Comment fonctionne Bitcoin

2022-03-03

# Comment fonctionne Bitcoin

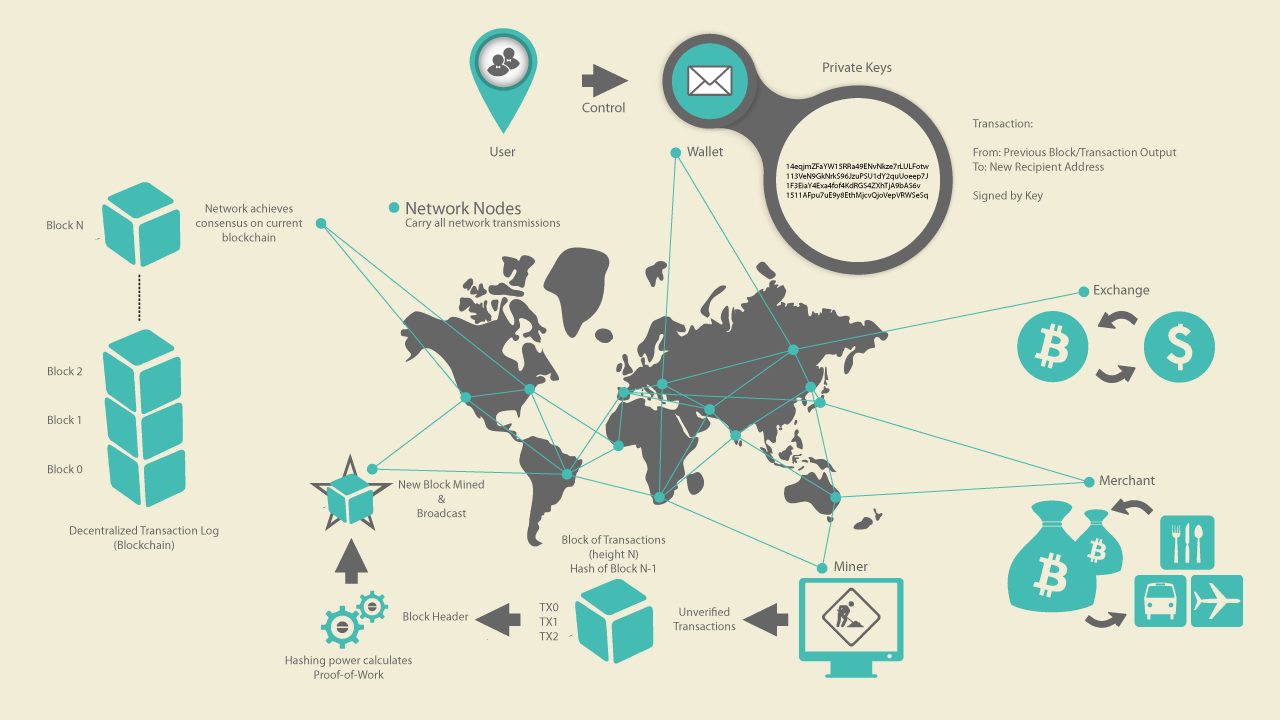
## Transactions, blocs, minage et la chaîne de blocs

Le système Bitcoin, contrairement aux systèmes bancaires et de paiement traditionnels, est basé sur la confiance décentralisée. Au lieu d'une autorité centrale de confiance, dans le bitcoin, la confiance est obtenue en tant que propriété émergente à partir des interactions des différents participants au système Bitcoin. Dans ce chapitre, nous examinerons le bitcoin d'un niveau élevé en suivant une seule transaction via le système Bitcoin et en observant qu'elle devient "de confiance" et acceptée par le mécanisme de consensus distribué bitcoin et est finalement enregistrée sur la chaîne de blocs, le grand livre distribué de toutes transactions. Les chapitres suivants approfondiront la technologie derrière les transactions, le réseau et l'exploitation minière.

### Présentation de Bitcoin

Dans le schéma d'ensemble présenté dans [figure\_title](#bitcoin-overview), nous voyons que le système Bitcoin se compose d'utilisateurs avec des portefeuilles contenant des clés, des transactions qui se propagent à travers le réseau et des mineurs qui produisent (par le calcul concurrentiel) le consensus de la chaîne de blocs, qui est le registre faisant autorité de toutes les transactions.

Chaque exemple de ce chapitre est basé sur une transaction réelle effectuée sur le réseau Bitcoin, simulant les interactions entre les utilisateurs (Joe, Alice, Bob et Gopesh) en envoyant des fonds à partir d'un portefeuille à un autre. Lors du suivi d'une transaction via le réseau Bitcoin jusqu'à la chaîne de blocs, nous utiliserons un site *explorateur de chaîne de blocs* pour visualiser chaque étape. Un explorateur de chaîne de blocs est une application Web qui fonctionne comme un moteur de recherche bitcoin, en ce sens qu'il vous permet de rechercher des adresses, des transactions et des blocs et de voir les relations et les flux entre eux.



Présentation de Bitcoin

Les explorateurs de blockchain populaires incluent :

* [Explorateur BlockCypher](https://live.blockcypher.com)
* [Blockchain.com](https://blockchain.com)
* [BitPay Insight](https://insight.bitpay.com)
* [Blockstream Explorer](https://blockstream.info)

Chacun d'eux a une fonction de recherche qui peut prendre une adresse Bitcoin, un hachage de transaction, un numéro de bloc ou un hachage de bloc et récupérer les informations correspondantes du réseau Bitcoin. Avec chaque exemple de transaction ou de bloc, nous fournirons une URL afin que vous puissiez la rechercher vous-même et l'étudier en détail.

### Acheter une tasse de café

Alice, présentée dans le chapitre précédent, est une nouvelle utilisatrice qui vient d'acquérir son premier bitcoin. Dans [???](#getting_first_bitcoin), Alice a rencontré son ami Joe pour échanger de l'argent contre du bitcoin. La transaction créée par Joe a financé le portefeuille d'Alice avec 0,10 BTC. Alice va maintenant faire sa première transaction de vente au détail en achetant une tasse de café au café de Bob à Palo Alto, en Californie.

Bob's Cafe a récemment commencé à accepter les paiements en bitcoin en ajoutant une option bitcoin à son système de point de vente. Les prix au Bob's Cafe sont indiqués dans la devise locale (dollars américains), mais à la caisse, les clients ont la possibilité de payer en dollars ou en bitcoins. Alice passe sa commande pour une tasse de café et Bob l'inscrit dans le registre, comme il le fait pour toutes les transactions. Le système de point de vente convertit automatiquement le prix total des dollars américains en bitcoins au taux du marché en vigueur et affiche le prix dans les deux devises :

Total:  
1,50 USD  
0,015 BTC

Bob dit : "C'est un dollar cinquante, ou quinze millibits."

Le système de point de vente de Bob créera également automatiquement un code QR spécial contenant une *demande de paiement* (voir [figure\_title](#payment-request-QR)).

Contrairement à un code QR qui contient simplement une adresse Bitcoin de destination, une demande de paiement est une URL encodée QR qui contient une adresse de destination, un montant de paiement et une description générique telle que "Bob's Cafe". Cela permet à une application de portefeuille bitcoin de pré-remplir les informations utilisées pour envoyer le paiement tout en affichant une description lisible par l'utilisateur à l'utilisateur. Vous pouvez scanner le code QR avec une application de portefeuille bitcoin pour voir ce qu'Alice verrait.



Code QR de la demande de paiement

Essayez de scanner ceci avec votre portefeuille pour voir l'adresse et le montant, mais N'ENVOYEZ PAS D'ARGENT.

**Le QR code de demande de paiement encode l'URL suivante, définie dans BIP-21 :**

bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?  
amount=0.015&  
label=Bob%27s%20Cafe&  
message=Acheter%20chez%20Bob%27s%20Café  
  
Composants de l&#39;URL  
  
Une adresse Bitcoin : &quot;1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA&quot;  
Le montant du paiement: &quot;0,015&quot;  
Une étiquette pour l&#39;adresse du destinataire : « Bob&#39;s Cafe »  
Une description du paiement : &quot;Acheter au Bob&#39;s Cafe&quot;

Alice utilise son smartphone pour scanner le code-barres affiché. Son smartphone affiche un paiement de 0,0150 BTC à Bob&#39;s Cafe et elle sélectionne Envoyer pour autoriser le paiement. En quelques secondes (environ le même temps qu'une autorisation de carte de crédit), Bob voit la transaction sur le registre, complétant la transaction.

Dans les sections suivantes, nous examinerons cette transaction plus en détail. Nous verrons comment le portefeuille d'Alice l'a construit, comment il s'est propagé sur le réseau, comment il a été vérifié et enfin, comment Bob peut dépenser ce montant lors de transactions ultérieures.

Le réseau Bitcoin peut effectuer des transactions en valeurs fractionnaires, par exemple à partir de millibitcoin (1/1000e de bitcoin ) jusqu'à 1/100 000 000e de bitcoin, connu sous le nom de satoshi. Tout au long de ce livre, nous utiliserons le terme "bitcoin" pour désigner toute quantité de monnaie bitcoin, de la plus petite unité (1 satoshi) au nombre total (21 000 000) de tous les bitcoins qui seront extraits.

Vous pouvez examiner la transaction d'Alice avec Bob's Cafe sur la blockchain en utilisant un site d'exploration de blocs ([example\_title](#view_alice_transaction)):

https://www.blockchain.com/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

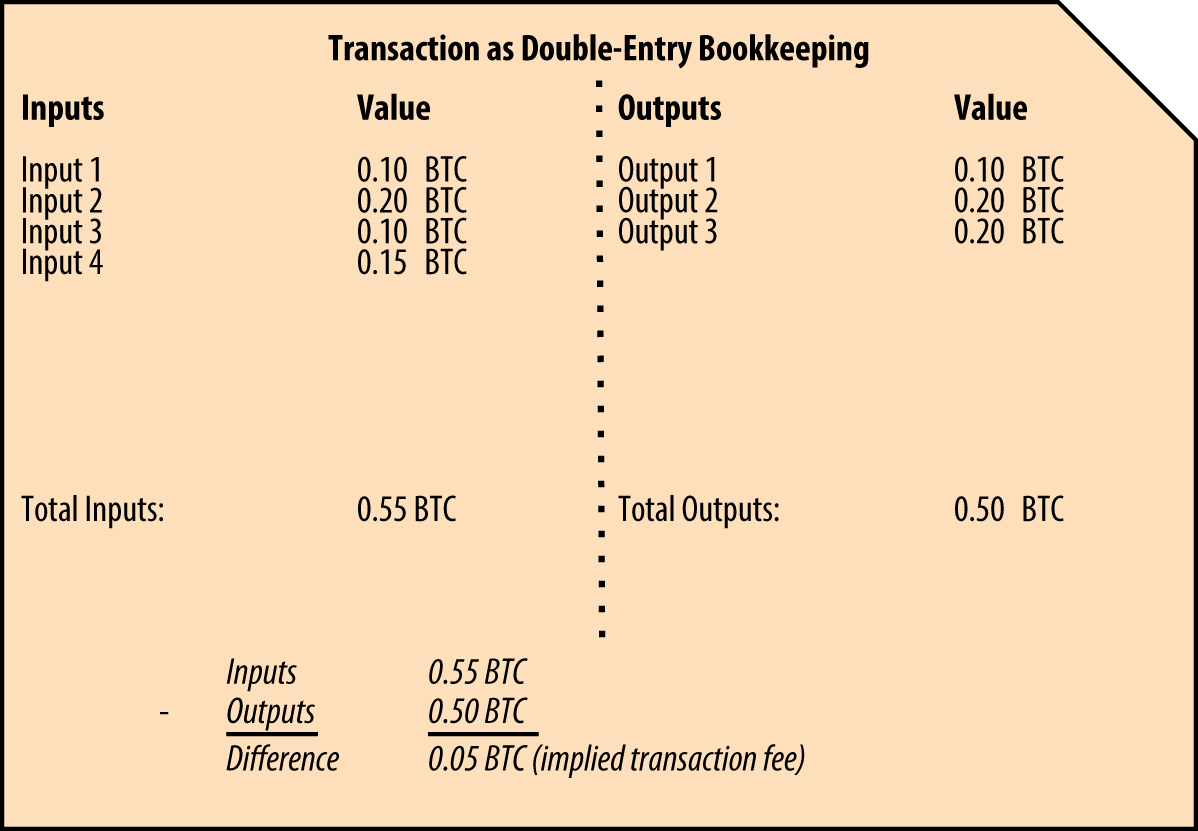
## Transactions en bitcoins

En termes simples, une transaction indique au réseau que le propriétaire d'une valeur bitcoin a autorisé le transfert de cette valeur à un autre propriétaire. Le nouveau propriétaire peut désormais dépenser le bitcoin en créant une autre transaction qui autorise le transfert à un autre propriétaire, et ainsi de suite, dans une chaîne de propriété.

### Entrées et sorties de transactions

Les transactions sont comme des lignes dans un livre comptable en partie double. Chaque transaction contient une ou plusieurs "entrées", qui sont comme des débits sur un compte bitcoin. De l'autre côté de la transaction, il y a une ou plusieurs "sorties", qui sont comme des crédits ajoutés à un compte bitcoin. Les entrées et les sorties (débits et crédits) ne totalisent pas nécessairement le même montant. Au lieu de cela, les sorties s'additionnent légèrement moins que les entrées et la différence représente des *frais de transaction* implicites, qui sont un petit paiement perçu par le mineur qui inclut la transaction dans le grand livre. Une transaction bitcoin s'affiche sous la forme d'une écriture comptable dans [figure\_title](#transaction-double-entry).

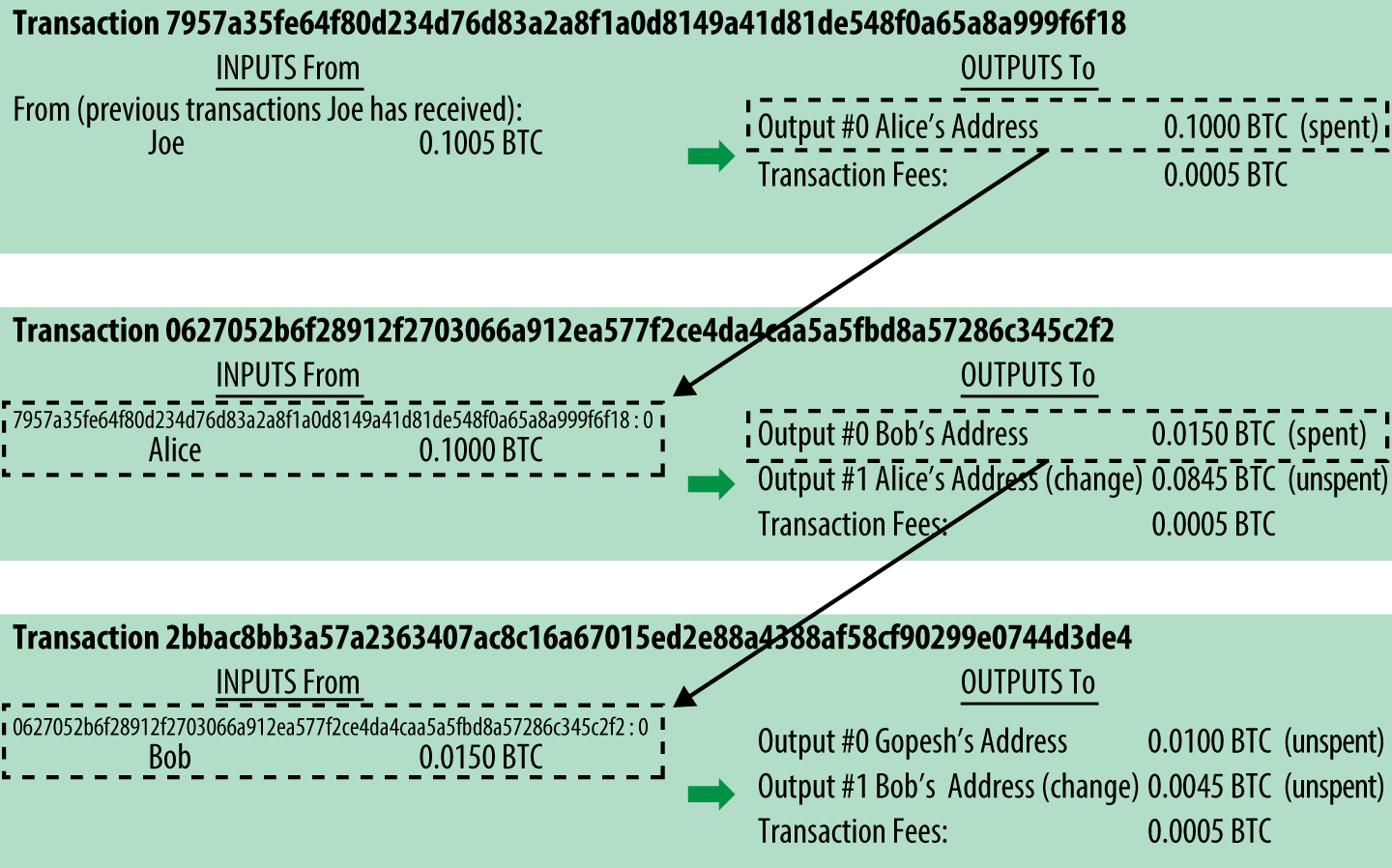
La transaction contient également une preuve de propriété pour chaque montant de bitcoin (entrées) dont la valeur est dépensée, sous la forme d'une signature numérique du propriétaire, qui peut être validée indépendamment par n'importe qui. En termes de bitcoin, "dépenser" consiste à signer une transaction qui transfère la valeur d'une transaction précédente à un nouveau propriétaire identifié par une adresse Bitcoin.



Transaction comptable en double parties

### Chaînes de transaction

Le paiement d'Alice à Bob's Cafe utilise la sortie d'une transaction précédente comme entrée. Dans le chapitre précédent, Alice a reçu des bitcoins de son ami Joe en échange d'argent. Cette transaction a créé une valeur bitcoin verrouillée par la clé d'Alice. Sa nouvelle transaction avec Bob's Cafe fait référence à la transaction précédente comme entrée et crée de nouvelles sorties pour payer la tasse de café et recevoir la monnaie. Les transactions forment une chaîne, où les entrées de la dernière transaction correspondent aux sorties des transactions précédentes. La clé d'Alice fournit la signature qui déverrouille ces sorties de transaction précédentes, prouvant ainsi au réseau Bitcoin qu'elle possède les fonds. Elle joint le paiement du café à l'adresse de Bob, "encombrant" ainsi cette sortie avec l'exigence que Bob produise une signature afin de dépenser ce montant. Cela représente un transfert de valeur entre Alice et Bob. Cette chaîne de transactions, de Joe à Alice à Bob, est illustrée dans [figure\_title](#blockchain-mnemonic).



Une chaîne de transactions, où la sortie d'une transaction est l'entrée de la transaction suivante

### Faire du change (ou de la petite monnaie)

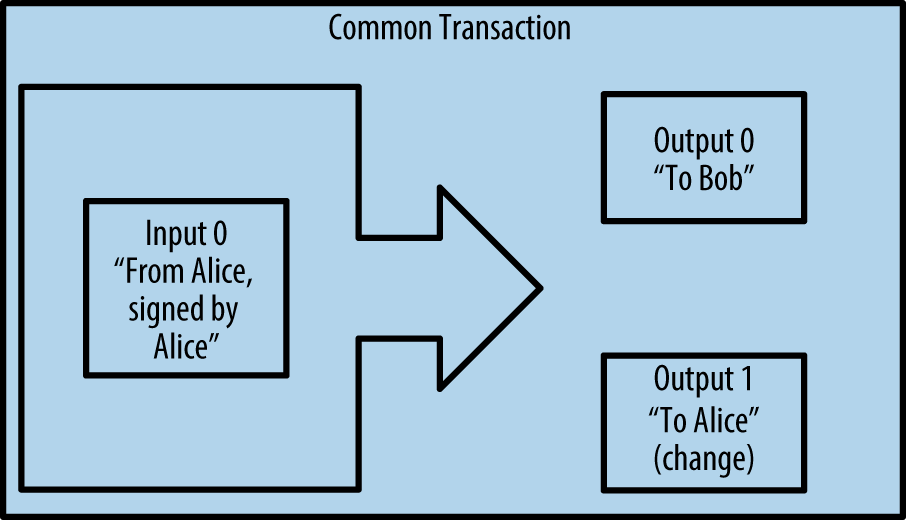
De nombreuses transactions bitcoin incluront des sorties qui référencent à la fois une adresse du nouveau propriétaire et une adresse du propriétaire actuel, appelée *adresse de change*. En effet, les entrées de transaction, comme les billets de banque, ne peuvent pas être divisées. Si vous achetez un article de 5 dollars américains dans un magasin mais que vous utilisez un billet de 20 dollars américains pour payer l'article, vous vous attendez à recevoir 15 dollars américains en monnaie. Le même concept s'applique aux entrées de transaction bitcoin. Si vous avez acheté un article qui coûte 5 bitcoins mais que vous n'aviez qu'une entrée de 20 bitcoins à utiliser, votre portefeuille créerait une seule transaction qui enverrait deux sorties, une sortie de 5 bitcoins au propriétaire du magasin et une sortie de 15 bitcoins à vous-même comme changement (moins les frais de transaction applicables). Il est important de noter que l'adresse de change ne doit pas nécessairement être la même que celle de l'entrée et, pour des raisons de confidentialité, il s'agit souvent d'une nouvelle adresse du portefeuille du propriétaire.

Différents portefeuilles peuvent utiliser différentes stratégies lors de l'agrégation des entrées pour effectuer un paiement demandé par l'utilisateur. Ils peuvent regrouper de nombreux petits intrants ou en utiliser un égal ou supérieur au paiement souhaité. À moins que le portefeuille ne puisse agréger les entrées de manière à correspondre exactement au paiement souhaité plus les frais de transaction, le portefeuille devra générer du change. C'est très similaire à la façon dont les gens gèrent l'argent liquide. Si vous utilisez toujours le plus gros billet dans votre poche, vous vous retrouverez avec une poche pleine de monnaie. Si vous n'utilisez que la petite monnaie, vous n'aurez toujours que de gros billets. Les gens trouvent inconsciemment un équilibre entre ces deux extrêmes, et les développeurs de portefeuilles Bitcoin s'efforcent de programmer cet équilibre.

En résumé, les *transactions* déplacent des valeurs des *entrées de transaction* aux *sorties de transaction*. Une entrée est une référence à la sortie d'une transaction précédente, indiquant d'où provient la valeur. Une transaction comprend généralement une sortie qui dirige une valeur spécifique vers l'adresse Bitcoin d'un nouveau propriétaire et une sortie de modification vers le propriétaire d'origine. Les sorties d'une transaction peuvent être utilisées comme entrées dans une nouvelle transaction, créant ainsi une chaîne de propriété lorsque la valeur est déplacée d'un propriétaire à l'autre (voir [figure\_title](#blockchain-mnemonic)).

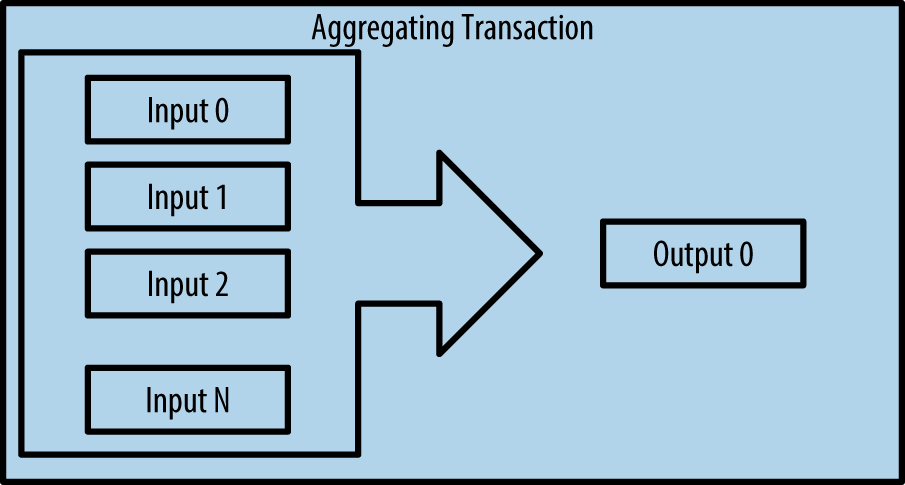
### Formulaires de transaction communs

La forme de transaction la plus courante est un simple paiement d'une adresse à une autre, qui comprend souvent une « monnaie » rendue au propriétaire d'origine. Ce type de transaction a une entrée et deux sorties et est affiché dans [figure\_title](#transaction-common).



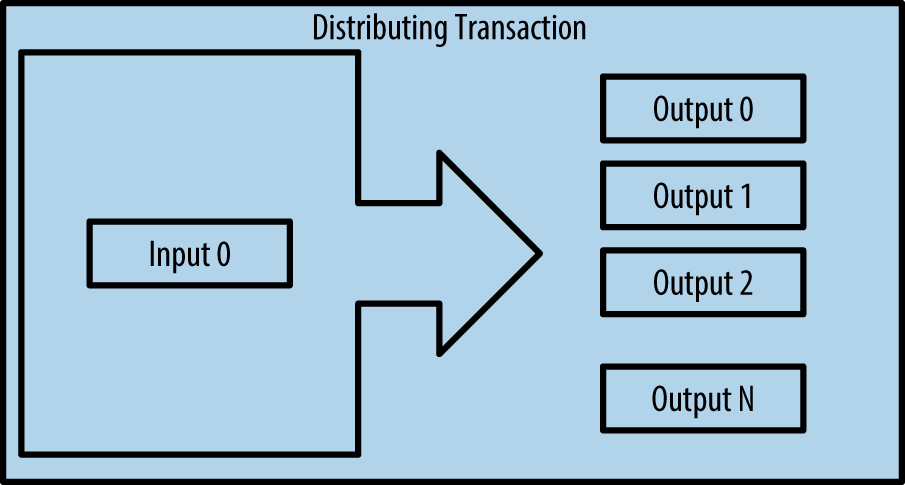
Transaction la plus courante

Une autre forme courante de transaction est celle qui agrège plusieurs entrées en une seule sortie (voir <<transaction-aggregating> >). Cela représente l'équivalent réel de l'échange d'une pile de pièces et de billets de banque contre un seul billet plus gros. Des transactions comme celles-ci sont parfois générées par des applications de portefeuille pour nettoyer de nombreux petits montants reçus en monnaie de paiement.



Transaction agrégeant des fonds

Enfin, une autre forme de transaction que l'on voit souvent sur le grand livre bitcoin est une transaction par lots, qui distribue une entrée à plusieurs sorties représentant plusieurs destinataires, une technique appelée "transactions par lot" (voir [figure\_title](#transaction-distributing)). Étant donné que ce type de transaction est utile pour économiser sur les frais de transaction, il est couramment utilisé par les entités commerciales pour distribuer des fonds, par exemple lorsqu'une entreprise traite les paiements de paie à plusieurs employés ou lorsqu'un échange de bitcoins traite les retraits de plusieurs clients en un seul. transaction.



Transaction distribuant des fonds

## Construction d'une transaction

L'application de portefeuille d'Alice contient toute la logique pour sélectionner les entrées et les sorties appropriées pour construire une transaction à la spécification d'Alice. Alice n'a qu'à spécifier une destination et un montant, et le reste se passe dans l'application portefeuille sans qu'elle ne voie les détails. Il est important de noter qu'une application de portefeuille peut créer des transactions même si elle est complètement hors ligne. Comme écrire un chèque à la maison et l'envoyer plus tard à la banque dans une enveloppe, la transaction n'a pas besoin d'être construite et signée tout en étant connectée au réseau Bitcoin.

### Obtenir les bonnes entrées

L'application de portefeuille d'Alice devra d'abord trouver des entrées qui peuvent payer le montant qu'elle veut envoyer à Bob. La plupart des portefeuilles gardent une trace de toutes les sorties disponibles appartenant aux adresses du portefeuille. Par conséquent, le portefeuille d'Alice contiendrait une copie de la sortie de transaction de la transaction de Joe, qui a été créée en échange d'argent (voir [???](#getting_first_bitcoin)). Une application de portefeuille bitcoin qui s'exécute en tant que client à nœud complet contient en fait une copie de chaque sortie non dépensée de chaque transaction dans la chaîne de blocs. Cela permet à un portefeuille de construire des entrées de transaction ainsi que de vérifier rapidement les transactions entrantes comme ayant des entrées correctes. Cependant, comme un client à nœud complet occupe beaucoup d'espace disque, la plupart des portefeuilles d'utilisateurs exécutent des clients "légers" qui ne suivent que les sorties non dépensées de l'utilisateur.

Si l'application de portefeuille ne conserve pas une copie des sorties de transaction non dépensées, elle peut interroger le réseau Bitcoin pour récupérer ces informations à l'aide d'une variété d'API disponibles par différents fournisseurs ou en demandant à un nœud complet via l'aide d'un appel d'interface de programmation d'application (API). [example\_title](#example_2-2) montre une requête API, construite comme une commande HTTP GET vers une URL spécifique. Cette URL renverra toutes les sorties de transaction non dépensées pour une adresse, donnant à toute application les informations dont elle a besoin pour construire des entrées de transaction pour les dépenses. Nous utilisons le simple client HTTP en ligne de commande *cURL* pour récupérer la réponse.

$ curl https://blockchain.info/unspent?active=1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

{  
  
 "unspent\_outputs":[  
  
 {  
 "tx\_hash":"186f9f998a5...2836dd734d2804fe65fa35779",  
 "tx\_index":104810202,  
 "tx\_output\_n": 0,  
 "script":"76a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac",  
 "value": 10000000,  
 "value\_hex": "00989680",  
 "confirmations":0  
 }  
  
 ]  
}

La réponse en [example\_title](#example_2-2) montre une sortie non dépensée (une qui n'a pas encore été échangée) sous la propriété de l'adresse d'Alice 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK. La réponse inclut la référence à la transaction dans laquelle cette sortie non dépensée est contenue (le paiement de Joe) et sa valeur en satoshis, à 10 millions, équivalent à 0,10 bitcoin. Avec ces informations, l'application de portefeuille d'Alice peut construire une transaction pour transférer cette valeur aux nouvelles adresses de propriétaire.

Voir la [transaction de Joe à Alice](https://www.blockchain.com/btc/tx/7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18).

Comme vous pouvez le voir, le portefeuille d'Alice contient suffisamment de bitcoins en une seule sortie non dépensée pour payer la tasse de café. Si cela n'avait pas été le cas, l'application de portefeuille d'Alice aurait peut-être dû "fouiller" dans une pile de petites sorties non dépensées, comme prendre des pièces dans un sac à main jusqu'à ce qu'elle puisse en trouver assez pour payer le café. Dans les deux cas, il peut être nécessaire de récupérer de la monnaie, ce que nous verrons dans la section suivante, car l'application de portefeuille crée les sorties de transaction (paiements).

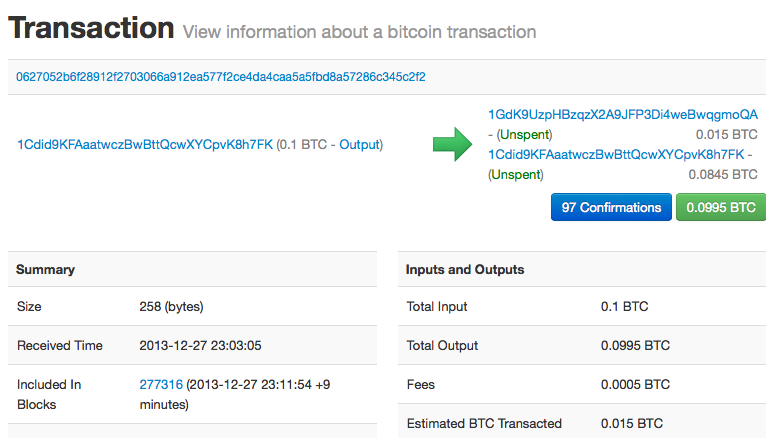
### Création des sorties

Une sortie de transaction est créée sous la forme d'un script qui crée une charge sur la valeur et ne peut être rachetée que par l'introduction d'une solution au script. En termes plus simples, la sortie de transaction d'Alice contiendra un script qui dit quelque chose comme "Cette sortie est payable à quiconque peut présenter une signature à partir de la clé correspondant à l'adresse de Bob." Étant donné que seul Bob possède le portefeuille avec les clés correspondant à cette adresse, seul le portefeuille de Bob peut présenter une telle signature pour racheter cette sortie. Alice « encombrera » donc la valeur de sortie avec une demande de signature de Bob.

Cette transaction comprendra également une deuxième sortie, car les fonds d'Alice se présentent sous la forme d'une sortie à 0,10 BTC, trop d'argent pour la tasse de café à 0,015 BTC. Alice aura besoin de 0,085 BTC en monnaie. Le paiement de monnaie d'Alice est créé par le portefeuille d'Alice en tant que sortie dans la même transaction que le paiement à Bob. Essentiellement, le portefeuille d'Alice divise ses fonds en deux paiements : un à Bob et un à elle-même. Elle peut ensuite utiliser (dépenser) la sortie de monnaie dans une transaction ultérieure.

Enfin, pour que la transaction soit traitée par le réseau en temps opportun, l'application de portefeuille d'Alice ajoutera une somme modique. Ce n'est pas explicite dans la transaction ; il est impliqué par la différence entre les entrées et les sorties. Si au lieu de prendre 0,085 en monnaie, Alice ne crée que 0,0845 comme deuxième sortie, il restera 0,0005 BTC (un demi-millibitcoin). Le 0,10 BTC de l'entrée n'est pas entièrement dépensé avec les deux sorties, car elles totaliseront moins de 0,10. La différence qui en résulte est le *frais de transaction* qui est perçu par le mineur en tant que frais de validation et d'inclusion de la transaction dans un bloc à enregistrer sur la chaîne de blocs.

La transaction résultante peut être vue à l'aide d'une application Web d'exploration de chaîne de blocs, comme indiqué dans [figure\_title](#transaction-alice).



Transaction d'Alice au Bob's Cafe

Voir la [transaction d'Alice à Bob's Cafe](https://www.blockchain.com/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2).

### Ajout de la transaction au grand livre

La transaction créée par l'application du portefeuille d'Alice fait 258 octets et contient tout le nécessaire pour confirmer la propriété des fonds et attribuer à de nouveaux propriétaires. Désormais, la transaction doit être transmise au réseau Bitcoin où elle fera partie de la chaîne de blocs. Dans la section suivante, nous verrons comment une transaction devient partie intégrante d'un nouveau bloc et comment le bloc est « miné ». Enfin, nous verrons comment le nouveau bloc, une fois ajouté à la chaîne de blocs, est de plus en plus approuvé par le réseau au fur et à mesure que de nouveaux blocs sont ajoutés.

#### Transmission de la transaction

La transaction contient toutes les informations nécessaires au traitement, et ce peu importe comment et où elle est transmise au réseau Bitcoin. Le réseau Bitcoin est un réseau pair à pair, chaque client Bitcoin participant en se connectant à plusieurs autres clients Bitcoin. Le but du réseau Bitcoin est de propager les transactions et les blocages à tous les participants.

#### Comment ça se propage

Tout système, tel qu'un serveur, une application de bureau ou un portefeuille, qui participe au réseau Bitcoin en "parlant", le protocole Bitcoin est appelé un *nœud Bitcoin*. L'application de portefeuille d'Alice peut envoyer la nouvelle transaction à n'importe quel nœud Bitcoin auquel elle est connectée via n'importe quel type de connexion : filaire, Wi-Fi, mobile, etc. Son portefeuille Bitcoin n'a pas besoin d'être connecté directement au portefeuille Bitcoin de Bob et elle n'a pas à nécessairement utiliser la connexion Internet offerte par le café, bien que ces deux options soient également possibles. Tout nœud Bitcoin qui reçoit une transaction valide qu'il n'a pas vue auparavant la transmettra immédiatement à tous les autres nœuds auxquels il est connecté , une technique de propagation connue sous le nom d'*inondation*. Ainsi, la transaction se propage (en inondant ou distribuant) rapidement à travers le réseau pair à pair, atteignant un grand pourcentage de nœuds en quelques secondes.

#### Le point de vue de Bob

Si l'application de portefeuille bitcoin de Bob est directement connectée à l'application de portefeuille d'Alice, l'application de portefeuille de Bob peut être le premier nœud à recevoir la transaction. Cependant, même si le portefeuille d'Alice envoie la transaction via d'autres nœuds, elle atteindra le portefeuille de Bob en quelques secondes. Le portefeuille de Bob identifiera immédiatement la transaction d'Alice comme un paiement entrant car il contient des sorties remboursables par les clés de Bob. L'application de portefeuille de Bob peut également vérifier de manière indépendante que la transaction est bien formée, utilise des sorties précédemment non dépensées et contient des frais de transaction suffisants pour être inclus dans le bloc suivant. À ce stade, Bob peut supposer, avec peu de risques, que la transaction sera bientôt incluse dans un bloc et confirmée.

Une idée fausse courante à propos des transactions bitcoin est qu'elles doivent être "confirmées" en attendant 10 minutes pour un nouveau bloc, ou jusqu'à 60 minutes pour six confirmations complètes. Bien que les confirmations garantissent que la transaction a été acceptée par l'ensemble du réseau, un tel délai n'est pas nécessaire pour les articles de petite valeur comme une tasse de café. Un commerçant peut accepter une transaction valide de petite valeur sans confirmation, sans plus de risque qu'un paiement par carte de crédit effectué sans pièce d'identité ni signature, comme les commerçants l'acceptent couramment aujourd'hui.("", startref="Tconstruct02" )

## Extraction de bitcoins

La transaction d'Alice est maintenant propagé sur le réseau Bitcoin. Il ne fait pas partie de la *chaîne de blocs* tant qu'il n'est pas vérifié et inclus dans un bloc par un processus appelé *minage*. Voir [???](#mining) pour une explication détaillée.

Le système de confiance Bitcoin est basé sur le calcul. Les transactions sont regroupées en *blocs*, qui nécessitent une énorme quantité de calculs pour prouver, mais seulement une petite quantité de calculs pour vérifier comme prouvé. Le processus de minage sert à deux fins dans le bitcoin :

* Les nœuds de minage valident toutes les transactions en se référant au *consensus des règles de bitcoin*. Par conséquent, le minage assure la sécurité des transactions bitcoin en rejetant les transactions invalides ou malformées.
* L'exploitation minière crée de nouveaux bitcoins dans chaque bloc, presque comme une banque centrale imprimant de la nouvelle monnaie. La quantité de bitcoin créée par bloc est limitée et diminue avec le temps, suivant un calendrier d'émission fixe.

L'exploitation minière atteint un bon équilibre entre le coût et la récompense. L'exploitation minière utilise l'électricité pour résoudre un problème mathématique. Un mineur qui réussit recevra une *récompense* sous la forme de nouveaux bitcoins et de frais de transaction. Cependant, la récompense ne sera perçue que si le mineur a correctement validé toutes les transactions, à la satisfaction des règles de *consensus*. Cet équilibre délicat assure la sécurité du bitcoin sans autorité centrale.

Une bonne façon de décrire l'exploitation minière est comme un jeu compétitif géant de sudoku qui se réinitialise chaque fois que quelqu'un trouve une solution et dont la difficulté s'ajuste automatiquement de sorte qu'il faut environ 10 minutes pour trouver une solution. Imaginez un puzzle sudoku géant, de plusieurs milliers de lignes et de colonnes. Si je vous montre un puzzle terminé, vous pouvez le vérifier assez rapidement. Cependant, si le puzzle a quelques cases remplies et que les autres sont vides, cela demande beaucoup de travail à résoudre ! La difficulté du sudoku peut être ajustée en modifiant sa taille (plus ou moins de lignes et de colonnes), mais elle peut toujours être vérifiée assez facilement même si elle est très grande. Le "casse-tête" utilisé dans le bitcoin est basé sur un hachage cryptographique et présente des caractéristiques similaires : il est asymétriquement difficile à résoudre mais facile à vérifier, et sa difficulté peut être ajustée.

In [???](#user-stories), nous avons présenté Jing est un entrepreneur à Shanghai. Jing dirige une *ferme minière*, qui est une entreprise qui gère des milliers d'ordinateurs miniers spécialisés, en compétition pour la récompense. Toutes les 10 minutes environ, les ordinateurs miniers de Jing rivalisent avec des milliers de systèmes similaires dans une course mondiale pour trouver une solution à un bloc de transactions. Trouver une telle solution, la soi-disant *Proof-of-Work (ou Preuve de travail)* (PoW), nécessite des quadrillions d'opérations de hachage par seconde sur l'ensemble du réseau Bitcoin. L'algorithme de preuve de travail implique de hacher à plusieurs reprises l'en-tête du bloc et un nombre aléatoire avec l'algorithme cryptographique SHA256 jusqu'à ce qu'une solution correspondant à un modèle prédéterminé émerge. Le premier mineur à trouver une telle solution remporte la compétition et publie ce bloc dans la chaîne de blocs.

Jing a commencé l'exploitation minière en 2010 en utilisant un ordinateur de bureau très rapide pour trouver une preuve de travail appropriée pour les nouveaux blocs. Au fur et à mesure que de plus en plus de mineurs rejoignaient le réseau Bitcoin, la difficulté du problème augmentait rapidement. Bientôt, Jing et d'autres mineurs sont passés à du matériel plus spécialisé, avec des unités de traitement graphique (GPU) dédiées de haute de gamme, souvent utilisées dans les ordinateurs de bureau ou les consoles de jeu. Au moment d'écrire ces lignes, la difficulté est si élevée qu'il n'est rentable de miner qu'avec des circuits intégrés à application spécifique (ASIC), essentiellement des centaines d'algorithmes de minage imprimé en matériel, fonctionnant en parallèle sur une seule puce de silicium. La société de Jing participe également à un *groupe ou bassin de mineurs*, qui, tout comme un groupe de loterie, permet à plusieurs participants de partager leurs efforts et leurs récompenses. La société de Jing gère désormais un entrepôt contenant des milliers de mineurs ASIC pour extraire du bitcoin 24 heures sur 24. L'entreprise paie ses frais d'électricité en vendant le bitcoin qu'elle est capable de générer à partir de l'exploitation minière, créant ainsi des revenus à partir des bénéfices.

## Transactions minières en blocs

De nouvelles transactions affluent constamment sur le réseau à partir des portefeuilles des utilisateurs et d'autres applications. Comme ceux-ci sont vus par les nœuds du réseau Bitcoin, ils sont ajoutés à un bassin temporaire de transactions non vérifiées maintenues par chaque nœud. Lorsque les mineurs construisent un nouveau bloc, ils ajoutent des transactions non vérifiées de ce bassin au nouveau bloc, puis tentent de prouver la validité de ce nouveau bloc, avec l'algorithme de minage (la preuve de travail). Le processus d'extraction est expliqué en détail dans [???](#mining).

Les transactions sont ajoutées au nouveau bloc, classées par ordre de priorité par les transactions les plus payantes en premier et quelques autres critères. Chaque mineur commence le processus d'extraction d'un nouveau bloc de transactions dès qu'il reçoit le bloc précédent du réseau, sachant qu'il a perdu le tour de compétition précédent. Ils créent immédiatement un nouveau bloc, le remplissent avec les transactions et l'empreinte numérique du bloc précédent, et commencent à calculer la preuve de travail pour le nouveau bloc. Chaque mineur inclut une transaction spéciale dans son bloc, une transaction qui paie à sa propre adresse Bitcoin la récompense du bloc (actuellement 6,25 bitcoins nouvellement créés) plus la somme des frais de transaction de toutes les transactions incluses dans le bloc. S'ils trouvent une solution qui rend ce bloc valide, ils "gagnent" cette récompense car leur bloc réussi est ajouté à la chaîne de blocs mondiale et la transaction de récompense qu'ils ont incluse devient dépensable. Jing, qui participe à un groupe de minage, a mis en place son logiciel pour créer de nouveaux blocs qui attribuent la récompense à une adresse de pool. À partir de là, une part de la récompense est distribuée à Jing et aux autres mineurs proportionnellement à la quantité de travail qu'ils ont apportée lors du dernier tour.

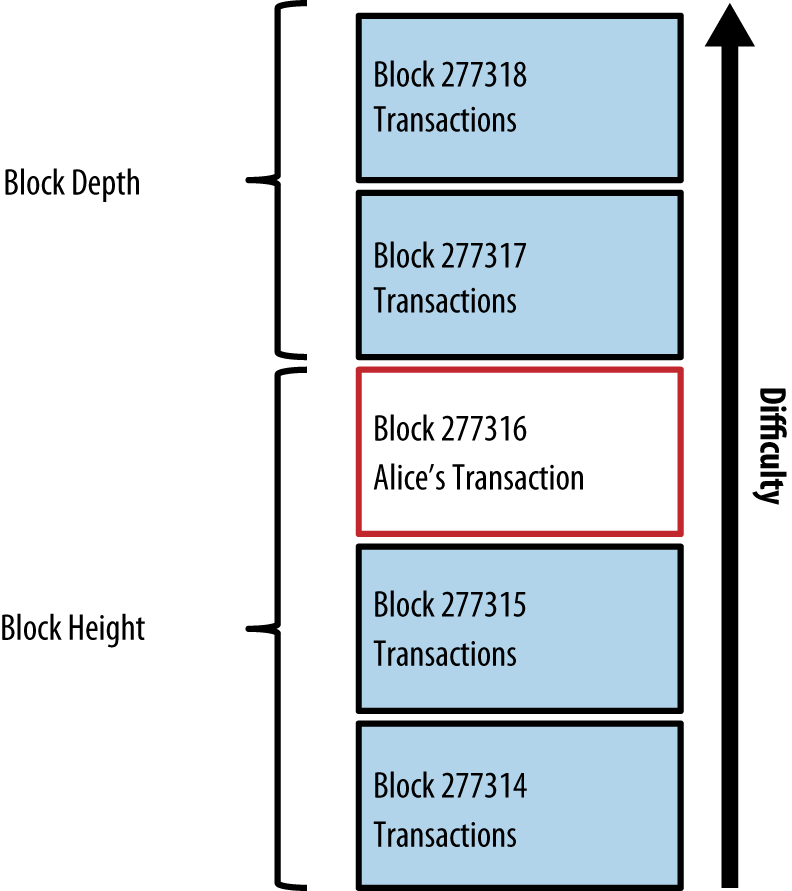
La transaction d'Alice a été récupérée par le réseau et incluse dans le groupe de transactions non vérifiées. Une fois validé par le logiciel de minage, il a été inclus dans un nouveau bloc, appelé *bloc candidat*, généré par le pool de minage de Jing. Tous les mineurs participant à ce pool de minage commencent immédiatement à calculer la preuve de travail pour le bloc candidat. Environ cinq minutes après la première transmission de la transaction par le portefeuille d'Alice, l'un des mineurs ASIC de Jing a trouvé une solution pour le bloc candidat et l'a annoncée au réseau. Une fois que les autres mineurs ont validé le bloc gagnant, ils ont commencé la course pour générer le bloc suivant.

Le bloc gagnant de Jing est devenu une partie de la blockchain en tant que bloc # 277316, contenant 419 transactions, y compris la transaction d'Alice. Le bloc contenant la transaction d'Alice est compté comme une "confirmation" de cette transaction.

Vous pouvez voir le bloc qui inclut [Transaction d’Alice](https://www.blockchain.com/btc/block/277316).

Environ 20 minutes plus tard, un nouveau bloc, #277317, est miné par un autre mineur. Parce que ce nouveau bloc est construit au-dessus du bloc #277316 qui contenait la transaction d'Alice, il a ajouté encore plus de calculs à la chaîne de blocs, renforçant ainsi la confiance dans ces transactions. Chaque bloc miné en plus de celui contenant la transaction compte comme une confirmation supplémentaire pour la transaction d'Alice. Au fur et à mesure que les blocs s'empilent les uns sur les autres, il devient exponentiellement plus difficile d'inverser la transaction, ce qui la rend de plus en plus fiable par le réseau.

Dans le diagramme en [figure\_title](#block-alice1), nous pouvons voir le bloc #277316, qui contient la transaction d'Alice. En dessous se trouvent 277 316 blocs (y compris le bloc #0), liés les uns aux autres dans une chaîne de blocs (blockchain) jusqu'au bloc #0, connu sous le nom de *bloc d’origine*. Au fil du temps, à mesure que la "hauteur" des blocs augmente, la difficulté de calcul de chaque bloc et de la chaîne dans son ensemble augmente également. Les blocs extraits après celui qui contient la transaction d'Alice agissent comme une assurance supplémentaire, car ils accumulent plus de calculs dans une chaîne de plus en plus longue. Par convention, tout bloc avec plus de six confirmations est considéré comme irrévocable, car il faudrait une immense quantité de calculs pour invalider et recalculer six blocs. Nous examinerons plus en détail le processus d'exploitation minière et la manière dont il renforce la confiance dans [???](#mining).



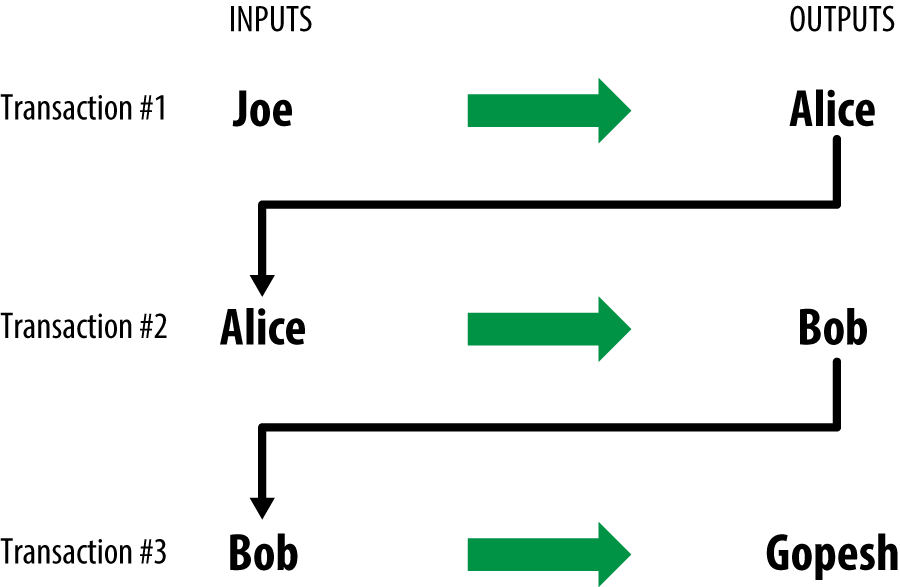
Transaction d'Alice incluse dans le bloc #277316

## Dépenser la transaction

Maintenant que la transaction d'Alice a été intégrée à la chaîne de blocs dans le cadre d’un bloc, il fait partie du grand livre distribué de Bitcoin et est visible par toutes les applications Bitcoin. Chaque client Bitcoin peut indépendamment vérifier que la transaction est valide et utilisable. Les clients du nœud complet peuvent suivre la source des fonds à partir du moment où les bitcoins ont été générés pour la première fois dans un bloc, progressivement d'une transaction à l'autre, jusqu'à ce qu'ils atteignent l'adresse de Bob. Les clients légers peuvent faire ce qu'on appelle une vérification de paiement simplifiée (voir [???](#spv_nodes)) en confirmant que la transaction est dans la chaîne de blocs et qu'elle a plusieurs blocs extraits après elle, fournissant ainsi l'assurance que les mineurs l'ont acceptée comme valide.

Bob peut maintenant dépenser le résultat de cette transaction et d'autres transactions. Par exemple, Bob peut payer un entrepreneur ou un fournisseur en transférant la valeur du paiement de la tasse de café d'Alice à ces nouveaux propriétaires. Très probablement, le logiciel Bitcoin de Bob regroupera de nombreux petits paiements en un paiement plus important, concentrant peut-être tous les revenus Bitcoin de la journée en une seule transaction. Cela regrouperait les différents paiements en un seul résultat (et une seule adresse). Pour un diagramme d'une transaction d'agrégation, voir [figure\_title](#transaction-aggregating).

Au fur et à mesure que Bob dépense les paiements reçus d'Alice et d'autres clients, il étend la chaîne des transactions. Supposons que Bob paie son concepteur Web Gopesh à Bangalore pour une nouvelle page Web. Maintenant, la chaîne de transactions ressemblera à [figure\_title](#block-alice2).



La transaction d'Alice dans le cadre d'une chaîne de transactions de Joe à Gopesh, où la sortie d'une transaction est utilisée comme entrée de la transaction suivante

Dans ce chapitre, nous avons vu comment les transactions construisent une chaîne qui déplace la valeur d'un propriétaire à l'autre. Nous avons également suivi la transaction d'Alice, à partir du moment où elle a été créée dans son portefeuille, via le réseau Bitcoin et jusqu'aux mineurs qui l'ont enregistrée sur la chaîne de blocs. Dans le reste de ce livre, nous examinerons les technologies spécifiques derrière les portefeuilles, les adresses, les signatures, les transactions, le réseau et enfin le minage.