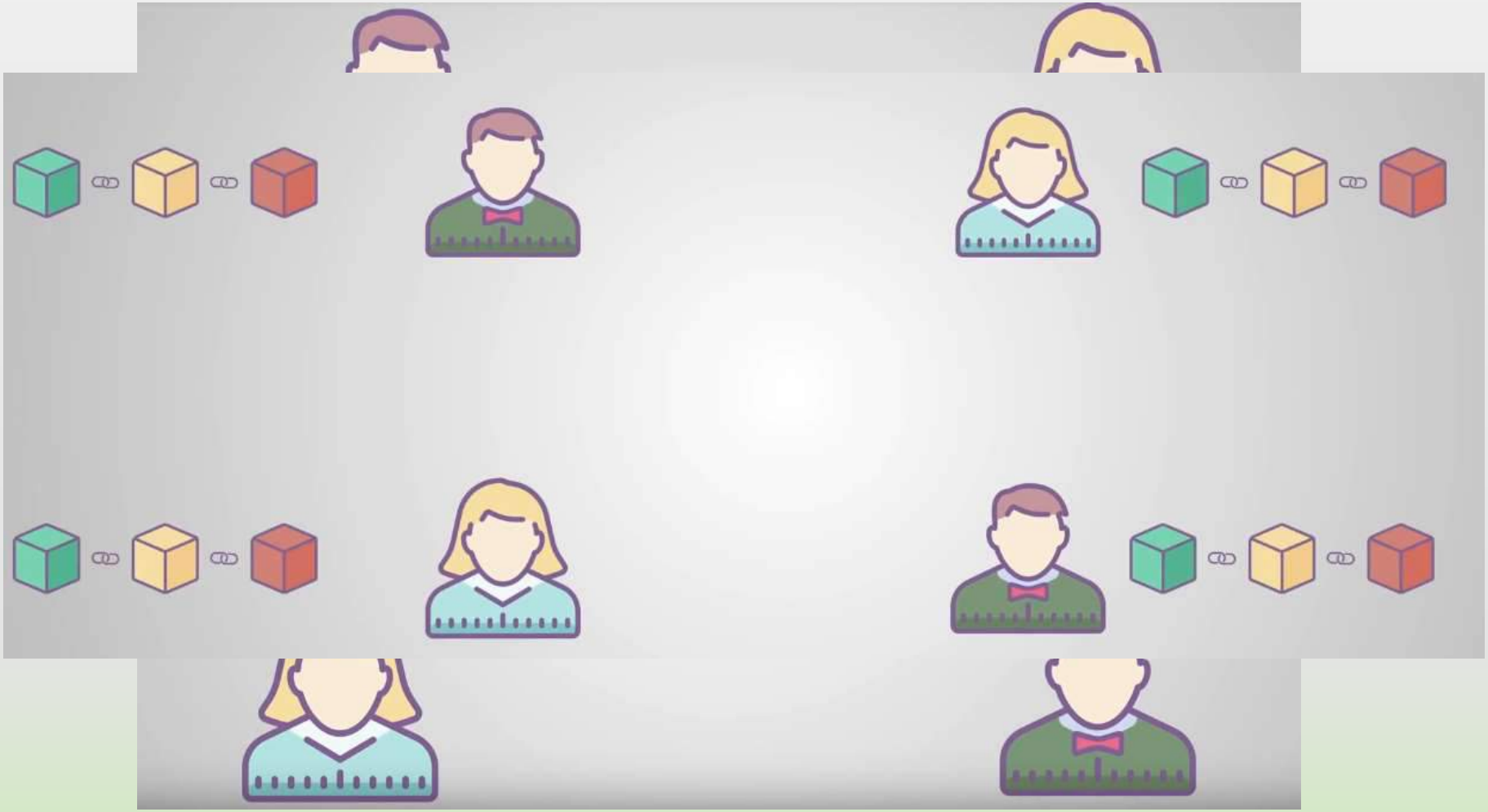
Preuve du travail exécuté



Mécanisme de ralentissement pour l'émission des nouveaux blocs
Dans le cas de Bitcoin: 10 minutes

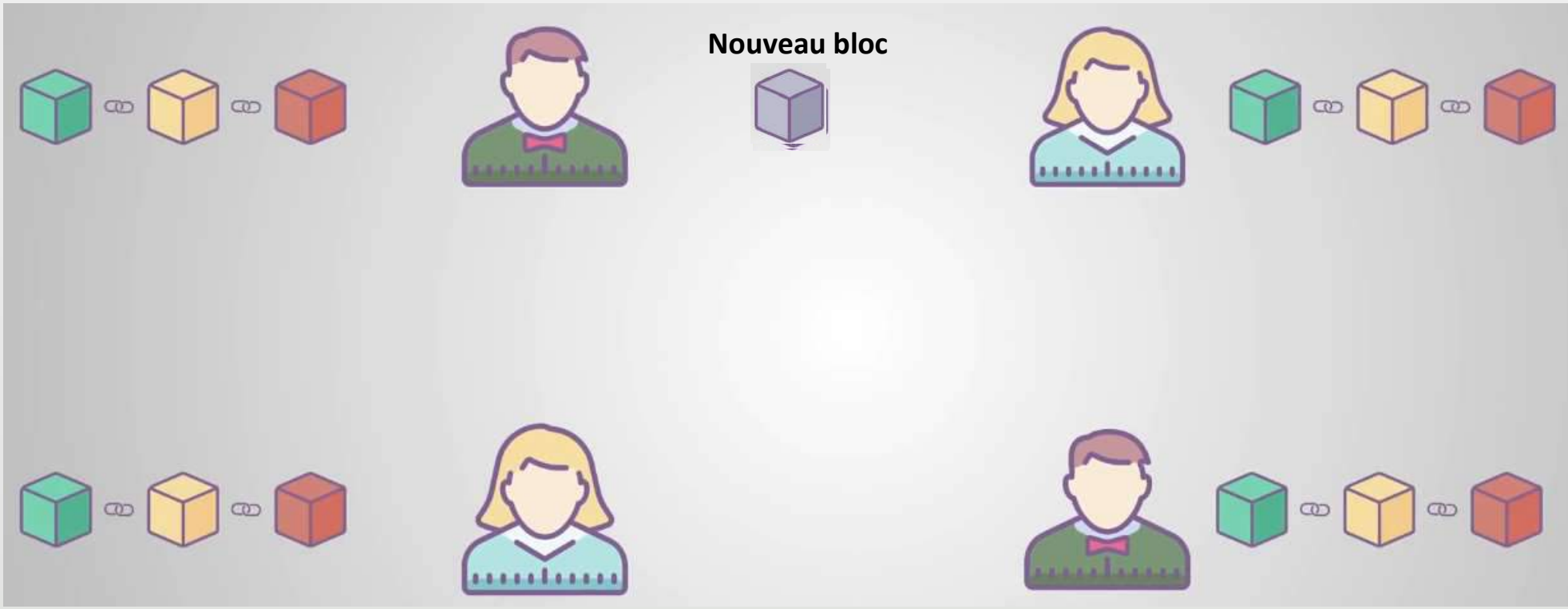
FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Le réseau



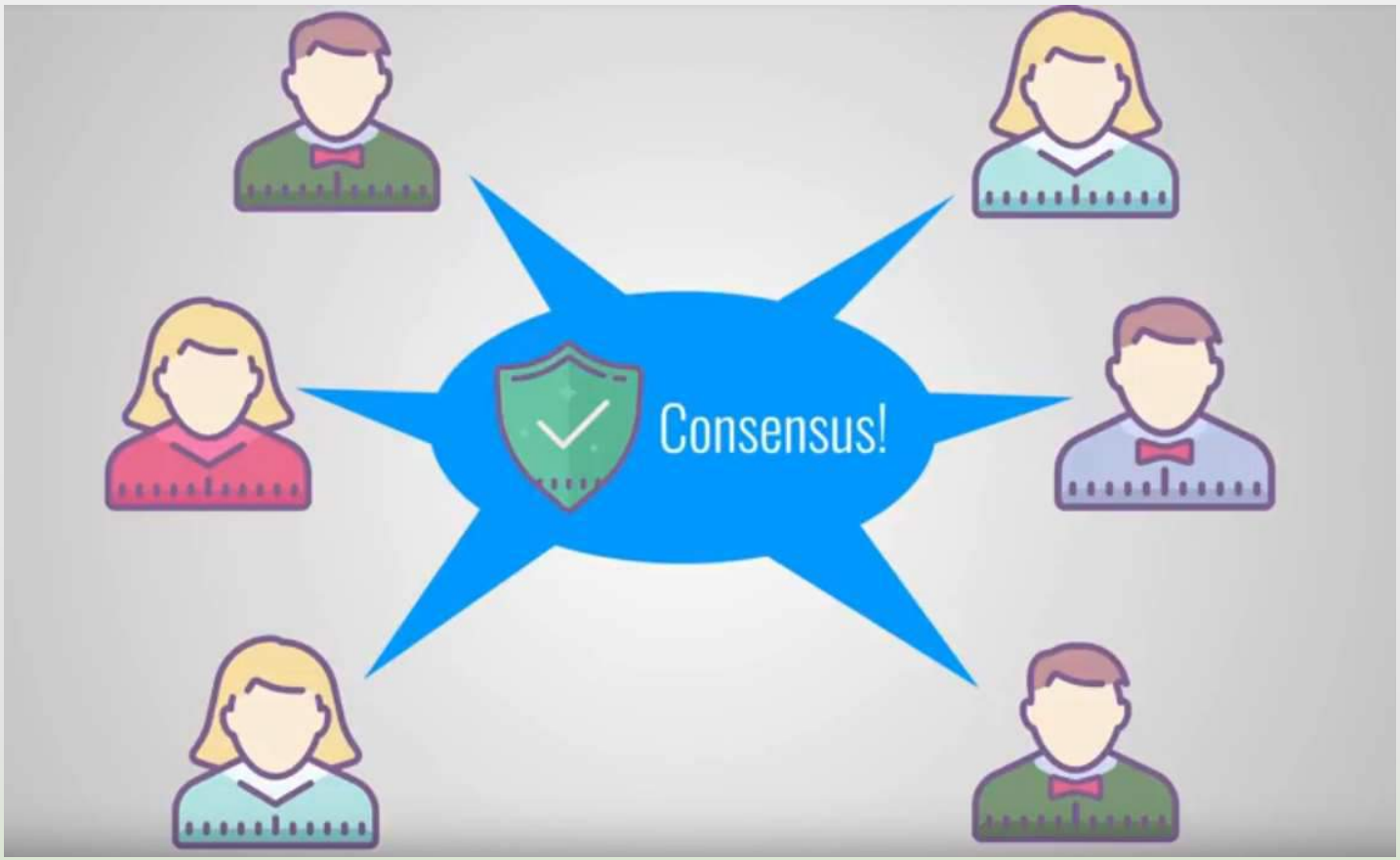
FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Création d'un nouveau bloc



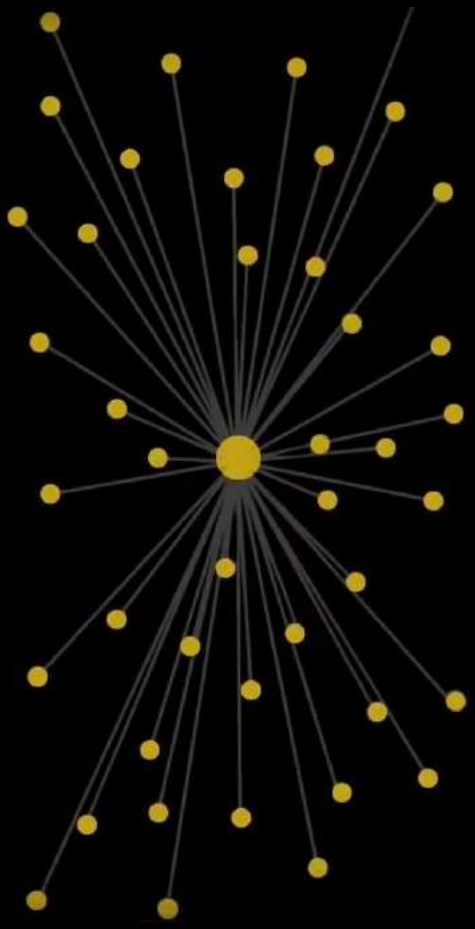
FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Données dans un bloc

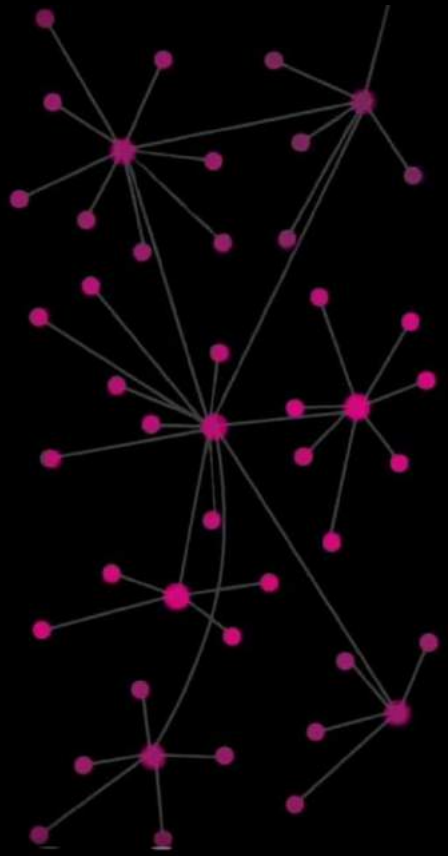


FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

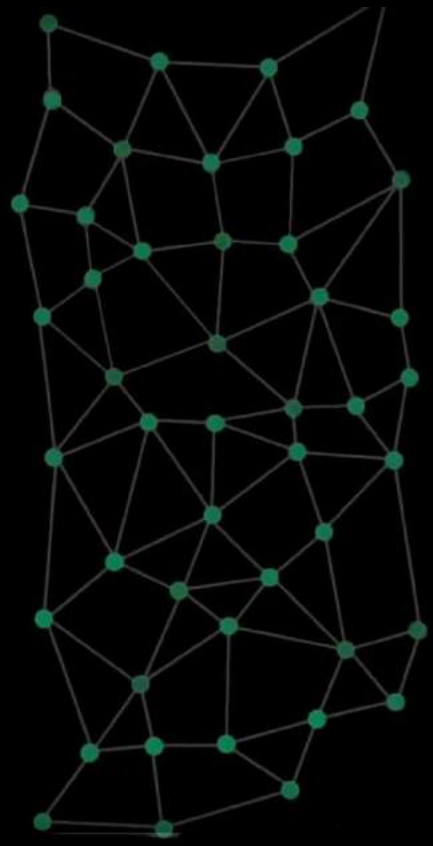
Centralisé



Décentralisé



Distribué



FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

- **Bitcoin** (de l'anglais *bit* : unité d'information binaire et *coin* : pièce de monnaie) est, d'une part, une monnaie virtuelle de type monnaie cryptographique e, d'autre part, un système de paiement égal à égal (peer to peer).

- Conçu et présenté par une personne sous le pseudonyme de Satoshi Nakamato qui annonce son système en 2008.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

Fonctionnement

- Bitcoin s'appuie sur un logiciel. Dans ce logiciel, les bitcoins sont créés conformément à un protocole qui rétribue les agents qui ont traité des transactions.

- Ces agents mettent à contribution leur puissance de calcul informatique afin de vérifier, de sécuriser et d'inscrire les transactions dans un registre virtuel, appelé la ***chaîne de blocs***.

- L'entité de base de Bitcoin s'appelle un bloc. Les blocs sont reliés en une chaîne, d'où le nom, « chaîne de blocs » ou « **blockchain** » en anglais.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

Fonctionnement

- Pour chaque nouveau bloc accepté, l'activité de vérification-sécurisation-enregistrement, appelée minage, est rémunérée par des bitcoins nouvellement créés et par les frais des transactions traitées.

- En tant que monnaie ou commodité, les bitcoins peuvent être échangés contre d'autres monnaies ou commodités, biens ou services.

- Le taux d'échange de la cryptomonnaie est fixé principalement sur des places de marché spécialisées et fluctue selon la loi de l’offre et de la demande.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

Unité de compte

- L'unité de compte du Bitcoin est le Bitcoin. Son émission est limitée à 21 millions d'unités, chacune divisible jusqu'à la huitième décimale.

- Il est à noter que Bitcoin n'est pas la seule cryptomonnaie, car des crypto monnaies concurrentes à bitcoin ont été crées, à savoir Bitcoin XT, Bitcoin Unlimited, Bitcoin Classic, etc.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

Distribution

- Le système fonctionne sans autorité centrale, ni administrateur unique, mais de manière décentralisée grâce au consensus de l'ensemble des nœuds du réseau.

- Bitcoin est la plus importante monnaie cryptographique décentralisée avec une capitalisation supérieure à 200 milliards de dollars début 2017.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

- Les bitcoins sont émis lentement et régulièrement de façon dégressive jusqu'à atteindre un montant maximal de 21 millions.

- La valeur du bitcoin s’apprécie à une vitesse folle. Si vous aviez acheté pour 100 $ de bitcoin en 2011, votre investissement vaudrait aujourd’hui plus de deux millions de dollars.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

Pourquoi le prix du bitcoin explose-t-il soudainement ?

- Parce que le marché découvre les caractéristiques uniques du bitcoin.
- Le fait qu'il est sécuritaire, que la quantité finale de bitcoins qui sera en circulation (21 millions) est déjà connue, tout comme le rythme d'émissions des nouveaux bitcoins (toutes les dix minutes). Tout cela est prévisible.
- À l'opposé du système monétaire actuel où les banques centrales peuvent émettre des nouveaux dollars à perpétuité et créer de l'inflation (qui fait perdre de la valeur à votre argent).

Bitcoin et chaîne de blocs

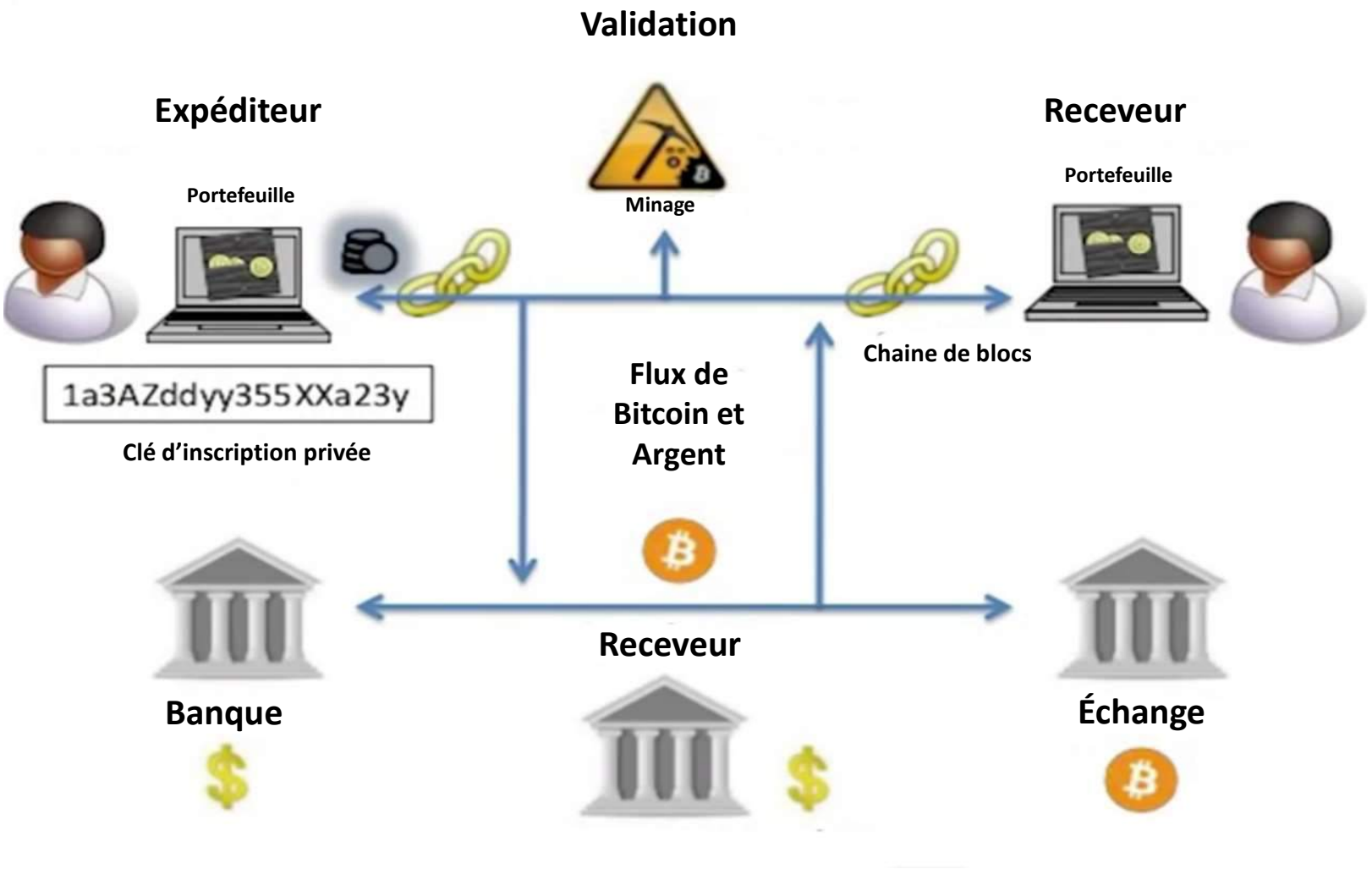
- Il faut comprendre une chose : Bitcoin n'est pas encore près de remplacer les PayPal, Interac et cartes de crédits.

- C'est d'abord un instrument financier.

- En ce moment, c'est surtout une valeur refuge qui concurrence l'or et le dollar. Son adoption ou non comme monnaie d'échange a peu d'importance pour déterminer sa valeur.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment ça marche



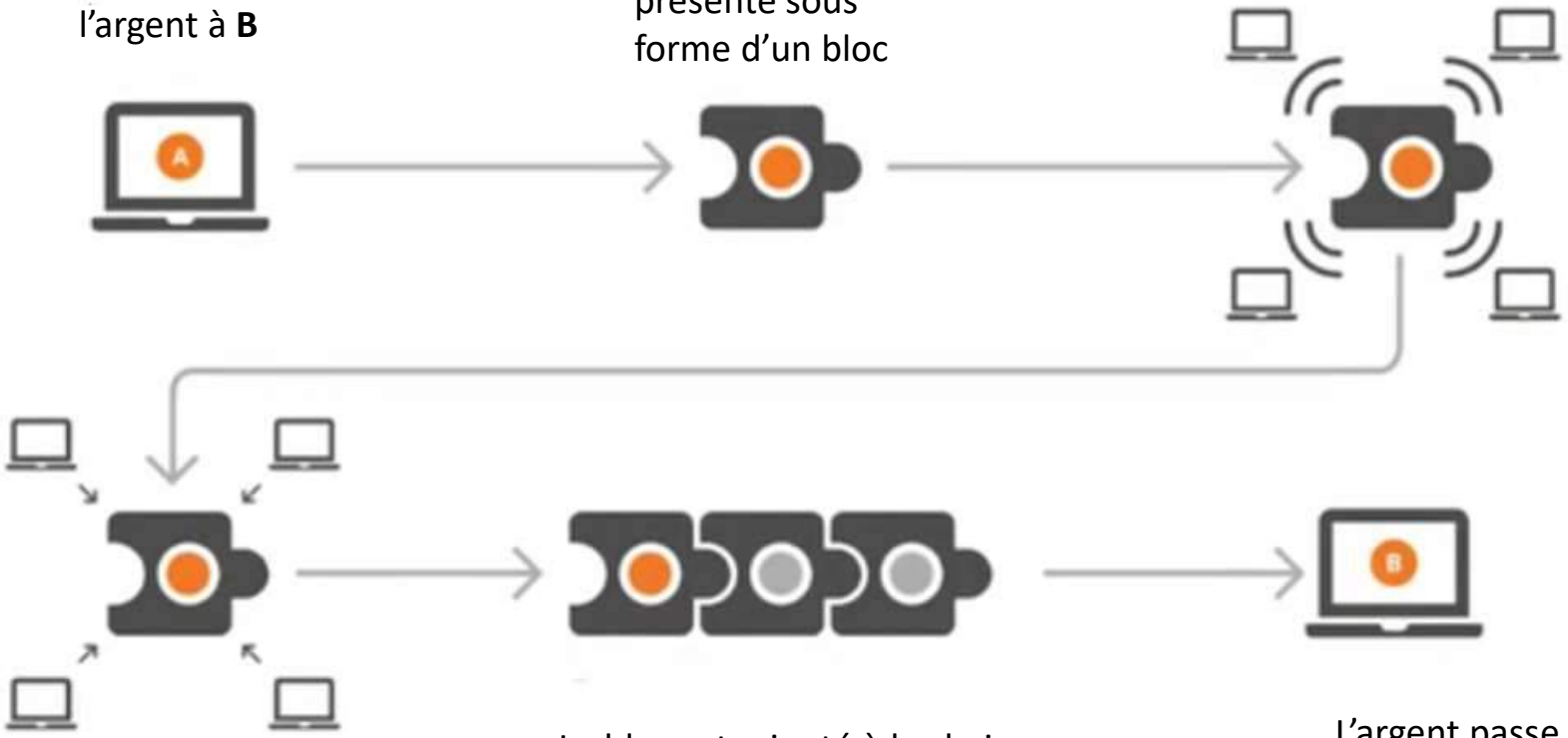
FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

FONCTIONNEMENT

A veut envoyer de l'argent à **B**

La transaction se présente sous forme d'un bloc

Le bloc est distribué à tout le réseau



Le réseau valide la transaction

Le bloc est rajouté à la chaine, qui assure une trace ineffaçable de la transaction

L'argent passe de A à B

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- Les gens envoient des bitcoins sur le réseau bitcoin tout le temps, mais à moins que quelqu'un ne garde un enregistrement de toutes ces transactions, personne ne pourrait garder une trace de qui a payé quoi. Le réseau bitcoin s'en occupe en collectant toutes les transactions effectuées pendant une période donnée dans une liste, appelée un bloc.

- C'est le travail des mineurs de confirmer ces transactions et de les écrire dans un grand livre général. Ce grand livre général est une longue liste de blocs, connus sous le nom de «***chaîne de blocs***». Il peut être utilisé pour explorer toute transaction effectuée entre n'importe quelle adresse bitcoin, à n'importe quel point du réseau.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- En principe n'importe quel ordinateur peut agir pour valider la transaction mais le système est rendu tellement gros et lourd que maintenant nous avons affaire à des fermes d'ordinateurs pour exécuter le travail.

- Le principe est que ceux qui utilisent leurs ordinateurs pour valider des transactions touchent une redevance pour leur travail. C'est donc devenu une véritable industrie.

- Le Blockchain c'est ça; une fois la transaction approuvée, elle est intégrée dans des milliers d'ordinateurs et elle est donc infalsifiable car il est impossible d'aller modifier l'information dans ces milliers d'ordinateurs.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- Comment pouvons-nous être sûrs que la chaîne de blocs reste intacte et qu'elle n'est jamais altérée ?
- C'est là que les mineurs entrent en jeu. Lorsqu'un bloc de transactions est créé, les mineurs le soumettent à un processus.
- Ils prennent l'information dans le bloc et appliquent une formule mathématique, la transformant en quelque chose d'autre.
- Ce quelque chose d'autre est une séquence apparemment plus courte et aléatoire de lettres et de chiffres connus sous le nom de hash.
- Ce hash est stocké avec le bloc, à la fin de la chaîne de blocs.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- Comme son nom l'indique (un peu), le minage s'apparente en fait à une recherche plus qu'à une production à proprement parler. Pour être rémunéré, un mineur doit trouver un bloc. Pour ce faire, il doit exécuter l'algorithme de hachage de nombreuses fois jusqu'à ce qu'il tombe sur un résultat qui montre de façon incontestable qu'il a bien trouvé un bloc.

- Un bloc contient actuellement environ 300 transactions. Chaque bloc possède un identifiant unique (son nom en quelque sorte) déterminé automatiquement par un algorithme en fonction des transactions qu'il contient.

- Pour qu'un mineur trouve un bloc, il faut que le hash de ce bloc commence par un certain nombre de zéros. Plus la difficulté est forte, plus le nombre de zéros par lequel le hash doit commencer est grand.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- Les ordinateurs des mineurs utilisent donc l'identifiant du bloc, y ajoutent un incrément, puis exécutent de nombreuses fois l'algorithme SHA-256 en augmentant l'incrément chaque fois. Ils font cela jusqu'à ce qu'ils trouvent un résultat qui commence par le bon nombre de zéros.

- Lorsque cela est fait, ils envoient leur découverte aux autres nœuds du réseau. Ceux-ci constatent que le bloc est bien valide et l'ajoutent à leur chaîne de bloc. Le mineur est alors rémunéré par le réseau qui émet une certaine somme prévue d'avance.

- La récompense est actuellement de 25 BTC par bloc trouvé. Comme il existe un nombre maximum de Bitcoins en circulation, la récompense baisse régulièrement. Elle est divisée par deux tous les 210.000 blocs trouvés.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- En soumettant au réseau l'identifiant du bloc, le numéro de l'incrément et le hash commençant par le bon nombre de zéros, le mineur apporte la preuve de son travail et des ressources qu'il a mises en œuvre pour miner le bloc. Le réseau lui octroie sa récompense et le bloc trouve sa place en bout de la chaîne de bloc.

- La notion de preuve de travail est centrale dans l'invention du Bitcoin. Sans elle, il ne serait pas possible d'inciter les mineurs à investir dans une grande puissance de calcul et donc impossible de sécuriser la chaîne de bloc

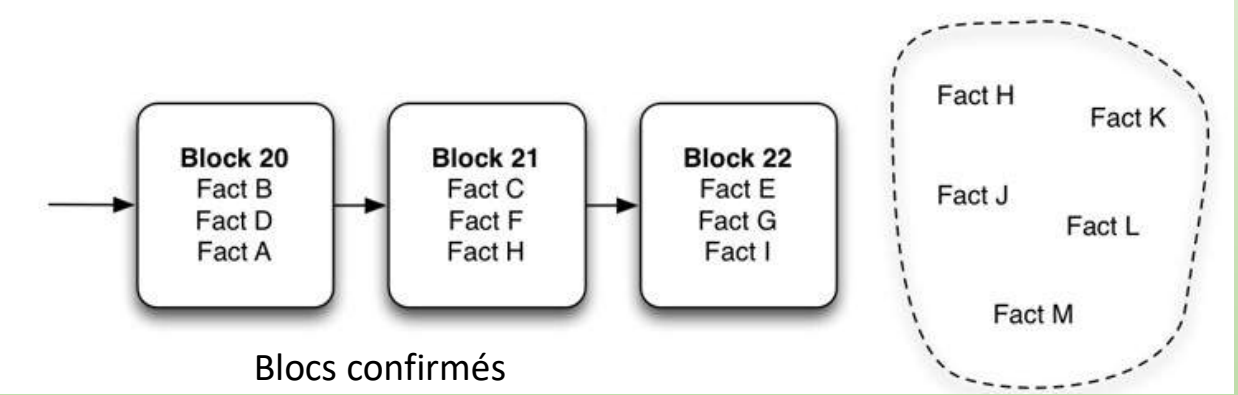
FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- Chaque fois que quelqu'un crée un hash avec succès, il reçoit une récompense de 25 bitcoins, la chaîne de blocs est mise à jour et tout le monde sur le réseau en entend parler.
- C'est donc comme ça que les mineurs 'obtiennent' un bloc. Pour ce faire, ils sont tous en concurrence les uns contre les autres
- Les transactions Bitcoin sont envoyées depuis et vers des portefeuilles Bitcoin électroniques et sont signées numériquement.

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

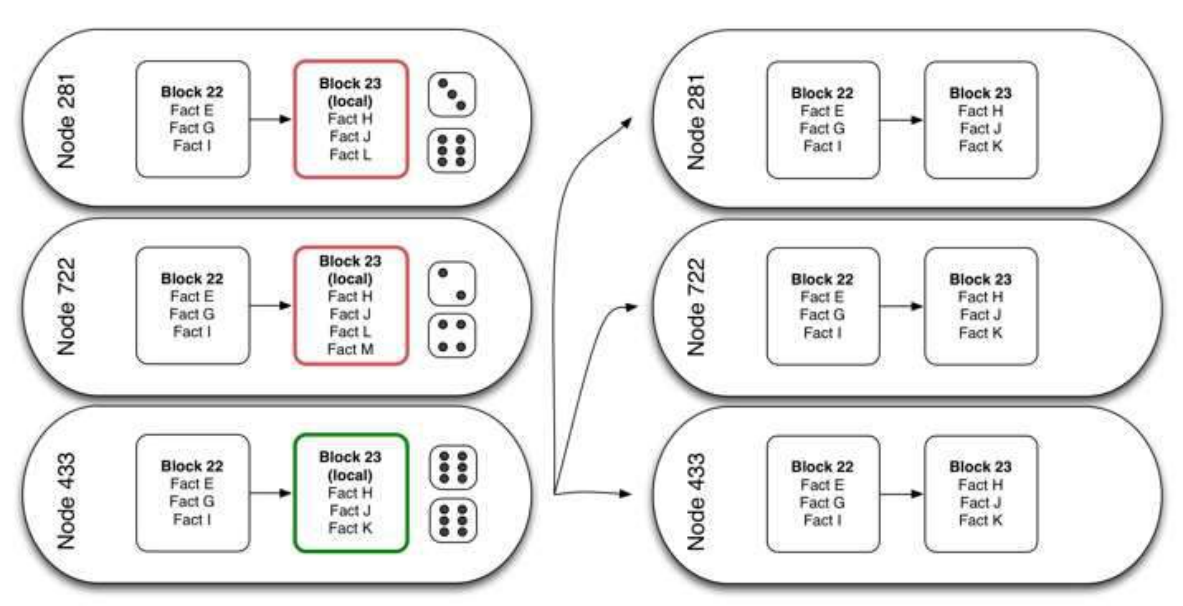


Blocs confirmés

Transactions en attentes

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?



Dans Bitcoin, le défi implique un double hash d'une séquence de faits en attente, l'identifiant du bloc précédent, et d'une séquence aléatoire, le tout avec l'algorithme SHA-256. Un nœud gagne si son hash contient au moins n zéros en entête.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

- Le **système hexadécimal** est un système de numération positionnel en base 16. Il utilise ainsi 16 symboles, en général les chiffres arabes pour les dix premiers chiffres et les lettres A à F pour les six suivants.

- il est particulièrement commode et permet un compromis entre le code binaire des machines et une base de numération pratique à utiliser

	8	*4*	*2*	*1*
$0_{hex} = 0_{dec} = 0_{oct}$	0	0	0	0
$1_{hex} = 1_{dec} = 1_{oct}$	0	0	0	1
$2_{hex} = 2_{dec} = 2_{oct}$	0	0	1	0
$3_{hex} = 3_{dec} = 3_{oct}$	0	0	1	1
$4_{hex} = 4_{dec} = 4_{oct}$	0	1	0	0
$5_{hex} = 5_{dec} = 5_{oct}$	0	1	0	1
$6_{hex} = 6_{dec} = 6_{oct}$	0	1	1	0
$7_{hex} = 7_{dec} = 7_{oct}$	0	1	1	1
$8_{hex} = 8_{dec} = 10_{oct}$	1	0	0	0
$9_{hex} = 9_{dec} = 11_{oct}$	1	0	0	1
$A_{hex} = 10_{dec} = 12_{oct}$	1	0	1	0
$B_{hex} = 11_{dec} = 13_{oct}$	1	0	1	1
$C_{hex} = 12_{dec} = 14_{oct}$	1	1	0	0
$D_{hex} = 13_{dec} = 15_{oct}$	1	1	0	1
$E_{hex} = 14_{dec} = 16_{oct}$	1	1	1	0
$F_{hex} = 15_{dec} = 17_{oct}$	1	1	1	1

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Comment fonctionne le minage du Bitcoin ?

Un hash perdant pour Bitcoin
787308540121f4afd2ff5179898934291105772495275df35f00cc5e44db42dd

Un hash gagnant pour Bitcoin si n=10
00000000009f766c17c736169f79cb0c65dd6e07244e9468bc60cde9538b551e

Le nombre n est ajusté de temps en temps afin de maintenir une durée de bloc fixe malgré les variations dans le nombre de nœuds. Ce nombre est appelé la ***difficulté****.*

Salle de serveurs de GOOGLE

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Les fermes de minage

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Topologie d'une mine

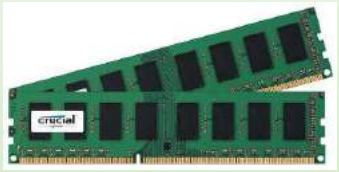
Carte mère

110 $

Processeur

75 $

RAM 2G



40 $

Disque dur

20 $

Carte Graphique

25-31 MH/s

245 $

Alimentation

151 $

641 $

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

[Transaction non confirmée en temps réel]

[Cours du Bitcoin en temps réel]

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

- Pour posséder des Bitcoin, il faut les acheter. Il faut donc que les ordinateurs du réseau valident si vous avez bien l'argent que vous désirez échanger. L'argent est remis à des gestionnaires de bitcoin ou de cryptomonnaie. Qui, en passant, prennent un pourcentage de redevance pour ce travail.

- Le bitcoin est une très mauvaise monnaie.

- 10 minutes avant d'être approuvée.

- La vraie valeur aujourd'hui est spéculative.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

La question qui tue:

Est-il judicieux d'investir dans des bitcoin?
Est-ce sûr ?

Il y a eu des détournements de millions d'argent chez des dépositaires et, en conclusion... Non, c'est pas plus sécuritaire.

Maintenant le bitcoin est rendu purement et simplement spéculatif car il y a de grandes variations de valeurs (jusqu'à 30 % dans une journée).

FORMATIO RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

L’avenir:

N'est pas dans le bitcoin mais plutôt dans l’utilisation de la chaîne de blocs afin de décentraliser les transactions.
Exemple: Uber, RB&B

Comment passer d’un Internet centralisé à un Internet décentralisé.
Technologie adéquate ???

Internet en 1994 n’était pas au point et maintenant on voit ce que c’est.

Actuellement la chaîne de blocs travaille mieux que l'internet en 1994.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Bitcoin et chaîne de blocs

La morale de cette histoire:

- Le bitcoin, c'est spectaculaire mais par intéressant.
- La chaîne de blocs, c'est le nouvel Internet de demain.

FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Guichet Bitcoin à Brossard

Pasta Tutti Giorni

7681 Boul. Taschereau, Brossard, QC J4Y 1A2 Itinéraire

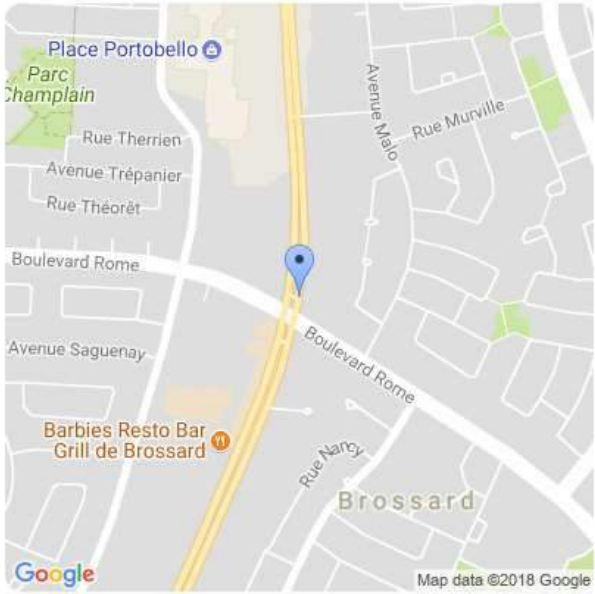
Accès à la distributrice par l'entrée secondaire à l'arrière du bâtiment.

EN LIGNE

Taux

Prix du Bitcoin

Acheter à:	15739.50 $ + 5 $ par transaction
Achat minimum	20 $ Renseignements
Vendre à:	n/d
Vente minimum	$200



FORMATIO | RESSOURCES INFORMATIQUES BUREAUTIQUES

Questions ?