Les premières communications publiques
du créateur de Bitcoin

SATOSHI NAKAMOTO

Volume 2

L'intégralité des postes et échanges
sur la bitcoin-list
(2008-2010)

Archive compilée et traduite par
Urbantech21

[bitcoin-list]

#1

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Welcome**
December 10, 2008 at 17:00:23 UTC

Bienvenue sur la liste de diffusion Bitcoin !

#2

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin v0.1.2 now available**
January 11, 2009 at 22:32:18 UTC

Satoshi Nakamoto
Bitcoin v0.1.2 est maintenant disponible en téléchargement.

Voir http://www.bitcoin.org pour le lien de téléchargement.

Tous les problèmes que j'ai trouvés se trouvent dans le code qui trouve et se connecte automatiquement à d'autres nœuds, puisque je n'étais pas en mesure de le tester sur le terrain jusqu'à présent. Il y a beaucoup plus de façons dont les connexions peuvent être perturbées sur le vrai Internet.

Bugs corrigés :
- Résolu divers problèmes qui rendaient difficile pour les nouveaux nœuds de voir d'autres nœuds auxquels se connecter.
- Si vous êtes derrière un pare-feu, il ne pourrait recevoir qu'une seule connexion, et la deuxième connexion se déconnecterait constamment et se reconnecter.

Ces problèmes perturbent un peu en l'air le réseau et vont s'aggraver. pire à mesure que de nouveaux utilisateurs arrivent, alors veuillez vous assurer de mettre à niveau.

Satoshi Nakamoto

#3

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin v0.1 Alpha release notes**
January 12, 2009 at 20:20:47 UTC

Satoshi Nakamoto
Notes de version pour Bitcoin v0.1 Alpha

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

Vous pouvez trouver des captures d'écran et le lien de téléchargement à :
http://www.bitcoin.org

Windows uniquement pour l'instant. Le code C++ open source est inclus.

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

Si vous pouvez faire fonctionner un nœud qui accepte les connexions entrantes, vous aiderez vraiment beaucoup le réseau. Le port 8333 de votre le 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 l'état du système ne devra pas être redémarré à un moment donné si cela deviendra nécessaire, bien que j'aie fait tout ce que je pouvais pour intégrer l'extensibilité et 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 petit moment au début, un PC typique pourra générer des pièces en seulement quelques heures. Cela deviendra beaucoup plus difficile lorsque la concurrence fera que l'ajustement automatique augmenter 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 clé 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 leur 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. est envoyé, et une certaine confidentialité peut être perdue 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 d'appels entrants connexions.

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.

4 premières 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 les transactions gratuitement.

Satoshi Nakamoto

#4

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin v0.1.3**
January 12, 2009 at 22:48:23 UTC

Satoshi Nakamoto
On dirait que nous sommes passés à travers avec la pire connexion Internet. Problèmes de connexion. 0.1.3 a corrigé un problème où les communications de votre nœud pouvaient s'interrompre après un certain temps. Le réseau fonctionne beaucoup plus facilement maintenant avec cette version.

Si vous avez réussi à générer un bloc, vous avez vu qu'il a une compte à rebours de maturation avant de pouvoir le dépenser. Une fois qu'il arrive à maturité, la colonne Crédit passera de 0,00 à 50,00. Pour qu'un bloc être valide, il doit être diffusé sur le réseau et entrer dans le chaîne de blocs, c'est pourquoi le fonction *Generate* ne fonctionne pas si vous n'êtes pas connecté. Si vous avez généré un bloc sans être connecté, le réseau ne le saurait pas et continuerait à construire le chaîne sans lui, le laissant derrière, et le compte à rebours de maturation changerait en "(non accepté)" lorsque votre nœud verrait que cela n'a pas été utilisé. Si vous soustrayez 1 de la colonne de statut, c'est ainsi quelle nombreux blocs ont été enchaînés après le vôtre.

Satoshi Nakamoto

#5

From: **Satoshi Nakamoto**
Subject: **Re: [bitcoin-list] Bitcoin v0.1 released**
January 16, 2009 at 18:35:32 UTC

> **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 échoués (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, c'était la caractéristique principale qui a attiré mon attention. Le vrai défi sera de faire en sorte que les gens apprécient réellement les bitcoins afin 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 celé ne soit inévitablement modifié lorsque le tiers de confiance a froid au pieds.

Cela pourrait commencer dans une niche étroite comme les points de récompense, jetons de don, monnaie pour un jeu ou micropaiements pour adultes sites. Initialement, il peut être utilisé dans des applications de preuve de travail. pour des services qui pourraient presque être 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 peut en lire, mais souhaiterait quand même avoir un moyen pour que les fans les contactent, ils pourraient mettre en place Bitcoin et donner son adresse IP sur son 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 cannibaliser les abonnements pourrait facturer bitcoins pour l'essai.

Cela pourrait avoir du sens de s'en procurer au cas où cela deviendrait populaire. 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

#6

From: **Satoshi Nakamoto**
Subject: **Re: [bitcoin-list] Problems**
January 25, 2009 at 16:45:25 UTC

> **Nicholas Bohm: :**
> J'ai eu quelques problèmes en faisant fonctionner Bitcoin : est-ce une liste appropriée pour les signaler (avec environ 70 Ko de pièces jointes) ?

Satoshi Nakamoto :
Quel est le problème que vous avez ?

Si vous m'envoyez directement votre fichier debug.log (il vaut mieux ne pas envoyer de pièces jointes à la liste), je pourrai jeter un coup d'œil à ce qui se passe.

Satoshi Nakamoto

#7

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin v0.1.5 released**
February 4, 2009 at 19:46:04 UTC

Satoshi Nakamoto
La version 0.1.5 est maintenant disponible. Elle inclut la correction du problème que Nicholas avait rencontré, la vérification de l'espace disque plein et des modifications pour essayer d'améliorer certains points qui étaient déroutants.

Un grand merci à Nicholas et Dustin pour toute leur aide et leurs retours !

Lien de téléchargement :
http://sourceforge.net/project/showfiles.php?group_id=244765&package_id=298441

Modifications :
- Avertissement en cas de disque plein
- Correction d'un bug qui pouvait survenir si la recherche DNS échouait
- Empêcher l'ajout de votre propre adresse dans le carnet d'adresses, ce qui pouvait prêter à confusion en changeant l'étiquette de votre propre adresse
- Déplacement du bouton de changement d'adresse dans le menu sous Options
- Ajustements pour se connecter plus rapidement
- Fermeture des sockets à la sortie
- Création d'un tarif minimum pour les transactions inférieures à 1 centime
- Masquage de la boîte de sélection du type de transaction qui n'avait qu'un seul choix
- Nettoyage du code de ParseMoney
- Formatage légèrement plus propre du texte des messages

- Changement de police dans la boîte de dialogue des détails de la transaction
- Ajout d'un texte explicatif aux détails de la transaction pour les pièces générées
- Reformulation de la description des transactions reçues avec l'adresse Bitcoin

Satoshi Nakamoto

#8

From: **Satoshi Nakamoto**
Subject: **Re: [bitcoin-list] Bitcoin v0.1.5 released**
February 22, 2009 at 17:47:52 UTC

Satoshi Nakamoto
Qu'est-ce qui vient ensuite ?

La prochaine étape pour la version 0.1.6 est de tirer parti de plusieurs processeurs pour générer des blocs. Actuellement, il ne démarre qu'un seul. thread. Si vous avez un processeur multi-cœurs comme un Core Duo ou Quad, cela doublera ou quadruplera votre production.

Plus tard, je veux ajouter des interfaces pour faciliter vraiment l'intégration. dans des sites web à partir de n'importe quel langage côté serveur.

Satoshi

#9

From: **Satoshi Nakamoto**
Subject: **Re: [bitcoin-list] Bitcoin v0.1.5 released**
March 4, 2009 at 16:59:12 UTC

Hal Finney :
Ça a l'air bien. J'aimerais également pouvoir faire fonctionner plusieurs générateurs de pièces/blocs sur plusieurs machines, toutes derrière une seule adresse NAT. Je n'ai pas encore essayé cela, donc je ne sais pas si ça fonctionne avec le logiciel actuel.

Satoshi Nakamoto :
La version actuelle fonctionnera bien. Ils se connecteront chacun via le Internet, tandis que les connexions entrantes ne vont qu'à l'hôte vers lequel le port 8333 est routé.

Comme optimisation, je vais faire un changement "-connect=1.2.3.4" pour que le noeud ne se connecte qu'à une adresse spécifique. Vous pourriez faire en sorte que vos nœuds supplémentaires les nœuds se connectent à votre nœud principal, et que seul le nœud principal se connecte à l'Internet. Cela n'a pas vraiment d'importance pour l'instant, puisque le réseau devrait devenir énorme avant que la bande passante ne soit autre chose que trivial.

Au fait Je ne me souviens pas si nous en avons parlé, mais l'autre jour, certaines des gens parlaient de l'horodatage sécurisé. Vous voulez pouvoir prouver qu'un certain document existait à un certain moment dans le passé. Il me semble que la pile de blocs de Bitcoin serait parfaite pour cela. Il me semble que la pile de blocs de Bitcoin serait parfaite pour cela.

En effet, Bitcoin est un serveur de timestamp sécurisé et distribué pour transactions. Quelques lignes de code pourraient créer une transaction avec un hash supplémentaire de tout ce qui doit être horodaté. Je devrais ajouter une commande pour horodater un fichier de cette manière.

Plus tard, je veux ajouter des interfaces pour rendre l'intégration vraiment facile. dans des sites web à partir de n'importe quel langage côté serveur.
D'accord, et j'aimerais voir plus d'une interface de bibliothèque qui pourrait être D'accord, et j'aimerais voir plus d'une interface de bibliothèque qui pourrait être appelé depuis des langages de programmation ou de script, côté client aussi aussi.

Exactement.

Satoshi Nakamoto

#10

From: **Satoshi Nakamoto**
Subject: **Re: [bitcoin-list] Does Bitcoin Crash in Windows?**
October 23, 2009 at 23:57:51 UTC

> **Liberty Standard :**
> Est-ce que vous, utilisateurs de Windows, rencontrez des plantages occasionnels de Bitcoin ?
> Les utilisateurs de Windows rencontrent-ils des plantages occasionnels de Bitcoin ? Dernièrement, Bitcoin fonctionnant sous wine-1.0.1 plante fréquemment. Je me demandais simplement si c'est un problème lié à Wine ou à Bitcoin.

Satoshi Nakamoto :
Je n'ai eu aucun rapport de crashs dans la version 0.1.5. Elle a été d'une solidité à toute épreuve. pour moi sur Windows. Je pense que cela doit être lié à Wine. Si tu as un autre plantage dans Wine et qu'il imprime quoi que ce soit sur le terminal, envoyez-moi un e-mail et je peut-être que je pourrai comprendre ce qui s'est passé, peut-être quelque chose que je peux contourner autour. Martti et moi avons travaillé sur une nouvelle version à sortir bientôt. et ce serait bien d'y inclure toutes les corrections de Wine.

Les quatre lignes suivantes s'affichent dans le terminal lorsque je démarre Bitcoin.
fixme:toolhelp:CreateToolhelp32Snapshot Non implémenté : instantané de la liste de tas
fixme:toolhelp:Heap32ListFirst : stub
fixme:toolhelp:CreateToolhelp32Snapshot Non implémenté : instantané de la liste des tas
fixme:toolhelp:Heap32ListFirst : stub

Cela ne semble pas être quelque chose d'inquiétant. Ce sont probablement des fonctions non implémentées par Wine qui sont remplacées sans conséquences par des stubs.

Je ne lançais pas Bitcoin depuis le terminal auparavant, donc je ne sais pas ce que s'affiche lorsqu'il plante, mais je répondrai avec les résultats la prochaine fois qu'il plante. Pendant que Bitcoin télécharge d'abord les blocs déjà complétés, le fichier debug. continue de croître jusqu'à atteindre 17,4 Mo puis cesse de croître. J'imagine qu'il continuera à croître à mesure que plus de bitcoins seront complétés.

Vous pouvez supprimer debug.log de temps en temps si vous ne voulez pas prendre de l'espace disque. espace. Ce ne sont que des messages d'état qui aident au débogage.

bitcoin.sourceforge.net a l'air bien maintenant. Peut-être que SourceForge était en train de faire un peu de maintenance.

Satoshi

#11

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin 0.2 released**
December 17, 2009 at 06:52:09 UTC

Satoshi Nakamoto
Bitcoin 0.2 est là !

Télécharger (Windows, et maintenant une version Linux disponible)
http://sourceforge.net/projects/bitcoin/files/

Nouvelles fonctionnalités

Martti Malmi
- Option de minimiser dans la zone de notification
- Option de démarrage automatique au boot pour que vous puissiez le garder en cours d'exécution en arrière-plan automatiquement
en arrière-plan automatiquement
- Nouvelle disposition de la boîte de dialogue des options pour une future expansion
- Programme d'installation pour Windows
- Version Linux (testée sur Ubuntu)
Satoshi Nakamoto
- Prise en charge multi-processeur pour la génération de pièces
- Support de proxy pour une utilisation avec TOR
- Corrigé quelques ralentissements dans le téléchargement initial du bloc

Nous avons également un nouveau forum à l'adresse http://www.bitcoin.org/smf/

Un grand merci à Martti (sirius-m) pour tout son travail de développement, et à
New Liberty Standard pour son aide avec les tests de la version Linux.

Satoshi Nakamoto

#12

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin 0.3 released!**
July 6, 2010 at 21:53:53 UTC

Satoshi Nakamoto
Annonce de la version 0.3 de Bitcoin, la cryptomonnaie P2P ! Bitcoin est une monnaie numérique utilisant la cryptographie et un réseau distribué pour remplacer le besoin d'un serveur central de confiance. Évitez le risque d'inflation arbitraire des monnaies gérées de façon centralisé ! La circulation totale de Bitcoin est limité à 21 millions de pièces. Les pièces sont progressivement libérées aux nœuds du réseau en fonction de la puissance CPU qu'ils contribuent, vous pouvez donc obtenir une part de ceux-ci en contribuant votre temps CPU inactif.

Quoi de neuf :
- Ligne de commande et contrôle RPC JSON
- Inclut une version daemon sans interface graphique
- Onglets de filtre de transaction
- Hachage 20% plus rapide
- Affichage des performances de Hashmeter
- Version Mac OS X (merci à Laszlo)
- Traductions en allemand, néerlandais et italien (merci à DataWraith, Xunie et Joozero)

Procurez-vous-le sur http://www.bitcoin.org, et lisez le forum pour en savoir plus.

#13

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Alert: upgrade to bitcoin 0.3.6**
July 30, 2010 at 06:02:38 UTC

Satoshi Nakamoto
Veuillez mettre à jour vers la version 0.3.6 dès que possible pour beneficier d’un correctif important.

Consultez la page d'accueil de bitcoin.org pour les liens de téléchargement.

#14

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] ALERT - we are investigating a problem**
August 15, 2010 at 20:38:33 UTC

Satoshi Nakamoto
*** AVERTISSEMENT *** Nous enquêtons sur un problème. NE FAITES CONFIANCE AUCUNES TRANSACTIONS QUI ONT EU LIEU APRÈS LE 15.08.2010 À 17:05 UTC (bloc 74638)
jusqu'à ce que le problème soit résolu.

#15

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin 0.3.18 is released**
December 8, 2010 at 23:11:55 UTC

Satoshi Nakamoto
La version 0.3.18 est maintenant disponible.

Changements :
- Résolution d'un problème de compatibilité avec wallet.dat si vous êtes revenu à la version 0.3.17, puis à nouveau mis à niveau
- Vérification IsStandard() pour n'inclure que les types de transactions connus dans les blocs
- Optimisation de Jgarzik pour accélérer un peu le téléchargement du bloc initial

La principale nouveauté de cette version est l'ajout de commande JSON-RPC basé sur les comptes, sur lesquelles Gavin a travaillé (plus de détails à http://www.bitcoin.org/smf/index.php?topic=1886.0).
- getaccountaddress
- sendfrom
- move
- getbalance
- listtransactions

Télécharger :
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.18/

#16

From: **Satoshi Nakamoto**
Subject: **[bitcoin-list] Bitcoin 0.3.19 is released**
December 13, 2010 at 16:12:09 UTC

Satoshi Nakamoto
Ceci est une mise à jour mineure visant à ajouter une protection contre les attaques par déni de service (DoS).

Changements :
- Ajout de quelques limites de DoS, bien que ce soit encore loin d'être totalement résistant aux DoS.
- Suppression des alertes "mode sécurisé".

http://www.bitcoin.org/smf/index.php?topic=2228.0

Télécharger :
http://sourceforge.net/projects/bitcoin/files/Bitcoin/bitcoin-0.3.19/