Les premières communications publiques
du créateur de Bitcoin

SATOSHI NAKAMOTO

Volume 1

*L'intégralité des échanges sur la Cryptography Mailing List
et la P2P-research list
(2008-2009)*

Archive compilée et traduite par
Urbantech21

Bitcoin P2P e-cash paper

#1

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Fri Oct 31 14:10:00 EDT 2008

The Cryptography Mailing List

J'ai travaillé sur un nouveau système de monnaie électronique qui est entièrement pair à pair, sans tiers de confiance.

Les principales propriétés :

La double dépense est évitée grâce à un réseau pair à pair.

Pas de *mint* ni d'autres tiers de confiance.

Les participants peuvent rester anonymes.

De nouvelles pièces sont fabriquées à partir d'une preuve de travail de style Hashcash.

La preuve de travail pour la génération de nouvelles pièces alimente également le réseau pour prévenir la double dépense.

Bitcoin : Un système de monnaie électronique pair à pair

Résumé. Une version purement pair-à-pair de la monnaie électronique qui permettrait d'envoyer des paiements en ligne directement d'une partie à l'autre sans les contraintes de passer par une institution financière. Les signatures numériques apportent une partie de la solution, mais les principaux avantages sont perdus si une partie de confiance est toujours requise pour prévenir la double-dépense. Nous proposons une solution au problème de la double dépense en utilisant un réseau pair à pair. Le réseau horodate les transactions en les hachant dans une chaîne continue de preuve de travail basée sur le hachage et la preuve de travail, formant un enregistrement qui ne peut pas être modifié sans refaire la preuve de travail.

La chaîne la plus longue ne sert pas seulement de preuve de la séquence des événements observés, mais de preuve qu'elle est venue de la plus grande pool de puissance CPU. Tant que les nœuds honnêtes contrôlent la plus grande puissance CPU sur le réseau, ils peuvent générer la plus longue chaîne et devancer tous les attaquants.

Le réseau lui-même nécessite une structure minimale.

Les messages sont diffusés sur la base du meilleur effort, et les nœuds peuvent quitter et rejoindre le réseau à volonté, acceptant la plus longue chaîne de preuve de travail comme preuve de ce qui s'est passé pendant qu'ils étaient partis.

Satoshi Nakamoto

#2

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sun Nov 2 20:37:43 EST 2008

The Cryptography Mailing List

James A. Donald :

Nous avons vraiment, vraiment besoin d'un tel système, mais d'après ce que je comprends de votre proposition, elle ne semble pas s'adapter à la taille requise. Pour que les jetons de preuve de travail transférables aient de la valeur, ils doivent avoir une valeur monétaire. Pour avoir une valeur monétaire, ils doivent être transférés au sein d'un très grand réseau - par exemple un réseau d'échange de fichiers semblable à bittorrent.

Pour détecter et rejeter un événement de double dépense en temps opportun, il faut avoir la plupart des transactions passées des pièces dans la transaction, ce qui, naïvement implémenté, nécessite que chaque pair ait la plupart des transactions passées, ou la plupart des transactions passées qui se sont produites récemment. Si des centaines de millions de personnes effectuent des transactions, c'est une large bande passante - chacun doit connaître tout, ou une partie substantielle de celle-ci.

Satoshi Nakamoto :

Bien avant que le réseau n'atteigne une taille aussi grande, il serait sûr pour les utilisateurs d'utiliser la Vérification Simplifiée des Paiements (section 8) pour vérifier les doubles dépenses, ce qui ne nécessite que d'avoir la chaîne des en-têtes de blocs, soit environ 12 Ko par jour. Seules les personnes essayant de créer de nouvelles pièces auraient besoin de faire fonctionner des nœuds du réseau. Au début, la plupart des utilisateurs feraient fonctionner des nœuds du réseau, mais à mesure que le réseau grandirait, au-delà d'un certain point, il serait de plus en plus laissé aux spécialistes avec des fermes de serveurs dotés de matériel spécialisé. Une ferme de serveurs n'aurait besoin de faire fonctionner qu'un seul nœud sur le réseau et le reste du LAN se connecterait à ce nœud.

La bande passante pourrait ne pas être aussi prohibitive que vous le pensez. Une transaction typique serait d'environ 400 octets (l'ECC est agréablement compact). Chaque transaction doit être diffusée deux fois, donc disons 1 Ko par transaction. Visa a traité 37 milliards de transactions en 2008, soit une moyenne de 100 millions de transactions par jour. Autant de transactions nécessiteraient 100 Go de bande passante, soit la taille de 12 DVD ou de 2 films en qualité HD, ou environ 18 \$ de bande passante aux prix actuels.

Si le réseau devait devenir aussi grand, cela prendrait plusieurs années, et d'ici là, envoyer 2 films en HD sur Internet ne semblerait probablement pas être un gros problème.

Satoshi Nakamoto

#3

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Mon Nov 3 11:23:49 EST 2008

The Cryptography Mailing List

John Levrine :

Satoshi Nakamoto :

« Tant que les nœuds honnêtes contrôlent la plus grande puissance CPU sur le réseau, ils peuvent générer la chaîne la plus longue et devancer tous les attaquants »

Mais ce n'est pas le cas. Les méchants contrôlent régulièrement des fermes de zombies de 100 000 machines ou plus. Les personnes que je connais qui gèrent une liste noire d'envoi de spam, de zombies, me disent qu'ils voient souvent un million de nouveaux zombies par jour.

C'est la même raison pour laquelle le hashcash ne peut pas fonctionner sur l'Internet d'aujourd'hui. Les gentils ont une puissance de calcul largement inférieure à celle des méchants.

Satoshi Nakamoto :

Merci d'avoir soulevé ce point.

Je n'ai pas vraiment formulé cette déclaration aussi fermement que j'aurais pu. La condition est que les gentils aient collectivement plus de puissance CPU qu'un attaquant individuel.

Il y aurait de nombreuses petites fermes de zombies qui ne sont pas assez grandes pour dominer le réseau, et elles pourraient quand même gagner de l'argent en générant des bitcoins. Les plus petites fermes sont alors les "nœuds honnêtes". (J'ai besoin d'un terme meilleur que "honnête") Plus il y a de petites exploitations qui se mettent à générer des bitcoins, plus la barre est haute pour prendre le contrôle du réseau, et à mesure que les exploitations plus grandes sont trop petites pour prendre le contrôle, elles peuvent elles aussi continuer à générer des bitcoins. Selon la théorie de la "longue traîne", les petites, moyennes et simplement grandes fermes additionnées devraient représenter beaucoup plus que la plus grande ferme zombie.

Même si un attaquant parvient à prendre le contrôle du réseau, ça ne veut pas dire qu'il sera instantanément riche. Tout ce qu'il peut faire, c'est récupérer l'argent qu'il a lui-même dépensé, comme faire un chèque sans provision. Pour l'exploiter, il devrait acheter quelque chose à un marchand, attendre qu'il soit expédié, puis prendre le contrôle du réseau et essayer de récupérer son argent. Je ne pense pas qu'il pourrait gagner autant d'argent en essayant de mettre en place un tel système, qu'en générant simplement des bitcoins. Avec une ferme de zombies aussi grande, il pourrait générer plus de bitcoins que tout le monde réuni.

Le réseau Bitcoin pourrait en fait réduire le spam en détournant les fermes zombies vers la génération de bitcoins.

Satoshi Nakamoto

#4

Satoshi Nakamoto satoshi at vistomail.com

Thu Nov 6 15:15:40 EST 2008

The Cryptography Mailing List

Message non référencé , auteur inconnu :

[Exposition longue de la vulnérabilité d'un système à l'utilisation de la force des monopoles éludés.]

Vous ne trouverez pas de solution aux problèmes politiques dans la cryptographie.

Satoshi Nakamoto :

Oui, mais nous pouvons gagner une bataille majeure dans la course aux armements et obtenir un nouveau territoire de liberté pour plusieurs années.

Les gouvernements sont bons pour couper les têtes des réseaux centralisés et contrôlés comme Napster, mais les réseaux P2P purs comme Gnutella et Tor semblent tenir bon.

Satoshi Nakamoto

#5

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sat Nov 8 13:54:38 EST 2008

The Cryptography Mailing List

Ray Dillinger :

Je pense que le véritable problème avec ce système est le marché pour les bitcoins. Le calcul des preuves de travail n'a aucune valeur intrinsèque. On peut avoir une courbe d'offre limitée (bien que la "monnaie" soit inflationniste à environ 35 % car c'est la vitesse à laquelle les ordinateurs progressent chaque année, mais il n'y a pas de courbe de demande qui l'intersecte à un prix positif.

Je sais que la même chose (absence de valeur intrinsèque) peut être dite des monnaies fiduciaires, mais une demande artificielle pour les monnaies fiduciaires est créée par (entre autres) la fiscalité et les lois sur la monnaie légale. De plus, même une monnaie fiduciaire peut être une protection contre l'inflation par rapport à une autre monnaie fiduciaire à taux d'inflation plus élevé. Mais dans le cas des bitcoins le taux d'inflation de 35 % est presque garanti par la technologie, il n'y a pas de mécanismes de soutien tels que la fiscalité, et aucune loi sur la monnaie légale. Les gens ne détiendraient pas d'actifs dans cette monnaie à forte inflation si ils on le choix.

Satoshi Nakamoto :

L'augmentation de la vitesse du matériel est prise en compte : "Pour compenser l'augmentation de la vitesse du matériel et l'intérêt variable pour faire fonctionner des nœuds au fil du temps, la difficulté de la preuve de travail est déterminée par une moyenne mobile visant un nombre moyen de blocs par heure." Si les blocs sont générés trop rapidement, la difficulté augmente."

À mesure que les ordinateurs deviennent plus rapides et que la puissance de calcul totale appliquée à la création de bitcoins augmente, la difficulté augmente proportionnellement pour maintenir la production totale, constante. Ainsi, nous connaissons à l'avance combien de nouveaux bitcoins seront créés chaque année dans l'avenir.

Le fait que de nouvelles pièces soient produites signifie que l'offre monétaire augmente à un montant prévu, mais cela ne se traduit pas nécessairement par de l'inflation. Si l'offre de monnaie augmente au même rythme que le nombre de personnes qui l'utilisent, les prix restent stables. Si elle n'augmente pas aussi rapidement que la demande, il y aura déflation et les premiers détenteurs de l'argent verront sa valeur augmenter.

Les pièces doivent être initialement distribuées d'une manière ou d'une autre, et un taux constant semble être la meilleure formule.

Satoshi Nakamoto

#6

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sat Nov 8 20:58:48 EST 2008

The Cryptography Mailing List

Hal Finney :

il est mentionné que si une transaction diffusée n'atteint pas tous les nœuds, c'est acceptable, car cela finira par entrer dans la chaîne de blocs. Comment cela se produit-il que se passe-t-il si le nœud qui crée le "prochain" bloc (le premier nœud trouver la collision hashcash) n'a pas entendu parler de la transaction, et ensuite quelques blocs supplémentaires sont ajoutés également par des nœuds qui n'en n'ont pas entendu parler non plus ? Est-ce que tous les nœuds qui l'ont entendu conservent cette transaction en attente, espérant l'incorporer dans un bloc si ils sont assez chanceux pour être celui qui trouve la prochaine collision ?

Satoshi Nakamoto :

Exactement, les nœuds conservent les transactions dans leur ensemble de travail jusqu'à ce qu'elles soient intégrées dans un bloc. Si une transaction atteint 90 % des nœuds, alors chaque fois qu'un nouveau bloc est trouvé, elle a 90 % de chances d'y être incluse.

Hal Finney :

Ou par exemple, que se passe-t-il si un nœud garde deux chaînes ou plus en attente, t attend de voir laquelle croît le plus rapidement, et un bloc arrive pour la chaîne A ce qui inclurait une double dépense d'une pièce qui est dans la chaîne B ? Est-ce que cela vérifié ou pas ? (Cela pourrait se produire si quelqu'un a dépensé deux fois et que deux différents ensembles de nœuds ont entendu parler des deux transactions différentes avec la même pièce.)

Satoshi Nakamoto :

Cela n'a pas besoin d'être vérifié. La transaction dans la branche qui finit par prendre de l'avance devient la valide, l'autre est invalide. Si quelqu'un essaie de dépenser deux fois de cette manière, une seule dépense deviendra toujours valide, les autres seront invalides.

Les destinataires des transactions devront normalement conserver les transactions pendant peut-être une heure ou plus pour permettre à ce genre de possibilité d'être résolu. Ils peuvent toujours dépenser à nouveau les pièces immédiatement, mais ils devraient attendre avant d'effectuer une action telle que l'expédition de marchandises.

Hal Finney :

Je ne comprends pas non plus exactement comment la double dépense, ou l'annulation des transactions, est accompli par un attaquant supérieur qui est capable de rassembler plus de puissance de calcul que tous les participants honnêtes. Je vois qu'il peut créer de nouveaux blocs et les ajouter pour créer la plus longue chaîne, mais comment il efface ou ajoute des anciennes transactions dans la chaîne ?

Alors que l'attaquant envoie ses nouveaux blocs, n'y a-t-il pas des vérifications de cohérence que les nœuds honnêtes peuvent effectuer, pour s'assurer que rien n'a été effacé ? Plus d'explications à ce sujet attaque serait utile, afin de juger les gains pour un attaquant de cela, par rapport à simplement utiliser sa puissance de calcul pour frapper de nouvelles pièces honnêtement.

Satoshi Nakamoto :

L'attaquant n'ajoute pas de blocs à la fin. Il doit revenir en arrière et refaire le bloc dans lequel se trouve sa transaction ainsi que tous les blocs suivants, tout en continuant de rattraper les nouveaux blocs que le réseau continue d'ajouter à la fin pendant qu'il est en train de faire cela. Il réécrit l'histoire. Une fois que sa branche est plus longue, elle devient la nouvelle branche valide.

Il est strictement nécessaire que la chaîne la plus longue soit toujours considérée comme la chaîne valide. Les nœuds qui étaient présents peuvent se souvenir qu'une branche était là en premier et a été remplacée par une autre, mais il n'y aurait aucun moyen pour eux de convaincre ceux qui n'étaient pas présents, de cela. Nous ne pouvons pas avoir de sous-factions de nœuds qui s'accrochent à une branche qu'ils pensent être la première, d'autres qui ont vu une autre branche en premier, et d'autres qui ont rejoint plus tard et n'ont jamais vu ce qui s'est passé. Le vote de preuve de travail via la puissance CPU doit avoir le dernier mot. La seule façon pour que tout le monde soit sur la même longueur d'onde est de croire que la chaîne la plus longue est toujours la chaîne valide, quoi qu'il arrive.

Hal Finney :

En ce qui concerne les transactions de dépense, quelles vérifications le destinataire d'une pièce doit-il effectuer ? Doit-elle revenir sur l'ensemble de l'historique histoire des transferts, et s'assurer que chaque transaction de la liste est effectivement lié à la chaîne de blocs "timestamp" ? Ou peut-elle simplement faire le la plus récente ?

Satoshi Nakamoto :

Le destinataire n'a besoin de vérifier que jusqu'à une profondeur suffisamment éloignée dans la chaîne de blocs, ce qui nécessitera souvent seulement une profondeur de 2 transactions. Toutes les transactions avant cela peuvent être ignorées.

Hal Finney :

Les nœuds d'horodatage vérifient-ils les transactions, en s'assurant que la transaction précédente sur une pièce est dans la chaîne, en appliquant ainsi la règle selon laquelle toutes les transactions dans la chaîne représentent des pièces valides ?

Satoshi Nakamoto :

Exactement, c'est ça. Lorsqu'un nœud reçoit un bloc, il vérifie les signatures de chaque transaction qu'il contient par rapport aux transactions précédentes dans les blocs. Les blocs ne peuvent contenir que des transactions qui dépendent de transactions valides dans des blocs antérieurs ou dans le même bloc. La transaction C pourrait dépendre de la transaction B dans le même bloc et B dépend de la transaction A dans un bloc précédent.

Hal Finney :

Désolé pour toutes les questions, mais comme je l'ai dit, cela semble être une idée très prometteuse et originale, et j'ai hâte de voir comment le concept sera davantage développé. Il serait utile de voir une description plus description orientée vers le processus de l'idée, avec des détails concrets sur les structures de données pour les différents objets (pièces, blocs, transactions), les données qui sont incluses dans les messages, et les descriptions algorithmiques des procédures pour gérer les divers événements qui se produiraient dans ce système. Vous avez mentionné que vous travaillez sur une mise en œuvre, mais je pense qu'une description textuelle plus formelle du système serait une étape suivante utile.

Satoshi Nakamoto :

J'apprécie vos questions. En fait, j'ai fait cela un peu à l'envers. J'ai dû écrire tout le code avant de pouvoir me convaincre que je pouvais résoudre tous les problèmes, puis j'ai écrit l'article. Je pense que je pourrai publier le code plus tôt que je ne pourrais écrire une

spécification détaillée. Tu as déjà raison sur la plupart de tes suppositions où tu as comblé les blancs.

Satoshi Nakamoto

#7

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sat Nov 8 22:09:49 EST 2008

The Cryptography Mailing List

James A. Donald :

Le concept de base est que de nombreuses entités conservent des informations complètes et cohérentes sur qui possède quels bitcoins. Mais maintenir la cohérence est délicat. Je ne comprends pas ce qui se passe lorsque quelqu'un transmet une transaction à un détenteur, et quelqu'un d'autre transmet une autre transaction à un autre détenteur. Le transaction ne peut être considérée comme valide tant qu'elle n'a pas été incorporée dans une vue partagée globalement de toutes les transactions passées, et personne ne peut savoir qu'une vue globalement partagée est effectivement partagée jusqu'à un certain temps, et après de nombreuses nouvelles transactions sont arrivées.

Avez-vous expliqué comment faire cela, car ça m'a simplement échappé, ou étiez-vous sûre que c'était faisable ? C'est un peu vague sur les détails ?

Satoshi Nakamoto :

La chaîne de preuve de travail est la solution au problème de synchronisation, elle permet de savoir quelle est la vue partagée globalement sans avoir à faire confiance à qui que ce soit.

Une transaction se propagera rapidement à travers le réseau, donc si deux versions de la même transaction étaient signalées presque en même temps, celle qui aurait une avance aurait un grand avantage en atteignant beaucoup plus de nœuds en premier. Les nœuds n'accepteront que la première transaction qu'ils voient, refusant la seconde qui arrive, donc la première transaction aurait beaucoup plus de nœuds travaillant à l'incorporer dans la

prochaine preuve de travail. En effet, chaque nœud vote pour son point de vue sur la transaction qu'il a vue en premier en l'incluant dans son effort de preuve de travail.

Si les transactions arrivent exactement au même moment et qu'il y avait une répartition égale, c'est une question de chance basée sur celle qui est incluse dans une preuve de travail en premier, et cela décide laquelle est valide.

Lorsqu'un nœud trouve une preuve de travail, le nouveau bloc est propagé à travers le réseau et tout le monde l'ajoute à la chaîne et commence à travailler sur le bloc suivant. Tous les nœuds qui avaient l'autre transaction cesseront d'essayer de l'inclure dans un bloc, car elle est désormais invalide selon la chaîne acceptée.

La chaîne de preuve de travail est en elle-même une preuve évidente qu'elle provient de la vision partagée globalement. Seule la majorité du réseau ensemble dispose de suffisamment de puissance CPU pour générer une chaîne de preuve de travail aussi difficile. Tout utilisateur, en recevant la chaîne de preuve de travail, peut voir ce que la majorité du réseau a approuvé. Une fois qu'une transaction est hachée dans un lien qui se trouve quelques liens en arrière dans la chaîne, elle est fermement gravée dans l'histoire mondiale.

Satoshi Nakamoto

#8

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sun Nov 9 11:31:26 EST 2008

The Cryptography Mailing List

James A. Donald :

D'accord, supposons qu'un nœud incorpore une série de transactions dans sa preuve de travail, toutes honnêtes, légitimes et correspondant à des dépenses uniques, et un autre nœud intègre une différente série de transactions dans sa preuve de travail, toutes également honnêtes, légitimes et à dépense unique, et les deux preuves sont générées à peu près en même temps.

Que se passe-t-il alors ?

Satoshi Nakamoto :

Ils diffusent tous les deux leurs blocs. Tous les nœuds les reçoivent et conservent les deux, mais ne travaillent que sur celui qu'ils ont reçu en premier. Supposons que exactement la moitié ait reçu l'un en premier, l'autre moitié l'autre.

Dans peu de temps, toutes les transactions auront fini de se propager de sorte que tout le monde dispose de l'ensemble complet. Les nœuds travaillant de chaque côté essaieront d'ajouter les transactions qui manquent de leur côté. Lorsque la prochaine preuve de travail est trouvée, quel que soit le bloc précédent sur lequel ce nœud travaillait, cette branche devient plus longue et la situation est résolue. Quelle que soit la branche, le nouveau bloc contiendra l'autre moitié des transactions, donc dans tous les cas, la branche contiendra toutes les transactions. Même dans le cas peu probable où une scission se produirait deux fois de suite, les deux côtés de la deuxième scission contiendraient de toute façon l'ensemble des transactions.

Ce n'est pas un problème si les transactions doivent attendre un ou quelques cycles supplémentaires pour entrer dans un bloc.

Satoshi Nakamoto

#9

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sun Nov 9 21:14:30 EST 2008

The Cryptography Mailing List

James A. Donald :

De plus, cela ne peut pas fonctionner, car dans le système proposé, le travail de suivi de qui possède quelles pièces est financé par le seigneurage, ce qui nécessite de l'inflation.

Satoshi Nakamoto :

Si vous avez des problèmes avec la question de l'inflation, il est facile de l'ajuster pour les frais de transaction à la place. C'est aussi simple que cela : laissez la valeur de sortie de toute transaction est inférieure d'un centime à la valeur d'entrée. Soit le logiciel client écrit automatiquement des transactions pour un centime de plus que la valeur de paiement

prévue, soit cela pourrait venir du côté du bénéficiaire. La valeur incitative lorsqu'un nœud trouve une preuve de travail pour un bloc pourrait être le total des frais dans le bloc.

Satoshi Nakamoto

#10

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Mon Nov 10 17:18:20 EST 2008

The Cryptography Mailing List

James A. Donald :

Alors, qu'est-il arrivé à la pièce qui a perdu la course ?

c'est un peu sévère si le gars qui est arrivé deuxième est susceptible de perdre sa pièce.

Satoshi Nakamoto :

Lorsqu'il y a plusieurs versions de la même transaction dépensée deux fois, une seule et unique version deviendra valide.

Le destinataire d'un paiement doit attendre environ une heure avant de croire qu'il est valide. Le réseau résoudra alors toute éventuelle course de double dépense.

Celui qui a reçu la double dépense qui est devenue invalide n'a jamais pensé qu'il la possédait en premier lieu. Son logiciel aurait indiqué que la transaction était passée de « non confirmée » à « invalide ». Si nécessaire, l'interface utilisateur peut être configurée pour masquer les transactions jusqu'à ce qu'elles soient suffisamment profondes dans la chaîne de blocs.

James A. Donald :

De plus, votre description des événements implique des restrictions sur le timing et la génération de pièces - à savoir que l'ensemble du réseau génère des pièces plus lentement par rapport au temps nécessaire à une nouvelle pièce inonder le réseau.

Satoshi Nakamoto :

Désolé si je ne l'ai pas précisé. Le temps cible entre les blocs sera probablement de 10 minutes.

Chaque bloc inclut son heure de création. Si le temps est décalé de plus de 36 heures, les autres nœuds ne travailleront pas dessus. Si la période écoulée sur les 6*24*30 derniers blocs est inférieure à 15 jours, les blocs sont générés trop rapidement et la difficulté de la preuve de travail double. Tout le monde effectue le même calcul avec les mêmes données de chaîne, donc ils obtiennent tous le même résultat du même maillon de la chaîne.

James A. Donald :

Nous voulons que les dépensiers aient la certitude que leur transaction est valide au moment où elle inonde le réseau, pas au moment où la course entre les branches est résolue.

Satoshi Nakamoto :

La non-répudiation instantanée n'est pas une fonctionnalité, mais c'est quand même beaucoup plus rapide que les systèmes existants. Les chèques papier peuvent être rejetés jusqu'à une ou deux semaines plus tard. Les transactions par carte de crédit peuvent être contestées jusqu'à 60 à 180 jours plus tard. Les transactions Bitcoin peuvent être suffisamment irréversibles en une heure ou deux.

James A. Donald :

Si un nœud ignore toutes les dépenses dont il ne se soucie pas, il ne subit aucune conséquence négative.

Satoshi Nakamoto :

Avec le système d'incitation basé sur les frais de transaction que j'ai récemment proposé, les nœuds auraient une incitation à inclure toutes les transactions payantes qu'ils reçoivent.

Satoshi Nakamoto

#11

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Thu Nov 13 17:56:55 EST 2008

The Cryptography Mailing List

James A. Donald :

Il ne suffit pas que tout le monde connaisse X. Nous avons également besoin que tout le monde sache que tout le monde sait X, et que tout le monde sait que tout le monde sait que tout le monde sait X ce qui, comme dans le problème des généraux byzantins, est le problème classique et difficile du traitement distribué des données.

Satoshi Nakamoto :

La chaîne de preuve de travail est une solution au problème des généraux byzantins. Je vais essayer de le reformuler dans ce contexte.

Un certain nombre de généraux byzantins ont chacun un ordinateur et veulent attaquer le Wi-Fi du roi en forçant le mot de passe, dont ils ont appris qu'il avait une certaine longueur en caractères. Une fois qu'ils stimulent le réseau pour générer un paquet, ils doivent craquer le mot de passe dans un temps limité pour pénétrer et effacer les journaux, sinon ils seront découverts et auront des ennuis. Ils n'ont suffisamment de puissance CPU pour le craquer rapidement que si la majorité d'entre eux attaquent en même temps.

Ils ne se soucient pas particulièrement du moment de l'attaque, juste qu'ils soient tous d'accord. Il a été décidé que quiconque le souhaite annoncera une heure, et quelle que soit l'heure entendue en premier, ce sera l'heure officielle de l'attaque. Le problème est que le réseau n'est pas instantané, et si deux généraux annoncent des heures d'attaque différentes presque en même temps, certains peuvent entendre l'une en premier et d'autres entendre l'autre en premier.

Ils utilisent une chaîne de preuve de travail pour résoudre le problème. Une fois que chaque général reçoit le premier temps d'attaque qu'il entend, il configure son ordinateur pour résoudre un problème de preuve de travail extrêmement difficile qui inclut le temps d'attaque dans son hachage. La preuve de travail est si difficile qu'il est prévu qu'il leur faudra 10 minutes de travail simultané avant que l'un d'eux ne trouve une solution. Une fois qu'un des généraux trouve une preuve de travail, il la diffuse sur le réseau, et tout le monde change son calcul de preuve de travail actuel pour inclure cette preuve de travail dans le hachage sur lequel ils travaillent. Si quelqu'un travaillait sur un autre temps d'attaque, il passe à celui-ci, car sa chaîne de preuve de travail est maintenant plus longue.

Après deux heures, un temps d'attaque devrait être haché par une chaîne de 12 preuves de travail. Chaque général, simplement en vérifiant la difficulté de la chaîne de preuve de

travail, peut estimer combien de puissance CPU parallèle par heure y a été dépensée et voir qu'il a dû falloir la majorité des ordinateurs pour produire autant de preuve de travail dans le temps imparti. Ils devaient tous l'avoir vu parce que la preuve de travail est la preuve qu'ils ont travaillé dessus. Si la puissance CPU exhibée par la chaîne de preuve de travail est suffisante pour craquer le mot de passe, ils peuvent attaquer en toute sécurité à l'heure convenue.

La chaîne de preuve de travail est la manière dont tous les problèmes de synchronisation, de base de données distribuée et de vue globale que vous avez mentionnés sont résolus.

James A. Donald :

Si la nouvelle chaîne est acceptée, alors ils abandonnent l'ajout de leur lien actuel, déversent toutes les transactions du pool L dans le pool A (ainsi que les transactions qu'ils ont reçues ou créées depuis qu'ils ont commencé à travailler), éliminer du pool A ces enregistrements de transactions qui font déjà partie d'un lien dans la nouvelle chaîne, et recommencez à travailler pour essayer d'étendre la nouvelle chaîne.

Satoshi Nakamoto :

D'accord. Ils se mettent aussi à jour dès qu'une nouvelle transaction arrive, donc L contient à peu près tout ce qu'il y a dans A tout le temps.

James A. Donald :

Algorithme de signature numérique intensif en CPU pour signer la chaîne y compris le nouveau bloc L.

Satoshi Nakamoto :

C'est une preuve de travail de style Hashcash SHA-256 (pré-image partielle de zéro), pas une signature.

Y a-t-il un mécanisme pour s'assurer que la "chaîne" ne se compose pas

James A. Donald :

uniquement de liens ajoutés par seulement les 3 ou 4 nœuds les plus rapides ? Parce qu'un l'enregistrement des transactions diffusées pourrait facilement manquer ces 3 ou 4 nœuds et si c'est le cas, et que ces nœuds continuent de dominer la chaîne, la transaction pourrait ne jamais être ajoutée.

Satoshi Nakamoto :

Si vous le considérez comme une signature numérique gourmande en CPU, alors vous pensez peut-être à une course pour terminer une longue opération en premier, où le plus rapide gagne toujours.

La preuve de travail est une recherche de collision SHA-256 de style Hashcash. C'est un processus sans mémoire où vous effectuez des millions de hachages par seconde, avec une petite chance d'en trouver un à chaque fois. La domination des 3 ou 4 nœuds les plus rapides ne serait que proportionnelle à leur part de la puissance totale du CPU. La chance de chacun de trouver une solution à tout moment est proportionnelle à sa puissance CPU.

Il y aura des frais de transaction, donc les nœuds auront une incitation à recevoir et à inclure toutes les transactions qu'ils peuvent. Les nœuds seront finalement compensés uniquement par les frais de transaction lorsque le nombre total de pièces créées atteindra le plafond prédéterminé.

James A. Donald :

De plus, l'exigence de travail pour ajouter un maillon à la chaîne devrait varier (encore une fois de manière exponentielle) avec le nombre de liens ajoutés à cette chaîne la semaine précédente, ce qui permet de strictement contrôler le taux de génération de pièces et donc l'inflation.

Satoshi Nakamoto :

D'accord.

Vous avez besoin d'agrégation de pièces pour que cela puisse se développer. Il doit y avoir une transaction "prouvable" où quelqu'un retire dix pièces uniques

James A. Donald :

Et crée une nouvelle pièce de monnaie de dénomination dix, etc.

Satoshi Nakamoto :

Chaque transaction est l'une de celles-ci. Section 9, Combiner et Diviser la Valeur.

Satoshi Nakamoto

#12

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Fri Nov 14 13:55:35 EST 2008

The Cryptography Mailing List

Hal Finney :

Je pense qu'il est nécessaire que les nœuds gardent une liste séparée des transactions en attente associée à chaque chaîne candidate.

... On pourrait également se demander ... Combien de chaînes candidate un nœud donné doit-il suivre en moyenne à un moment donné ?

Satoshi Nakamoto :

Heureusement, il n'est nécessaire de maintenir un pool de transactions en attente que pour la meilleure branche actuelle. Lorsqu'un nouveau bloc arrive pour la meilleure branche, ConnectBlock retire les transactions du bloc du pool de transactions en attente. Si une autre branche devient plus longue, elle appelle DisconnectBlock sur la branche principale jusqu'à la fourche, renvoyant les transactions du bloc au pool de transactions en attente, et appelle ConnectBlock sur la nouvelle branche, récupérant toutes les transactions qui étaient dans les deux branches. Il est prévu que des réorganisations comme celle-ci soient rares et superficielles.

Avec cette optimisation, les branches candidates ne sont pas vraiment une charge. Elles restent simplement sur le disque et ne nécessitent pas d'attention à moins qu'ils ne deviennent la chaîne principale.

Hal Finney :

Ou comme James l'a soulevé plus tôt, si le réseau diffuse est fiable mais dépend d'un algorithme d'inondation potentiellement lent, comment cela impacte-t-il la performance ?

Satoshi Nakamoto :

Les diffusions seront probablement presque entièrement fiables. Les transmissions TCP sont rarement interrompues de nos jours, et le protocole de diffusion dispose d'un mécanisme de réessai pour récupérer les données des autres nœuds après un certain temps. Si les diffusions s'avèrent plus lentes en pratique que prévu, le temps cible entre les blocs devra peut-être être augmenté pour éviter de gaspiller des ressources. Nous voulons que les blocs se propagent généralement en beaucoup moins de temps qu'il n'en faut pour les générer, sinon les nœuds passeraient trop de temps à travailler sur des blocs obsolètes.

Je prévois de lancer un test automatisé avec des ordinateurs envoyant des paiements les uns aux autres de manière aléatoire et perdant des paquets de manière aléatoire.

Hal Finney :

3. Le système bitcoin s'avère socialement utile et précieux, de sorte que les opérateurs de nœuds sentent qu'ils apportent une contribution bénéfique au monde par leurs efforts (similaire aux divers calculs "@Home" des projets où les gens mettent leurs ressources informatiques à disposition pour de bonnes causes). Dans ce cas, il me semble que le simple altruisme peut suffire à maintenir le réseau en fonctionnement.

Satoshi Nakamoto :

C'est très attrayant d'un point de vue libertarien si on peut l'expliquer correctement. Je suis meilleur avec le code qu'avec les mots, cependant.

Satoshi Nakamoto

#13

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Fri Nov 14 13:55:35 EST 2008

The Cryptography Mailing List

Je vais essayer de me dépêcher et de publier le code source dès que possible pour servir de référence afin de clarifier toutes ces questions d'implémentation.

Ray Dillinger :

Lorsqu'une pièce est dépensée, l'acheteur et le vendeur signent numériquement un enregistrement de transaction (aveuglé). Enregistrement de transaction.

Satoshi Nakamoto :

Seul l'acheteur signe, et il n'y a pas d'aveuglement.

Ray Dillinger :

Si quelqu'un dépense deux fois, alors l'enregistrement de la transaction peut être démasqué, révélant l'identité du tricheur.

Satoshi Nakamoto :

Les identités ne sont pas utilisées, et il n'y a pas de recours. Ce n'est que de la prévention.

Ray Dillinger :

Cela se fait via un algorithme de cut-and-choose assez standard, où l'acheteur répond à plusieurs défis avec des parts secrètes

Satoshi Nakamoto :

Pas de défis ni de parts secrètes. Une transaction de base est exactement ce que vous voyez dans la figure de la section 2. Une signature (de l'acheteur) satisfaisant la clé publique de la transaction précédente, et une nouvelle clé publique (du vendeur) qui doit être satisfaite pour la dépenser la prochaine fois.

Ray Dillinger :

Ils peuvent également recevoir des chaînes aussi longues que celle qu'ils essaient d'étendre pendant qu'ils travaillent, dans lequel les dernières "maillons" sont des maillons qui ne sont *pas* en commun avec la chaîne sur laquelle ils travaillent. Ceux-là, ils les ignorent.

Satoshi Nakamoto :

D'accord, si c'est de la même longueur, les égalités sont départagées en gardant le premier reçu.

Ray Dillinger :

S'il contient une double dépense, alors ils créent une "transaction" qui est une preuve de double dépense, l'ajoutent à leur pool A, la diffusent, et continuent à travailler.

Satoshi Nakamoto :

Il n'est pas nécessaire de signaler une "preuve de double dépense" de cette manière. Si la même chaîne contient les deux dépenses, alors le bloc est invalide et rejeté.

Il en va de même si un bloc n'avait pas assez de preuve de travail. Ce bloc est invalide et rejeté. Il n'est pas nécessaire de diffuser un rapport à ce sujet. Chaque nœud peut le voir et le rejeter avant de le relayer.

S'il y a deux chaînes concurrentes, chacune contenant une version différente de la même transaction, l'une essayant de donner de l'argent à une personne et l'autre essayant de donner le même argent à quelqu'un d'autre, résoudre laquelle des dépenses est valide est ce dont toute la chaîne de preuve de travail parle.

Nous ne sommes pas "à l'affût" des doubles dépenses pour tirer la sonnette d'alarme et attraper le tricheur. Nous ne faisons que juger laquelle des dépenses est valide. Les destinataires des transactions doivent attendre quelques blocs pour s'assurer que la résolution a eu le temps de se compléter. Les tricheurs potentiels peuvent essayer de dépenser deux fois en même temps autant qu'ils le souhaitent, et tout ce qu'ils accomplissent, c'est qu'en quelques blocs, l'une des dépenses devient valide et les autres deviennent invalides. Toute double-dépense ultérieure est immédiatement rejetée une fois qu'il y a déjà une dépense dans la chaîne principale.

Même si une dépense antérieure n'était pas encore dans la chaîne, si elle était déjà dans les pools de tous les nœuds, alors la deuxième dépense serait rejetée par tous ces nœuds qui ont déjà la première dépense.

Satoshi Nakamoto

#14

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sat Nov 15 13:02:00 EST 2008

The Cryptography Mailing List

Ray Dillinger:

Une façon de le faire serait de faire en sorte que la personne recevant la pièce génère une paire de clés asymétriques paire de clés, puis d'en publier la moitié avec le transaction. Pour dépenser la pièce plus tard, il/elle doit démontrer la possession de l'autre moitié de la paire de clés asymétriques, probablement en l'utilisant pour signer la clé fournie par le nouveau vendeur.

Satoshi Nakamoto :

D'accord, ce sont des signatures numériques ECC. Une nouvelle paire de clés est utilisée pour chaque transaction.

Ce n'est pas pseudonyme dans le sens où les pseudonymes identifient des personnes, mais cela est au moins un peu pseudonyme en ce sens que la prochaine action sur une pièce peut être identifiée comme provenant du propriétaire de cette pièce.

Ray Dillinger :

Mmmm. Je ne sais pas si je suis à l'aise avec ça. Vous dites qu'il n'y a aucun effort pour identifier et exclure les nœuds qui ne coopèrent pas ? Je soupçonne que cela va causer des problèmes et éventuellement des attaques DOS.

Satoshi Nakamoto :

Il n'y a aucune dépendance à identifier qui que ce soit. Comme vous l'avez dit, c'est futile et peut être facilement contourné avec des faux comptes.

La preuve qui établit quelqu'un comme réel est la capacité de fournir de la puissance CPU.

Ray Dillinger :

Jusqu'à.... jusqu'à quoi ? Comment quelqu'un sait-il quand une transaction est devenue irrévocable ? Est-ce que "quelques" blocs, c'est trois ? Trente ? Un cent ? Est-ce que cela dépend du nombre de nœuds ? Est-ce logarithmique ou linéaire en nombre de nœuds ?

Satoshi Nakamoto :

La section 11 calcule le pire scénario en cas d'attaque. Typiquement, 5 ou 10 blocs suffisent pour ça. Si vous vendez quelque chose qui ne mérite pas une attaque à l'échelle du réseau pour le voler, en pratique vous pourriez le réduire davantage.

Ray Dillinger :

Mais en l'absence d'identité, il n'y a aucun inconvénient pour eux. si les dépenses deviennent invalides, s'ils ont déjà reçu les biens pour lesquels ils ont dépensé deux fois (accès au site web, téléchargement, peu importe). Les marchands se retrouvent avec des pièces "invalides", à moins qu'ils n'attendent ces "quelques blocs" magiques et comment peuvent-ils savoir combien ?) avant de considérer le dépensier comme s'il avait payé. Les consommateurs ne le feront pas si ils dépensent leur argent et que cela prend une heure pour se valider avant qu'ils puissent faire ce pour quoi ils ont dépensé leur argent.

Les commerçants ne le feront pas s'il n'y a pas moyen de rembourser un client lorsqu'ils découvrent que leur pièce est invalide parce que le client a effectué une double dépense.

Satoshi Nakamoto :

C'est un problème de version 2 que je crois pouvoir résoudre assez bien. satisfaisant pour la plupart des applications.

La course consiste à diffuser votre transaction sur le réseau en premier. Pensez à 6 degrés de liberté -- cela se propage de manière exponentielle. Cela ne prendrait que quelque chose comme 2 minutes pour qu'une transaction se propage suffisamment qu'un concurrent commençant tard aurait peu de chances de saisir très nombreux nœuds avant que le premier ne dépasse tout le réseau. Pendant ces 2 minutes, les nœuds du marchand peuvent surveiller un transaction à double dépense. Le double dépensier ne serait pas capable de diffuser sa transaction alternative dans le monde sans que le marchand le recevoir, donc il doit attendre avant de commencer.

Si la transaction réelle atteint 90 % et que la transaction doublement dépensée atteint 10%, le double dépensier n'a qu'une chance de 10% de ne pas payer, et 90% chance que son argent soit dépensé. Pour presque tous les types de biens, cela pas rentable pour l'escroc.

Les biens basés sur l'information, comme l'accès à un site web ou les téléchargements, sont non-clôturable. Personne ne pourra en tirer un revenu. voler l'accès aux sites web ou aux téléchargements. Ils peuvent aller sur les réseaux de partage de fichiers pour voler cela. La plupart des produits à accès instantané n'ont pas une énorme incitation à voler.

Si un commerçant a réellement un problème de vol, il peut faire attendre le faire attendre le client 2 minutes, ou attendre quelque chose par e-mail, ce que beaucoup déjà le font. S'ils veulent vraiment optimiser, et que c'est un gros téléchargement, ils pourraient annuler le téléchargement en cours si le la transaction revient comme étant doublement dépensée. Si c'est l'accès au site web, typiquement, ce ne serait pas un gros problème de laisser l'accès au client pendant 5 minutes et ensuite couper l'accès s'il est rejeté. Beaucoup de ces lessites ont de toute façon un essai gratuit.

Satoshi Nakamoto

#15

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Mon Nov 17 12:24:43 EST 2008

The Cryptography Mailing List

James A. Donald :

Heureusement, il est seulement nécessaire de garder un pool de transactions en attente pour la meilleure branche actuelle. Cela nécessite que nous sachions, c'est-à-dire une personne honnête, un pair bienveillant dont les communications et le stockage des données fonctionne bien sait, quelle est la meilleure branche actuelle -

Satoshi Nakamoto :

Je veux dire qu'un nœud n'a besoin du pool de transactions en attente que pour la meilleure branche qu'il a. La branche qu'il considère actuellement comme la meilleure branche. C'est la branche à partir de laquelle elle essaiera de créer un bloc, ce qui est tout ce dont il a besoin pour la piscine.

James A. Donald :

Les diffusions seront probablement presque complètement fiables.

Plutôt que de supposer que chaque message arrive au moins une fois, nous devons mettre en place un mécanisme tel que le l'information arrive même si elle est transmise par des messages qui échouent fréquemment.

Satoshi Nakamoto :

Je pense que j'ai couvert le mécanisme de diffusion du réseau pair-à-pair.

Chaque nœud envoie à ses voisins une liste d'inventaire des hachages des nouveaux blocs et transactions qu'il possède. nouveaux blocs et transactions qu'il possède. Les voisins demandent les articles qu'ils n'ont pas encore. Si l'article ne parvient jamais après un délai d'attente, ils le demandent à un autre voisin qui l'avait. Puisque tous ou la plupart des voisins devraient finalement avoir chaque article, même si les communications sont brouillées avec l'un d'eux, ils peuvent l'obtenir de n'importe lequel des autres, en essayant un à la fois.

Le schéma de demande de données d'inventaire introduit un peu de latence, mais cela aide finalement à augmenter la vitesse en gardant des blocs de données supplémentaires hors des files d'attente de transmission et en conservant la bande passante.

James A. Donald :

Vous avez un plan et une proposition pour un tel design, ce qui est un grand pas en avant, mais le diable est dans les petits détails.

Satoshi Nakamoto :

Je crois que j'ai travaillé sur tous ces petits détails au cours de l'année et demie écoulée en le codant, et il y en avait beaucoup. Les détails fonctionnels ne sont pas couverts dans l'article, mais le code source arrive bientôt. Je t'ai envoyé les fichiers principaux. (disponible sur demande pour le moment, sortie complète bientôt)

Satoshi Nakamoto

Bitcoin v0.1 released

#1

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Thu Jan 8 14:27:40 EST 2009

The Cryptography Mailing List

Annnonce de la première version de Bitcoin, un nouveau système de monnaie électronique qui utilise un réseau pair-à-pair pour empêcher la double dépense. C'est complètement décentralisé, sans serveur ni autorité centrale.

Si vous pouvez maintenir un nœud en fonctionnement qui accepte les connexions entrantes, vous aiderez vraiment beaucoup le réseau. Le port 8333 de votre pare-feu doit être ouvert pour recevoir les connexions entrantes.

Le logiciel est encore en phase alpha et expérimental. Il n'y a aucune garantie que l'état du système ne devra pas être redémarré à un moment donné si cela devient nécessaire, bien que j'aie fait tout ce que je pouvais pour intégrer l'extensibilité et le versionnage.

Vous pouvez obtenir des pièces en demandant à quelqu'un de vous en envoyer, ou en activant Options->Générer des pièces pour exécuter un nœud et générer des blocs. J'ai rendu la difficulté de la preuve de travail ridiculement facile au départ, donc pendant un certain temps au début, un PC typique sera capable de générer des pièces en seulement quelques heures. Cela deviendra beaucoup plus difficile lorsque la concurrence fera que l'ajustement automatique augmente la difficulté. Les pièces générées doivent attendre 120 blocs pour mûrir avant de pouvoir être dépensées.

Il y a deux façons d'envoyer de l'argent. Si le destinataire est en ligne, vous pouvez entrer son adresse IP et cela se connectera, obtiendra une nouvelle clé publique et enverra la transaction avec des commentaires. Si le destinataire n'est pas en ligne, il est possible d'envoyer à son adresse Bitcoin, qui est un hachage de sa clé publique qu'ils vous donnent. Ils recevront la transaction la prochaine fois qu'ils se connectent et obtiennent le bloc dans lequel elle se trouve dedans. Cette méthode a l'inconvénient de ne pas transmettre d'informations de commentaire, et un peu de vie privée peut être perdu si l'adresse est utilisée plusieurs fois, mais c'est une alternative utile si les deux utilisateurs ne peuvent être en ligne en même temps ou le destinataire ne peut pas recevoir des connexions entrantes.

La circulation totale sera de 21 000 000 de pièces. Il sera distribué aux nœuds du réseau lorsqu'ils créent des blocs, avec la quantité réduite de moitié tous les 4 ans.

premières 4 années : 10 500 000 pièces
les 4 prochaines années : 5 250 000 pièces
prochaines 4 années : 2 625 000 pièces
prochaines 4 années : 1 312 500 pièces
etc...

Quand cela sera épuisé, le système pourra prendre en charge les frais de transaction si nécessaire. C'est basé sur la concurrence du marché libre, et il y aura probablement toujours des nœuds prêts à traiter des transactions gratuitement.

Satoshi Nakamoto

#2

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Fri Jan 16 11:03:14 EST 2009

The Cryptography Mailing List

Dustin D. Trammell :

Satoshi Nakamoto :

Tu sais, je pense qu'il y avait beaucoup plus de gens intéressés dans les années 90, mais après plus d'une décennie de systèmes basés sur des tiers de confiance qui ont échoué (Digicash, etc), ils le voient comme une cause perdue. J'espère qu'ils pourront faire la distinction que c'est la première fois à ma connaissance que nous essayons un système non basé sur la confiance.

Oui, c'était la caractéristique principale qui a attiré mon attention. Oui. Le vrai défi sera de faire en sorte que les gens apprécient réellement les Bitcoins pour qu'ils deviennent une monnaie.

Satoshi Nakamoto :

Je serais surpris que dans 10 ans nous n'utilisions pas la monnaie électronique d'une manière ou d'une autre, maintenant que nous savons comment le faire sans que ce soit inévitablement abandonné lorsque le tiers de confiance a froid aux pieds.

Cela pourrait commencer dans une niche étroite comme des points de récompense, jetons de don, monnaie pour un jeu ou micropaiements sur des sites pour adultes. Initialement,

il peut être utilisé dans des applications de preuve de travail. Pour des services qui pourraient être presque gratuits mais pas tout à fait.

Il peut déjà être utilisé pour les e-mails payants. La boîte de dialogue d'envoi est redimensionnable et vous pouvez entrer un message aussi long que vous le souhaitez. Il est envoyé directement lorsqu'il se connecte. Le destinataire double-clique sur la transaction pour voir le message complet. Si quelqu'un de célèbre reçoit plus de mails qu'ils ne peuvent en lire, mais souhaiteraient quand même avoir un moyen pour que les fans le contact, ils pourraient mettre en place Bitcoin et donner l'adresse IP sur leur site web. Envoyez X bitcoins sur ma ligne directe prioritaire à cette adresse IP et je lirai le message personnellement.

Les sites d'abonnement qui ont besoin d'une preuve de travail supplémentaire pour leur essai gratuit pour ne pas se faire cannibaliser les abonnements, pourrait facturer bitcoins pour l'essai.

Cela pourrait avoir du sens d'en prendre juste au cas où ça marcherait. Si assez de gens pensent de la même manière, cela devient une prophétie auto-réalisatrice. Une fois qu'il sera lancé, il y a tant de applications si vous pouviez facilement payer quelques centimes à un site web aussi facilement que de mettre des pièces dans un distributeur automatique.

Satoshi Nakamoto

#3

Satoshi Nakamoto [satoshi at vistomail.com](mailto:satoshi@vistomail.com)

Sun Jan 25 10:47:10 EST 2009

The Cryptography Mailing List

Hal Finney :

Les botnets de spammeurs pourraient facilement contourner trivialement les filtres de messagerie payants. Si les jetons POW deviennent utiles, et surtout s'ils deviennent de l'argent, les machines ne resteront plus inactives. Les utilisateurs s'attendent à ce que leurs ordinateurs gagnent de l'argent (en supposant que la récompense soit supérieure au coût de fonctionnement). Un ordinateur dont les gains sont volés par un botnet va être plus perceptible pour son propriétaire qu'aujourd'hui, donc nous pourrions nous attendre à ce que dans ce monde, les utilisateurs travaillent plus dur pour entretenir leurs ordinateurs et les nettoyer des infestations de botnets.

Satoshi Nakamoto :

Un autre facteur qui atténuerait le spam si les jetons POW ont de la valeur : il y aurait un motif de profit pour les gens de créer des quantités massives de faux comptes e-mail pour récolter des jetons POW de spam. Ils feraient essentiellement du spam inversé sur les spammeurs avec des boîtes aux lettres automatisées qui collectent leur POW et ne lisent pas le message. Le ratio de fausses boîtes aux lettres par rapport aux vraies personnes pourrait devenir trop élevé pour que le spam soit rentable.

Le processus a le potentiel d'établir la valeur du jeton POW. En premier lieu, puisque les spammeurs qui n'ont pas de botnet pourraient acheter des jetons auprès des collecteurs. Bien que le rachat permettrait de laisser temporairement passer plus de spam, cela ne ferait qu'accélérer le cycle autodestructeur conduisant à trop de collecteurs exploitant les spammeurs.

Il est intéressant de noter qu'un des systèmes e-gold a déjà une forme de spam appelé "dusting". Les spammeurs envoient une petite quantité de poussière d'or. afin de mettre un message de spam dans le champ de commentaire de la transaction. Si le système permettait aux utilisateurs de configurer le paiement minimum qu'ils sont prêts à recevoir, ou au moins le minimum qui peut avoir un message avec cela, les utilisateurs pourraient définir combien ils sont prêts à recevoir payé pour recevoir des spams.

Satoshi Nakamoto

[p2p-research] Bitcoin open source implementation of P2P currency

#1

Satoshi Nakamoto [satoshin at gmx.com](mailto:satoshin@gmx.com)

Wed Feb 11 23:30:54 CET 2009

P2P-research list

J'ai développé un nouveau système de monnaie électronique P2P open source appelé Bitcoin. C'est complètement décentralisé, sans serveur central ni parties de confiance, car tout est basé sur des preuves cryptographiques au lieu de la confiance. Essayez le, ou jetez un œil aux captures d'écran et au document de conception :

Téléchargez Bitcoin v0.1 sur <http://www.bitcoin.org>

Le problème fondamental avec la monnaie conventionnelle est toute la confiance nécessaire pour qu'elle fonctionne.

nécessaire pour le faire fonctionner. La banque centrale doit être digne de confiance pour ne pas dévaluer la monnaie, mais l'histoire des monnaies fiduciaires est pleine de violations de cette confiance. Les banques doivent être dignes de confiance pour garder notre argent et le transférer électroniquement, mais ils le prêtent par vagues de bulles crédit avec à peine une fraction en réserve. Nous devons leur faire confiance pour notre vie privée, leur faire confiance pour ne pas laisser les voleurs d'identité vider nos comptes. Leurs coûts généraux massifs rendent les micropaiements impossibles.

Il y a une génération, les systèmes informatiques à temps partagé multi-utilisateurs avaient un problème similaire. Avant le chiffrement fort, les utilisateurs devaient se fier aux mots de passe pour sécuriser leurs fichiers, plaçant leur confiance dans le système administrateur pour garder leurs informations privées. La vie privée pourrait toujours être contournée par l'administrateur en fonction de son jugement, en pesant le principe de la vie privée par rapport à d'autres préoccupations, ou à la simple demande de ses supérieurs. Puis, le chiffrement fort est devenu accessible au grand public, et la confiance n'était plus nécessaire. Les données pouvaient être sécurisées de manière à ce qu'il soit physiquement impossible pour les autres d'y accéder, peu importe la raison, peu importe l'excuse soit bonne, ou quoi que ce soit.

Il est temps que nous ayons la même chose pour l'argent. Avec une monnaie électronique basée sur preuve cryptographique, sans avoir besoin de faire confiance à un intermédiaire tiers, l'argent peut être sécurisé et les transactions opérées sans effort.

L'un des éléments fondamentaux d'un tel système est la signature numérique.. Une pièce numérique contient la clé publique de son propriétaire. Pour le transférer, le propriétaire signe la pièce avec la clé publique du prochain propriétaire. Tout le monde peut vérifier les signatures pour vérifier la chaîne de propriété. Cela fonctionne bien pour sécuriser la propriété, mais laisse un gros problème non résolu : la double dépense. Tout propriétaire pourrait essayer de dépenser à nouveau une déjà dépensé en le signant à nouveau à un autre propriétaire. La solution habituelle solution est qu'une entreprise de confiance avec une base de données centrale vérifie la double dépense, mais cela revient simplement au modèle de confiance. Dans sa position centrale, l'entreprise peut contourner les utilisateurs, et les frais nécessaires pour soutenir l'entreprise rendent les micropaiements impraticables.

La solution de Bitcoin est d'utiliser un réseau peer-to-peer pour vérifier double dépense. En résumé, le réseau fonctionne comme un serveur de d'horodatage distribué, estampillant la première transaction pour dépenser une pièce. Il profite de la nature de l'information, qui est facile à diffuser mais difficile à étouffer. Pour des détails sur son fonctionnement, consultez le document de conception à :
<http://www.bitcoin.org/bitcoin.pdf>

Le résultat est un système distribué sans point de défaillance unique. Les utilisateurs détiennent les clés cryptographiques de leur propre argent et effectuent des transactions directement avec les uns avec les autres, avec l'aide du réseau P2P pour vérifier les doubles dépenses.

Satoshi Nakamoto
<http://www.bitcoin.org>

#2

Satoshi Nakamoto [satoshin at gmx.com](mailto:satoshin@gmx.com)

Thu Feb 12 20:01:24 CET 2009

P2P-research list

Martien van Steenbergen :

Très intéressant. Est-ce similaire à l'argent numérique anonyme de David Chaum ? Son concept garantit que l'argent est anonyme à moins qu'il ne soit compromis, c'est-à-dire. le même argent dépensé plus d'une fois. Dès qu'il est compromis, le « contrefacteur » est immédiatement exposé publiquement.

Satoshi Nakamoto :

C'est similaire en ce sens qu'il utilise des signatures numériques pour les pièces, mais différent dans l'approche de la confidentialité et de la prévention de la double dépense. Le destinataire d'un paiement en Bitcoin est capable de vérifier s'il s'agit du premier dépensé ou non, et les secondes dépenses ne sont pas acceptées. Il n'y a pas de mode hors ligne où les double dépensiers sont attrapés et honteux après fait, car cela nécessiterait que les participants aient des identités.

Pour protéger la vie privée, les paires de clés ne sont utilisées qu'une seule fois, avec une nouvelle pour chaque transaction. Le propriétaire d'une pièce est simplement celui qui possède sa clé privée.

Bien sûr, la plus grande différence est l'absence de serveur central. Cela était le talon d'Achille des systèmes Chaumiens; lorsque l'entreprise centrale s'est arrêtée, alors la monnaie aussi.

De plus, dans le cas du bitcoin, y a-t-il une quantité limitée de monnaie (ceci doit être géré) ? Ou l'argent est-il créé exactement au moment de la transaction ?

Il y a une offre limitée de monnaie. La circulation sera de 21 000 000 de pièces. Les transactions ne transfèrent que la propriété.

Merci pour vos questions,

Satoshi

#3

Satoshi Nakamoto [satoshin at gmx.com](mailto:satoshin@gmx.com)

Fri Feb 13 03:31:20 CET 2009

P2P-research list

Martien van Steenbergen ::

J'aimerais également voir un soutien pour ne pas avoir à fournir et gérer l'argent. Rendrait la gestion plus facile et moins coûteuse, et en résultat avoir suffisamment d'argent, toujours et partout. Pas de rareté, pas d'abondance, juste la bonne quantité tout le temps, auto-organisée.

Satoshi Nakamoto :

C'est faisable. Il peut être programmé pour suivre n'importe quel ensemble de règles.

Je vois Bitcoin comme une fondation et un premier pas si vous voulez mettre en œuvre des monnaies sociales P2P programmables, comme les idées de Marc et d'autres discutées ici. D'abord, vous avez besoin d'une monnaie P2P normale et basique qui fonctionne. Une fois que cela est établi et prouvé, l'argent intelligent dynamique est une étape.

J'adore l'idée de communautés virtuelles, non géographiques, expérimentant de nouveaux paradigmes économiques.

Martien van Steenbergen :

Ça me rappelle :

AardRock » Wizard Rabbit Treasurer

AardRock » Pekunio

Satoshi Nakamoto :

En effet, c'est très similaire à Pekunio dans le concept de pulvériser des copies redondantes des copies de chaque transaction à un certain nombre de pairs sur le réseau, mais le l'implémentation n'est pas un réseau de réputation comme Wizard Rabbit Treasurer.

En fait, Bitcoin n'utilise pas du tout la réputation. Il voit le réseau comme une grande foule et ne se soucie pas vraiment à qui il parle ou à qui il dit quelque chose, tant qu'au moins l'un d'eux relaie l'information diffusé à travers le réseau. Ça ne lui importe pas parce qu'il n'y a pas manière de lui mentir. Soit vous lui dites la preuve cryptographique de quelque chose, soit il vous ignore.

Martien van Steenbergen :
Connaissez-vous Ripple ?

Satoshi Nakamoto :

En matière de systèmes de confiance, Ripple est unique en répartissant la confiance plutôt que de la concentrer.

Martien van Steenberge :

Le bitcoin est-il également disponible en tant que spécification de protocole (facilitant différentes liaisons et implémentations de langage; s'unir sur les spécifications, rivaliser sur mise en œuvre).

Satoshi Nakamoto :

Il serait préférable de se référer au code source C++. Je prévois de mettre en œuvre une interface pour utiliser le logiciel, envoyer et recevoir des transactions depuis n'importe quelle langue, afin que le code côté serveur puisse facilement l'utiliser pour les sites de commerce électronique basés sur le web.

Satoshi

#4

Satoshi Nakamoto [satoshin at gmx.com](mailto:satoshin@gmx.com)

Fri Feb 13 19:29:45 CET 2009

P2P-research list

Michel Bauwens :

À quel point votre projet est-il opérationnel ? À quelle vitesse pensez-vous que les gens pourront être capables de l'utiliser dans la vie réelle ?

Satoshi Nakamoto :

C'est entièrement opérationnel et le réseau est en pleine expansion. Si vous essayez le logiciel, envoyez-moi votre adresse Bitcoin par e-mail et je vous enverrai quelques pièces.

Nous devons simplement faire passer le mot et continuer à intéresser plus de gens.

Je transmettrai l'introduction de la version dans le prochain message.

Satoshi

#5

Satoshi Nakamoto [satoshin at gmx.com](mailto:satoshin@gmx.com)

Fri Feb 13 19:45:41 CET 2009

P2P-research list

Annnonce de la sortie de Bitcoin, un nouveau système de monnaie électronique peer-to-peer open source système de monnaie électronique entièrement décentralisé, sans serveur central serveur ou parties de confiance. Les utilisateurs détiennent les clés cryptographiques de leur propre argent et effectuent des transactions directement entre eux, avec l'aide du réseau P2P réseau pour vérifier les doubles dépenses.

Windows NT/2000/XP/Vista. Le code C++ open source est inclus.

Télécharger : <http://www.bitcoin.org>

- Décompressez les fichiers dans un répertoire
- Exécutez BITCOIN.EXE
- Il se connecte automatiquement à d'autres nœuds

Si vous pouvez maintenir un nœud en fonctionnement qui accepte les connexions entrantes, vous vraiment aider le réseau énormément. Le port 8333 sur votre pare-feu doit pour être ouvert à recevoir des connexions entrantes.

Vous pouvez obtenir des pièces en demandant à quelqu'un de vous en envoyer, ou en activant Options->Générer des pièces pour exécuter un nœud et générer des blocs. J'ai rendu la la difficulté de preuve de travail ridiculement facile au départ, donc pour un peu de temps au début, un PC typique pourra générer des pièces en seulement quelques heures. Ça deviendra beaucoup plus difficile quand la concurrence rend l'ajustement automatique plus difficile. Pièces générées doivent attendre 120 blocs pour mûrir avant de pouvoir être dépensés.

Il y a deux façons d'envoyer de l'argent. Si le destinataire est en ligne, vous pouvez entrer leur adresse IP et cela se connectera, obtiendra une nouvelle clé publique et envoyer la transaction avec des commentaires. Si le destinataire n'est pas en ligne, cela il est possible d'envoyer à leur adresse Bitcoin, qui est un hachage de leur clé publique qu'ils vous donnent. Ils recevront la transaction la prochaine la prochaine fois qu'ils se connectent et obtiennent le bloc dans lequel il se trouve. Cette méthode a le inconvénient qu'aucune information de commentaire n'est envoyée, et un peu de vie privée peut être perdu si l'adresse est utilisée plusieurs fois, mais c'est une utile alternative si les deux utilisateurs ne peuvent pas être en ligne en même temps ou si le le destinataire ne peut pas recevoir de connexions entrantes.

La circulation totale sera de 21 000 000 pièces. Il sera distribué aux les nœuds du réseau lorsqu'ils créent des blocs, avec la quantité réduite de moitié tous les 4 années.

premières 4 années : 10 500 000 pièces
les 4 prochaines années : 5 250 000 pièces
prochaines 4 années : 2 625 000 pièces
prochaines 4 années : 1 312 500 pièces
etc...

Quand cela sera épuisé, le système pourra prendre en charge les frais de transaction si nécessaire.

C'est basé sur la concurrence du marché libre, et il y aura probablement toujours nœuds prêts à traiter les transactions gratuitement.

Satoshi Nakamoto

Remerciements à :

Ulrich Fromy
Regorski