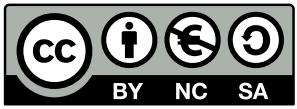
L'Élégance de Bitcoin (chapitre 1)

Ludovic Lars

3 janvier 2024



Chapitre 1

Les débuts de Bitcoin

Le 31 octobre 2008, un individu se faisant appeler Satoshi Nakamoto partageait sur Internet un court document qui décrivait le fonctionnement technique d'un système novateur de monnaie numérique : Bitcoin. Ce livre blanc de 9 pages, présenté comme un article scientifique, s'intitulait en anglais *Bitcoin: A Peer-to-Peer Electronic Cash System – Bitcoin : un système d'argent liquide électronique pair à pair*. Dans celui-ci, Satoshi proposait une solution au problème des paiements en ligne, par la mise en œuvre d'un serveur d'horodatage distribué basé sur un algorithme de preuve de travail.

Mais cela allait beaucoup plus loin. Le livre blanc de Bitcoin posait les bases d'une révolution conceptuelle profonde : une monnaie exclusivement numérique qui ne reposait sur aucun tiers de confiance, ni pour la confirmation des transactions, ni pour l'émission des nouvelles unités. Ce que Satoshi venait de découvrir, c'était bien plus qu'un système de paiement ; c'était un nouveau type de monnaie, quelque chose que nul n'avait su concevoir jusqu'alors, un phénomène économique et social qui rencontrerait un succès inouï au cours des années qui suivraient.

En particulier, la création de Satoshi Nakamoto réalisait le vieux rêve d'une monnaie numérique échappant au contrôle de l'État : un

rêve cher aux cypherpunks dont le mouvement, remontant au début des années 1990, prônait l'utilisation proactive de la cryptographie dans le but d'assurer la confidentialité et la liberté des individus sur Internet. Ces cryptographes rebelles avaient en effet désiré et tenté de concevoir un tel argent liquide électronique pendant des années, celui-ci étant un élément constitutif de leur idéal. Malheureusement, cela n'avait pas abouti, du moins jusqu'à l'apparition de Bitcoin.

À partir de cette date fatidique, Bitcoin a été mis en œuvre et a connu un certain nombre d'évènements fondateurs qui l'ont mené où il est aujourd'hui. Ces évènements ont façonné la compréhension que nous en avons, et l'histoire des débuts de Bitcoin constitue donc un récit unique qu'il convient de raconter.

Une naissance difficile

Bitcoin a été conçu par un individu qui utilisait le pseudonyme de Satoshi Nakamoto et prétendait être un homme japonais de 33 ans [1]. On sait peu de choses sur lui en dehors de ses messages publics et du code informatique qu'il a publié. Satoshi a disparu en 2011, et on ignore s'il est toujours vivant.

D'après son propre témoignage, Satoshi Nakamoto se met à travailler sur Bitcoin au printemps 2007. Pendant plus d'un an, il garde son modèle secret, souhaitant être sûr qu'il fonctionne correctement avant de le présenter au monde. Il affirmera ainsi avoir codé le prototype avant d'écrire le papier [2].

En août 2008, Satoshi a terminé de rédiger le livre blanc et commence à préparer l'annonce de la sortie de Bitcoin. Le 18 août, il réserve le nom de domaine Bitcoin.org via le service anonyme AnonymousSpeech [3]. Le nom de domaine sera utilisé pour héberger le site principal de Bitcoin.

Quelques jours plus tard, il rentre en contact avec Adam Back, le cryptographe et cypherpunk britannique à l'origine de Hashcash, la technique utilisée dans Bitcoin pour calculer la preuve de travail. Adam

Back le renvoie vers le cryptographe Wei Dai, inventeur en 1998 du concept de b-money, un concept qui possède des similarités notables avec Bitcoin. Le 22 août, Satoshi envoie donc un courriel à Wei Dai pour lui dire qu'il « se prépare à publier un document qui étend [ses] idées à un système complètement fonctionnel » et pour lui demander « l'année de publication de [sa] page sur la b-money » afin d'y faire référence dans le livre blanc [4]. Cependant, malgré ces interactions, Adam Back et Wei Dai ne s'intéressent pas à Bitcoin immédiatement. Ce ne sera que des années plus tard qu'ils reviendront vers la découverte révolutionnaire de ce mystérieux personnage.

À l'automne 2008, Satoshi décide de rendre public son système. Le 5 octobre, il s'inscrit sur la plateforme de gestion de projets SourceForge, là où le code source ouvert de Bitcoin sera hébergé et maintenu jusqu'en 2011. Le 31 octobre, il publie le livre blanc sur une liste de diffusion de courrier électronique dédiée à la cryptographie. Cette liste est la *Metzdowd Cryptography Mailing List* gérée par Perry Metzger sur son site web Metzdowd.com où participent un certain nombre d'anciens cypherpunks [5]. Dans son courriel d'introduction, il écrit :

> « J'ai travaillé sur un nouveau système d'argent liquide électronique qui est entièrement pair à pair, dépourvu de tiers de confiance. [6] »

Le livre blanc est centré sur le problème des paiements en ligne et le but de Bitcoin est clairement énoncé dès le début :

> « Le commerce sur Internet repose aujourd'hui presque exclusivement sur des institutions financières qui servent de tiers de confiance pour traiter les paiements électroniques. Bien que ce système fonctionne assez bien pour la plupart des transactions, il souffre toujours des faiblesses inhérentes à son modèle basé sur la confiance. [...] Ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur des preuves cryptographiques plutôt que sur la confiance, qui permettrait à deux parties volontaires de réaliser directement des transactions entre elles sans avoir recours à un tiers de confiance. [7] »

D'un point de vue technique, il s'agit de mettre en place un registre de transactions distribué sur un réseau pair à pair et ouvert d'ordinateurs. Ce registre est composé de blocs de transactions qui sont liés les uns à la suite des autres au cours du temps, formant une « chaîne de blocs ». Bitcoin constitue ainsi un « serveur d'horodatage distribué », qui répertorie l'ordre des transactions de façon à créer un historique cohérent, sans « double dépense ». Cela permet de gérer l'émission et les échanges d'une unité de compte numérique, qui sera appelée le bitcoin.

La fiabilité du système repose sur des « preuves de travail » qui lient les blocs entre eux de façon à rendre difficile la modification de la chaîne. Ces preuves sont produites périodiquement par des membres du réseau qui fournissent de l'énergie pour cela et qui sont rémunérés par une « incitation » en bitcoins composée des pièces nouvellement créées et des frais de transaction. Les personnes qui dépensent ainsi leur énergie électrique sont comparées par Satoshi aux « mineurs d'or qui dépensent des ressources pour ajouter de l'or dans la circulation », d'où le nom de mineurs qu'ils prendront plus tard.

Suite à l'annonce de Bitcoin et la publication du livre blanc, Satoshi reçoit peu de réponses, et beaucoup d'entre elles sont sceptiques. D'abord, le cypherpunk James A. Donald remet en cause le passage à l'échelle du système en disant qu'« il ne semble pas pouvoir s'adapter à la taille requise [8] ». Ensuite, John Levine critique sa sécurité en évoquant la puissance de calcul détenue par les « fermes de machines zombies [9] » composées d'ordinateurs contrôlés par des pirates. Enfin, un troisième individu du nom de Ray Dillinger s'interroge sur la valeur de l'unité de compte, déplorant le fait que « les preuves de travail informatiques n'ont pas de valeur intrinsèque [10] ».

Cependant, cet accueil sceptique n'est pas partagé par l'intégralité des personnes inscrites sur la liste de diffusion. En particulier, Hal Finney, un informaticien et cryptographe américain d'une cinquantaine d'années, est résolument enthousiaste et écrit dans son message du 7 novembre que « Bitcoin semble être une idée très prometteuse [11] ». Hal Finney n'est pas une personne comme les autres : il s'agit d'un

membre historique du mouvement cypherpunk qui a participé au développement du logiciel de chiffrement PGP dans les années 90 aux côtés de Philip Zimmermann, qui a expérimenté avec les premiers systèmes de monnaie électronique et qui a même tenté de créer son propre système de preuves de travail réutilisables. Malgré son expérience, il reste optimiste et devient ainsi le tout premier soutien de Satoshi dans son projet. Quelques années plus tard, il déclarera à ce sujet que « les cryptographes grisonnants [...] ont tendance à devenir cyniques » mais que lui « était plus idéaliste » ayant « toujours aimé la cryptographie, son mystère et son paradoxe [12] ».

Par la suite, Satoshi distribue les principaux fichiers du code aux personnes intéressées, dont notamment Hal Finney, Ray Dillinger et James A. Donald [13]. Hal et Ray réalisent alors un examen minutieux du code, en se concentrant chacun sur une partie spécifique du système. Ce code inclut déjà tous les éléments constitutifs de Bitcoin. Le prototype est alors prêt à être lancé.

Une enfance timide

Deux mois après la publication du livre blanc, le 8 janvier 2009 à 19 heures 27, Satoshi Nakamoto partage la première version du logiciel sur la liste de diffusion de Metzdowd. Le code source en C++ est publié de manière ouverte sous licence libre (MIT), de sorte que n'importe qui peut copier, modifier et utiliser le logiciel à sa guise. Celui-ci contient les données du bloc de genèse, le premier bloc de la chaîne à partir duquel celle-ci doit se prolonger.

Quelques heures plus tard, Satoshi commence à miner. Le deuxième bloc de la chaîne, le bloc 1, est validé par Satoshi le 9 janvier à 2 heures 54 du matin, ce qui marque le lancement effectif du réseau.

Le 10 janvier, Hal tente de faire fonctionner le logiciel. Après avoir échangé avec Satoshi pour faire en sorte que le logiciel fonctionne, il se met à miner et trouve son premier bloc (le bloc 78) à 1 heure du matin (UTC), gagnant de ce fait 50 bitcoins. Deux heures et demie plus tard,

il partage son expérience sur Twitter (média social alors naissant) en écrivant « *Running bitcoin* [14] ». Le lendemain, dans la nuit du 11 au 12 janvier, Satoshi envoie 10 bitcoins à Hal par l'intermédiaire de son adresse IP : il s'agit du premier transfert d'une personne à une autre sur le réseau [15].

Hal n'est pas la seule personne à expérimenter sur le réseau à ce moment-là : c'est également le cas de Dustin Trammell, un chercheur en sécurité informatique américain ayant découvert Bitcoin par la liste de diffusion. Celui-ci communique aussi avec Satoshi par courriel, et reçoit 25 bitcoins de sa part le 15 janvier [16].

Mais les quelques personnes qui font fonctionner le logiciel ne suffisent pas. Dès le début, Satoshi sait bien que peu de gens se sont penchés sérieusement sur son modèle et qu'il va être compliqué d'attirer de nouveaux utilisateurs et contributeurs. C'est pourquoi il essaie de susciter l'enthousiasme en vendant son idée du mieux possible.

Le premier élément est le programme d'émission du bitcoin, qui a pour limite 21 millions d'unités. Dans le courriel d'annonce du prototype, Satoshi explicite le rythme de création monétaire :

> « La circulation totale sera de 21 000 000 de pièces. Elles seront distribuées aux nœuds du réseau lorsqu'ils créeront des blocs, la quantité émise étant divisée par deux tous les 4 ans. [...] Lorsque cela sera épuisé, le système pourra prendre en charge les frais de transaction si nécessaire. [17] »

Le bitcoin a donc vocation à devenir une monnaie à offre fixe, déflationniste par nature, et cette particularité crée un enthousiasme. Le 11 janvier, Hal Finney est le premier à réagir en s'enthousiasmant du fait que « le système peut être configuré pour n'autoriser qu'un nombre maximum certain de pièces à être générées ». Il estime alors que si « Bitcoin [réussit] et [devient] le système de paiement dominant utilisé dans le monde entier », chaque pièce aura alors « une valeur d'environ 10 millions » de dollars [18]. L'estimation est contestable mais le raisonnement reste pertinent en raison du fonctionnement de Bitcoin.

Le 16 janvier, Satoshi reprend ainsi cet élément de communication dans un courriel qu'il partage à la liste de diffusion, où il déclare qu'il « pourrait être judicieux d'en avoir au cas où cela prendrait » et que « si suffisamment de gens pensent la même chose, cela deviendra une prophétie autoréalisatrice [19] ». Cet élément est crucial, comme le montre le témoignage de Dustin Trammell qui confie à Satoshi que le raisonnement de Hal est « l'une des autres raisons pour lesquelles [il a] démarré un nœud si rapidement ».

Outre le programme d'émission du bitcoin, Satoshi choisit de communiquer sur les défaillances du système bancaire, ce qui constitue le deuxième élément dans sa stratégie pour attirer l'attention.

En réalité, il le fait dès le bloc de genèse en y incluant le titre de la une du quotidien britannique *The Times* du 3 janvier 2009 annonçant que le ministre des finances britannique est sur le point de renflouer les banques pour la deuxième fois :

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

Cette phrase présente dans le premier bloc de la chaîne possède un rôle double : d'une part, elle empêche l'antidatage en prouvant que le système n'a pas été lancé avant le 3 janvier (Satoshi ne pouvait pas connaître cette une avant) ; d'autre part, elle indique symboliquement ce à quoi Bitcoin s'oppose en faisant référence au contexte monétaire et financier de l'époque.

En janvier 2009, le monde subit en effet de plein fouet les effets de la crise financière amorcée en 2007 par le dégonflement de la bulle immobilière aux États-Unis aussi connu sous le nom de la crise des subprimes. Les États renflouent les banques pour éviter de nouvelles faillites bancaires après celle de Lehman Brothers survenue le 15 septembre 2008, et les banques centrales procèdent à des assouplissements quantitatifs en injectant des liquidités sur les marchés financiers. Cette utilisation d'argent public, qui est littéralement créé pour l'occasion, choque profondément un certain nombre de citoyens qui réalisent que le système bancaire est en fait un système de profits privés et de pertes

socialisées.

De par son absence de tiers de confiance, Bitcoin n'est, lui, pas soumis à l'arbitraire d'une banque centrale. Il contraste ainsi avec les monnaies étatiques, telles que le dollar ou l'euro, dont la quantité peut être modifiée arbitrairement par ceux qui contrôlent la création monétaire, au moyen de ce qu'on appelle une politique monétaire. La politique monétaire du bitcoin est programmée, inscrite en dur dans le protocole, pour en théorie ne plus jamais être altérée.

C'est ce que met en avant Satoshi lorsqu'il intervient sur le forum de la Fondation P2P, une organisation étudiant l'impact des infrastructures pair à pair sur la société, le 11 février 2009. Dans son message d'introduction à Bitcoin, il écrit :

> « Le problème fondamental de la monnaie conventionnelle est toute la confiance nécessaire pour la faire fonctionner. Il faut faire confiance à la banque centrale pour qu'elle ne déprécie pas la monnaie, mais l'histoire des monnaies fiat est pleine de violations de cette confiance. Il faut faire confiance aux banques pour détenir notre argent et le transférer par voie électronique, mais elles le prêtent par vagues de bulles de crédit avec à peine une fraction en réserve. [20] »

Sur son profil où il indique sur son profil être un homme de 33 ans habitant au Japon, il donne une date de naissance particulière : le 5 avril 1975. Cette date, probablement fictive et composite, fait vraisemblablement référence à l'interdiction pour les particuliers de détenir de l'or aux États-Unis. Le jour du 5 avril se rapporte au jour de l'instauration de cette interdiction par l'Ordre exécutif 6102 signé par Franklin Delano Roosevelt le 5 avril 1933, et l'année 1975 correspond à son année d'abrogation lors de l'entrée en vigueur de la *Public Law* 93-373. Ce détail n'est pas anodin, puisque cette prohibition a permis en fin de compte d'instaurer un régime monétaire flottant n'ayant plus aucun lien avec l'or.

Ce n'est pas la seule référence aux métaux précieux. Satoshi écrit dans les commentaires le 18 février :

> « Il n'y a personne pour agir en tant que banque centrale ou réserve fédérale afin d'ajuster l'offre monétaire au fur et à mesure que le nombre d'utilisateurs augmente. [...] En ce sens, il se comporte davantage comme un métal précieux. Plutôt que de faire varier l'offre pour que la valeur reste la même, on détermine l'offre à l'avance et la valeur change. Plus le nombre d'utilisateurs augmente, plus la valeur d'une pièce augmente. Cela peut créer une boucle de rétroaction positive ; plus le nombre d'utilisateurs grandit, plus la valeur augmente, ce qui peut attirer davantage d'utilisateurs désireux de profiter de cet accroissement de la valeur. [21] »

Cette méthode de communication porte peu à peu ses fruits. Ainsi, même si certaines personnes finissent de se détourner de Bitcoin à l'instar de Hal Finney, Satoshi continue de recevoir des messages de la part de personnes intéressées. Le 11 avril 2009, Mike Hearn, un développeur britannique travaillant pour Google et s'adonnant au logiciel libre sur son temps libre, lui envoie un courriel posant une série de questions à propos de Bitcoin, en précisant qu'« il est rare de rencontrer des idées vraiment révolutionnaires [22] ». Hearn s'intéresse alors aux monnaies numériques, et notamment à Ripple.

Début mai 2009, c'est un jeune étudiant en informatique finlandais qui contacte Satoshi : il s'agit de Martti Malmi. Celui-ci a découvert Bitcoin début avril, s'est mis à miner et a même rédigé une courte description de Bitcoin sur le forum de Freedomain Radio où il soutenait l'hypothèse anarchiste que la monnaie pair à pair pourrait faire disparaître l'État [23]. Dans son courriel à Satoshi, il écrit :

> « J'ai une bonne connaissance des langages Java et C grâce aux cours que j'ai suivis à l'école (j'étudie l'informatique) mais je n'ai pas encore beaucoup d'expérience en matière de développement. J'aimerais aider avec Bitcoin, s'il y a quelque chose que je peux faire. [24] »

Malgré son manque d'expérience, Martti devient dans les mois qui suivent le principal contributeur à Bitcoin en dehors de Satoshi. Étant étudiant, il a en effet beaucoup de temps à consacrer au projet.

En particulier, Satoshi lui confie la charge du site web. Dès le mois de mai, Martti Malmi rédige une première version de la description sur SourceForge où il présente Bitcoin comme une « monnaie numérique anonyme basée sur un réseau pair à pair » permettant de « transférer de l'argent facilement par Internet, sans avoir à faire confiance à des tiers » et d'être « à l'abri de l'instabilité causée par le système de réserves fractionnaires et par les mauvaises politiques des banques centrales [25] ». Cette ébauche servira de base pour la présentation de Bitcoin sur le site web.

À l'époque le bitcoin n'a pas de prix. Les gens qui testent le système se contentent de lancer le logiciel pour « générer des pièces ». Les transactions sont peu nombreuses, et consistent le plus souvent en des auto-transferts. Les bitcoins sont alors vus comme des collectionnables réservés aux passionnés d'informatique. Les utilisateurs ont l'impression de contribuer à quelque chose, à l'instar des projets de calcul distribué (dits « @home ») où les gens mettent à disposition leurs ressources informatiques au service de bonnes causes.

Certains individus minent en continu. C'est le cas de Hal Finney qui fait fonctionner le logiciel entre janvier et mars, de James Howells qui valide des blocs entre février et avril, de Dustin Trammell qui fait tourner ses serveurs pendant plus d'un an, ou de Martti Malmi qui met son ordinateur portable à profit à partir d'avril. Mais le principal mineur de l'année de 2009 reste Satoshi, qui déploie une puissance de calcul bien plus grande et dont la production de blocs représente près de la moitié de celle du réseau.

En 2009, la difficulté de minage est de 1, ce qui impose à tous les nœuds du réseau de réaliser environ 4,3 millions de calculs pour miner un bloc, et ce n'est pas rien pour un processeur. De ce fait, la production est plus lente que prévue : entre le 3 janvier 2009 et le 3 janvier 2010, seulement 32 880 blocs sont trouvés sur les 52560 attendus, ce qui correspond à une durée moyenne entre chaque bloc de 16 minutes au lieu des 10 minutes prévues. En particulier, le mois d'août 2009 constitue le pire mois pour l'activité minière : seuls 1 564 sur 4 464 blocs attendus sont trouvés, soit un temps moyen de 28 minutes et 30

secondes !

Des premiers pas incertains

Malgré son lancement timide, Bitcoin survit à l'été et franchit une étape cruciale en octobre : son unité de compte acquiert un prix. Un individu utilisant le pseudonyme NewLibertyStandard (NLS), nouvellement arrivé dans la communauté, met en place sur sa page personnelle un service de change permettant aux gens de convertir leurs dollars en bitcoins et inversement. Pour estimer le taux de change, il se base sur le coût énergétique nécessaire pour obtenir un bitcoin, en prenant en compte le coût de l'électricité à son emplacement et la fréquence de sa production personnelle. Les prix sont publiés quotidiennement sur son site.

Le 12 octobre 2009, a ainsi lieu la première vente de bitcoins en dollars entre Martti Malmi et NewLibertyStandard : Martti cède 5050 bitcoins à NLS pour 5,02 $ virés sur son compte PayPal, ce qui correspond à un prix d'environ 0,001 $ par bitcoin [26]. NLS effectuera par la suite d'autres échanges au cours des mois suivants, constituant la seule passerelle entre le dollar et le bitcoin.

Le 22 novembre marque l'ouverture du nouveau forum, sobrement appelé le *Bitcoin Forum*, qui est hébergé sur Bitcoin.org et géré par Martti Malmi. Ce forum abrite l'essentiel des discussions sur Bitcoin à partir de cette date. Il sera renommé en Bitcointalk en août 2011 et hébergé à une nouvelle adresse.

Le 16 décembre 2009, Satoshi annonce la sortie de la version 0.2 du logiciel, version pour laquelle Martti Malmi est grandement crédité, ce qui clôt la première période de développement informatique de Bitcoin. L'année se termine en beauté lorsque la difficulté augmente enfin, en passant de 1 à 1,18 le 30 décembre.

Au début de l'année 2010, le bitcoin est désigné comme une « cryptomonnaie » (*cryptocurrency*) sur le site web. Le préfixe crypto- (qui vient du grec ancien κρυπτος, kruptós, indiquant ce qui est caché, oc-

culté) possède une signification double : il renvoie à la cryptographie sur laquelle Bitcoin s'appuie, et à la confidentialité, Bitcoin étant alors présenté comme une « monnaie numérique anonyme ».

Ce nouveau terme confirme le but central de Bitcoin : devenir une monnaie, c'est-à-dire un intermédiaire dans les échanges. Cela nécessite des personnes qui génèrent des transactions (par le biais du commerce) et d'autres qui traitent ces transactions (par le biais du minage). C'est donc tout naturellement que l'expansion de ces deux aspects complémentaires se produit à ce moment-là.

Le premier développement est l'essor commercial dont NewLibertyStandard peut être considéré comme le pionnier. Non seulement il est le premier commerçant à accepter le bitcoin comme moyen de paiement par l'intermédiaire de son service d'échange, mais il est aussi l'un des promoteurs originels de cet effort de construction économique. Dans son premier message sur le forum le 19 janvier 2010, il écrit ainsi :

> « Des gens m'ont acheté des bitcoins et m'en ont vendus. L'offre et la demande, même si elle sont faibles, existent déjà et c'est tout ce qu'il faut. Proposer d'échanger des bitcoins contre une autre monnaie n'est en fin de compte pas différent de l'échange de bitcoins contre des biens ou des services. Les monnaies sont des biens et le change est un service. [...] Vous pouvez acheter tous mes dollars ou bitcoins aujourd'hui, mais il y en aura toujours plus demain et après-demain. Toutes les personnes qui achètent ou vendent des biens en utilisant des bitcoins, y compris les changeurs, font progresser l'économie de Bitcoin. Que tout le monde fasse sa part. Achetez ou vendez quelque chose en échange de bitcoins ! [27] »

Dans les mois qui suivent, les services de change se développent, comme BitcoinFX ou Bitcoin Market. C'est pourquoi NLS propose que le bitcoin, à l'instar des monnaies échangées sur le marché des changes, adopte le sigle boursier BTC et le symbole du baht thaïlandais. L'utilisation du sigle BTC se normalise rapidement. Quant au symbole (le B majuscule traversé par deux barres verticales rappelant immanquablement le dollar), c'est Satoshi lui-même qui le conçoit, en s'inspirant de

la proposition de NLS, lors de la création du premier véritable logo de Bitcoin [28].

FIGURE 1.1 – Logo de Bitcoin conçu par Satoshi Nakamoto en février 2010.

Les vendeurs de biens et de services apparaissent également. Outre son service de change, NLS ouvre un magasin en ligne où il propose à la vente des timbres et des autocollants. D'autres services acceptant le bitcoin apparaissent comme le service de voix sur IP Link2VoIP, l'hébergeur web Vekja.net et le vendeur de noms de domaines Privacy Shark. En parallèle, la première partie de poker mettant en jeu des bitcoins est organisée, ce qui inaugure la relation forte qui existera entre le jeu d'argent et la cryptomonnaie.

Enfin, en avril 2010, naît MyBitcoin, une application web dépositaire permettant un usage facile et serein de Bitcoin, notamment sur mobile. Grâce à celle-ci, les utilisateurs n'ont en effet pas besoin de télécharger les données complètes pour envoyer et recevoir des transactions, ni de conserver leurs bitcoins eux-mêmes en sauvegardant leurs clés privées. À cette époque, les portefeuilles légers n'existent pas, si bien que Satoshi lui-même juge qu'il est alors acceptable de passer par ce type d'application, même si cela va à l'encontre du principe de désintermédiation à la base de Bitcoin :

> « Le seul inconvénient c'est qu'il faut faire confiance au site, mais cela ne pose pas de problème pour la petite monnaie, pour les micropaiements et les dépenses diverses. [29] »

L'année 2010 est également celle de l'essor du minage, qui se manifeste en premier lieu par l'émergence du minage par processeur

graphique (GPU). Jusqu'alors, les mineurs sollicitaient leur processeur central (CPU) pour extraire de nouveaux bitcoins. Néanmoins, ces derniers processeurs s'avèrent peu performants pour effectuer des opérations répétées, comparés aux cartes graphiques qui sont largement plus adaptées à ce type de calcul répétitif. Par conséquent, tout le monde sait à ce moment-là que cette évolution est inéluctable, y compris Satoshi qui déclare en décembre 2009 que la communauté doit « se mettre d'accord pour reporter la course aux armements des GPU aussi longtemps que possible pour le bien du réseau [30] ».

La boîte de Pandore est ouverte par Laszlo Hanyecz, un développeur américain d'origine hongroise de 28 ans, qui découvre Bitcoin en avril. Après avoir acheté des bitcoins à NLS et essayé le système de transactions, celui-ci programme début mai un logiciel de minage qui s'adapte aux cartes graphiques. Cette optimisation lui permet d'occuper rapidement une place importante dans la production des blocs. Ceci attire l'attention de Satoshi Nakamoto qui le contacte et lui demande de ralentir ses opérations afin que le minage reste accessible à tous :

> « L'un des principaux attraits pour les nouveaux utilisateurs est que toute personne disposant d'un ordinateur peut générer des pièces gratuites. Lorsqu'il y aura 5 000 utilisateurs, cette incitation s'estompera peut-être, mais pour l'instant, c'est toujours vrai. Les GPU limiteraient prématurément cette incitation à ceux qui disposent d'un matériel GPU haut de gamme. Il est inévitable que les clusters de calcul GPU finiront par accaparer toutes les pièces générées, mais je ne veux pas précipiter l'arrivée de ce jour-là. [...] Je ne veux pas passer pour un socialiste, je me moque de la concentration des richesses, mais pour l'instant, nous obtenons plus de croissance en donnant cet argent à 100 % des gens qu'en le donnant à 20 %. [31] »

Laszlo abaisse sa cadence, mais continue à miner avec sa carte graphique. Avec sa méthode, il accumule ainsi des dizaines de milliers de bitcoins.

Toutefois, cela n'est pas entièrement négatif pour le projet car il finit par réinjecter ses bitcoins dans l'économie de la façon la plus emblémа-

tique possible : en achetant quelque chose avec, et plus précisément des pizzas. Le 18 mai 2010, il écrit ainsi l'annonce suivante sur le forum :

> « Je paierai 10 000 bitcoins pour deux ou trois pizzas... genre peut-être 2 grandes pour qu'il m'en reste le lendemain. J'aime avoir des restes de pizza à grignoter pour plus tard. Vous pouvez faire la pizza vous-même et l'amener jusqu'à chez moi ou la commander pour moi dans un service de livraison, mais mon objectif c'est de me faire livrer, en échange de bitcoins, de la nourriture que je n'ai pas à commander ou à préparer moi-même. [...] Si vous êtes intéressé, faites-le moi savoir et nous pourrons nous arranger. [32] »

Cette offre trouve preneur au bout de quatre jours. Le 22 mai, un jeune Californien du nom de Jeremy Sturdivant accepte l'échange sur la messagerie instantanée IRC : il commande deux pizzas de Papa John's qui sont livrées chez Laszlo à Jacksonville en Floride, et reçoit en échange 10 000 bitcoins [33], ce qui représente alors environ 44 $ sur Bitcoin Market. Cela clôt le premier achat d'un bien physique en bitcoins ! Cet évènement symbolique sera par la suite commémoré tous les ans à cette date comme le *Bitcoin Pizza Day*.

Une autre personne vient contribuer au succès du projet. Vers la fin du mois de mai, un développeur américain de 44 ans, nommé Gavin Andresen, découvre Bitcoin par le biais d'un article publié sur InfoWorld. De retour d'Australie, momentanément sans emploi, il se met à travailler sur son premier projet : un robinet à bitcoins (*bitcoin faucet*) qui donne des bitcoins à quiconque en fait la requête. Le 11 juin, Gavin lance son service et le présente sur le forum :

> « Pour mon premier projet de programmation sur Bitcoin, j'ai décidé de faire quelque chose qui semble vraiment stupide : j'ai créé un site web qui distribue des bitcoins. [...] Pourquoi ? Parce que je veux que le projet Bitcoin réussisse, et je pense qu'il a plus de chances de réussir si les gens peuvent obtenir une poignée de pièces pour l'essayer. [34] »

Ce *faucet*, qui offre d'abord 5 bitcoins par requête au tout début, est approuvé par Satoshi, ce dernier ayant « prévu de faire exactement

la même chose si quelqu'un d'autre ne l'avait pas fait [35] ». Le service, sollicité par beaucoup de personnes, distribuera plus de 19 700 bitcoins jusqu'à sa fermeture deux ans plus tard.

De plus, Gavin s'implique dans le développement du logiciel et échange beaucoup avec Satoshi par courriel. Il en devient rapidement le bras droit grâce à la confiance qu'il lui inspire.

Malgré cette croissance économique encourageante, l'activité reste extrêmement réduite sur le réseau. Le 30 juin, sur la liste de diffusion de Bitcoin, James A. Donald déclare ainsi que « Bitcoin est en quelque sorte mort » et que « le problème est que le bitcoin a besoin d'une écologie d'utilisateurs pour être utile [36] ». Toutefois, quelques jours plus tard, un évènement vient lui donner tort.

Le slashdotting

Le 11 juillet 2010, suite à la sortie de la version 0.3 du logiciel, une courte présentation de Bitcoin rédigée par un utilisateur est publiée sur Slashdot, un site d'actualité très populaire traitant de sujets pour les *nerds* comme l'informatique, les jeux vidéo, la science, Internet, etc. L'argumentaire de vente est le suivant :

> « Que pensez-vous de cette technologie disruptrice ? Bitcoin est une monnaie numérique basée sur un réseau pair à pair, sans banque centrale, et sans frais de transaction. À l'aide d'un concept de preuve de travail, les nœuds brûlent des cycles de processeur pour chercher des paquets de pièces et diffusent leurs résultats sur le réseau. L'analyse de la consommation d'énergie révèle que la valeur marchande des bitcoins est déjà supérieure à la valeur de l'énergie nécessaire pour les générer, ce qui indique une demande saine. La communauté a bon espoir que la monnaie restera hors de portée de tout État. [37] »

Ceci provoque un afflux massif de nouveaux visiteurs sur le site et sur le forum, ainsi qu'une augmentation du nombre d'utilisateurs et de mineurs sur le réseau. Le réseau tient le coup malgré la montée en

charge. En conséquence, le prix du bitcoin connaît la première hausse majeure de son histoire, en passant de 0,008 $ à 0,08 $ en une semaine, soit une multiplication par 10 !

Parmi les personnes qui découvrent Bitcoin grâce à Slashdot, il y a Jed McCaleb, un entrepreneur et programmeur américain de 35 ans, connu pour avoir cofondé et développé le logiciel de partage de fichiers en pair à pair eDonkey2000 dans les années 2000. Constatant à quel point il est pénible de se procurer du bitcoin contre des dollars, il décide de créer une place de marché spécialisée. Pour ce faire, il réutilise un de ses anciens projets mis au point en 2007 : *Magic The Gathering Online eXchange* (MTGOX), un site web qui permettait d'acheter et de vendre des cartes du jeu en ligne *Magic: The Gathering Online* [38]. Il reprend le même nom de domaine au passage : mtgox.com.

Une semaine plus tard, le 18, la plateforme de change Mt. Gox (« *Mount Gox* ») est lancée et annoncée officiellement sur le forum par Jed. Grâce à son expertise, il fait en sorte que la plateforme fonctionne comme une place de marché automatisée, à l'instar des bourses en ligne modernes. Elle se distingue de Bitcoin Market par le fait qu'elle est « toujours en ligne, automatisée », que « le site est plus rapide et a un hébergement dédié » et que « l'interface est plus agréable [39] ». Par conséquent, Mt. Gox s'impose rapidement comme le moyen principal de se procurer du bitcoin, devenant la référence en ce qui concerne le cotation en dollars.

Le minage connaît également une phase ascendante. L'afflux de nouveaux mineurs fait passer le taux de hachage du réseau (le nombre de calculs par seconde) au-dessus du milliard de calculs par seconde (1 GH/s) dès le 13 juillet. Certains mineurs développent leur propre algorithme de minage par GPU. C'est le cas de ArtForz, un développeur allemand, qui se met à miner le 19 juillet et qui construit au cours du temps la première ferme de minage de Bitcoin, qui sera connue sous le nom d'« ArtFarm » [40].

Mais cette croissance suivant la présentation sur Slashdot provoque également des problèmes d'ordre technique, mettant le système à l'épreuve. Deux incidents viennent ainsi perturber le projet.

Le premier incident est la découverte d'une vulnérabilité dans le code de Bitcoin qui rend possible la dépense de bitcoins à partir de n'importe quelle adresse (cette vulnérabilité sera appelée le « 1 RETURN bug » en référence au script nécessaire pour réaliser cette dépense). C'est ArtForz qui en découvre l'existence à la fin du mois de juillet 2010. Au lieu d'exploiter cette faille et de s'emparer de la richesse présente sur le réseau pour la revendre discrètement, il choisit de prévenir Satoshi et Gavin par courriel. Satoshi s'empresse d'inclure la correction dans la mise à jour 0.3.6 et recommande à tous les utilisateurs de mettre à jour leur logiciel. La vulnérabilité n'est pas exploitée et Bitcoin échappe ainsi au pire.

Le second évènement est le *value overflow incident*. Le 15 août vers 17 heures, un bloc miné contient une transaction qui crée plus de 184 milliards de bitcoins. Cette création exploite une vulnérabilité de dépassement de mémoire (*overflow*) dans la représentation des quantités dans Bitcoin. Une heure plus tard, le problème est repéré par Jeff Garzik, un ingénieur américain ayant découvert Bitcoin grâce à Slashdot, qui avertit la communauté sur le forum [41].

La réaction de Satoshi ne se fait pas attendre. Un peu avant minuit, il publie un correctif créant une chaîne alternative ne contenant pas la transaction incriminée. La situation conflictuelle est résolue lorsque la chaîne correcte devient plus longue que l'autre le lendemain à 8 heures 10 du matin. Cet incident perturbe l'activité du réseau pendant 15 heures environ mais le problème est vite résolu grâce à une réactivité forte de la communauté. Suite à cet incident, Satoshi implémente un système d'alerte dans Bitcoin, lui permettant d'avertir tous les nœuds du réseau en cas de problème technique [42].

Au cours de l'automne, la popularisation du minage par processeur graphique rend le minage par CPU quasi-impossible. C'est ce qui provoque l'apparition de la première coopérative de minage le 27 novembre, Bitcoin.cz Mining, une organisation permettant aux petits mineurs de lisser leurs revenus en regroupant leurs puissances de calcul respectives [43]. Créée par Marek Palatinus (connu sous le pseudonyme de slush), un architecte informatique tchèque, la coopérative sera par la

suite renommée en Slush Pool en son hommage.

De manière générale, à la fin de l'année 2010, on peut considérer que le projet Bitcoin a pris son envol : l'économie s'est fortifiée, notamment avec les services de change, le minage s'est spécialisé avec l'apparition du minage par GPU et le protocole a été mis à l'épreuve par la découverte de failles dans le logiciel. Ces éléments montrent que les incitations des différents acteurs du système sont alignées. C'est à ce moment-là que Satoshi décide de disparaître.

La disparition de Satoshi Nakamoto

La disparition de Satoshi Nakamoto se fait progressivement à partir de décembre 2010. Satoshi n'explicite pas les raisons qui le poussent à s'éclipser, mais nous pouvons les deviner. Tout d'abord, le projet a pris : il a grossi à tel point qu'il devient difficile de diriger le mouvement. Mais surtout Satoshi redoute la réaction des agences étatiques, une préoccupation qu'il exprime dans un message daté du 5 juillet 2010 (commentant le brouillon de la présentation de Bitcoin qui sera proposée à Slashdot), où il déclare ne pas vouloir mettre trop en avant l'aspect « anonyme » de Bitcoin ou son opposition aux autorités légales qui constituerait une « provocation [44] ».

L'élément déclencheur est l'affaire WikiLeaks. WikiLeaks est une organisation non gouvernementale à but non lucratif fondée par le cypherpunk Julian Assange en 2006, dont la raison d'être est de donner une audience aux lanceurs d'alertes et aux fuites d'information, tout en protégeant leurs sources. À partir de 2010, les documents confidentiels révélés de l'ONG commencent à être relayés par les grands médias et à faire du bruit dans l'opinion publique. C'est notamment le cas de l'*Afghan War Diary*, un ensemble de documents et de rapports militaires américains secrets sur la guerre en Afghanistan faisant notamment état de la dissimulation des victimes civiles, qui est publié le 25 juillet 2010 grâce à la contribution de Bradley Manning, un analyste militaire de l'armée des États-Unis [45]. On peut également citer les *Iraq War Logs*, documents secrets sur la guerre en Irak entre 2004 et 2009

publiés le 23 octobre et révélant le nombre de victimes civiles et les actes de torture perpétrés.

Le financement de WikiLeaks repose essentiellement sur les dons du public. Il s'agit d'une activité sensible pour les firmes réglementées qui craignent les potentielles représailles des autorités. C'est ainsi que la société de paiement en ligne Moneybookers gèle le compte de l'ONG le 14 octobre 2010. À la suite de ces révélations, il est ainsi de plus en plus probable que WikiLeaks s'expose à davantage de sanctions.

Le 10 novembre, Amir Taaki, un jeune anglais d'origine iranienne ayant fraîchement découvert Bitcoin, voit dans la situation de WikiLeaks une opportunité de démontrer l'utilité de la résistance à la censure du système. Il écrit ainsi sur le forum :

> « Je voulais envoyer une lettre à Wikileaks à propos de Bitcoin car, malheureusement, ils ont subi plusieurs incidents où leurs fonds ont été saisis dans le passé. Quelqu'un sait où leur envoyer un message ? [46] »

Les réactions sont mitigées. D'après un utilisateur, « cela peut être bénéfique pour wikileaks, mais pas nécessairement pour Bitcoin [47] ».

Un mois plus tard, le 3 décembre, PayPal gèle le compte de WikiLeaks. Certaines personnes sur le forum suggèrent d'encourager WikiLeaks à accepter le bitcoin : cela paraît en effet le « moment idéal pour commencer les dons en bitcoins [48] ». Cela fait réagir Satoshi le lendemain qui s'oppose à cette évolution et déclare :

> « Le projet a besoin de grandir progressivement pour que le logiciel puisse se renforcer en cours de route.
>
> J'appelle WikiLeaks à ne pas commencer à utiliser Bitcoin. Bitcoin est une petite communauté expérimentale encore naissante. Vous n'obtiendriez rien de plus que quelques piécettes et l'agitation que vous apporteriez nous détruirait probablement à ce stade. [49] »

Dans les jours qui suivent, c'est un véritable blocus financier qui se met en place contre WikiLeaks, auquel participent Mastercard et Visa,

mais aussi Western Union, Bank of America et d'autres acteurs, ce qui met en péril la survie financière de l'ONG. Tout naturellement certains insistent pour que Bitcoin soit mis à profit.

Le 11 décembre, un article est publié sur PC World pour mettre en avant la possibilité d'un usage de Bitcoin par WikiLeaks. Cet article est rapidement évoqué sur le forum et la réaction de Satoshi est sans appel. Il écrit :

> « Il aurait été bon d'attirer cette attention dans un tout autre contexte. WikiLeaks a donné un coup de pied dans la fourmilière, et la colonie se dirige maintenant vers nous. [50] »

C'est son avant-dernier message public. Le lendemain, il poste son dernier message sur le forum pour annoncer la version 0.3.19 du logiciel, puis se volatilise. Il transmet les rênes du projet à ses deux bras droits historiques : Martti Malmi et Gavin Andresen.

Martti Malmi hérite du site web et du forum. Néanmoins, à l'instar de Satoshi, il se détourne progressivement de Bitcoin et délègue la gestion de ces plateformes à d'autres personnes, à qui il cèdera le contrôle entièrement en 2015 [51]. Il vendra ses 55 000 bitcoins pour s'acheter un appartement près de Helsinki.

De son côté, Gavin Andresen hérite de la clé d'alerte, du dépôt SourceForge et de la liste de diffusion. Dès le 19 décembre, il annonce « commencer à gérer le projet Bitcoin de manière plus active [52] » et crée le dépôt GitHub de Bitcoin, où le projet sera dorénavant développé. Il ignore alors qu'il est devenu le développeur en chef du projet et que le créateur de Bitcoin va disparaître.

Satoshi se volatilise définitivement durant le printemps 2011. Le 23 avril, il adresse un dernier courriel à Mike Hearn, l'ingénieur de Google qui l'avait approché deux ans auparavant et qui était resté en contact avec lui, dans lequel il écrit :

> « Je suis passé à autre chose. [Bitcoin] est entre de bonnes mains avec Gavin et les autres. [53] »

Il fait également ses adieux à Gavin et Martti. En particulier, il demande à Gavin d'éviter de parler de lui comme d'une « personnalité sombre et mystérieuse » à la presse [54].

Le 27 avril, Gavin annonce qu'il a été invité par la CIA à faire une présentation sur Bitcoin. Cette visite se passe le 14 juin. De manière intéressante, c'est également le jour où WikiLeaks se met finalement à accepter les dons en bitcoin [55]. Ces deux évènements viennent confirmer ce que Satoshi redoutait.

Satoshi Nakamoto laisse derrière lui une fortune colossale : 1 122 693 bitcoins selon une estimation de 2020 [56]. Cela représente plus de 5 % de la quantité totale de bitcoins. Ces fonds ne bougeront jamais.

Quelques messages émaneront de ses différents comptes [57], mais on supposera qu'ils ont été piratés.

L'identité de Satoshi Nakamoto restera inconnue, celui-ci ayant réussi à conserver son anonymat grâce à l'usage de Tor et de services respectueux de la vie privée. Dans les années qui suivront, sa « personnalité sombre et mystérieuse » deviendra un mythe à part entière, suscitant les spéculations les plus diverses. Tout le monde se demandera « Qui est Satoshi Nakamoto ? » à l'instar des personnages de *La Grève* d'Ayn Rand s'interrogeant sur l'identité de John Galt. On cherchera à savoir qui il est, quelques pistes seront privilégiées [58], mais jamais son identité civile ne sera formellement identifiée.

En 2013, dans l'un de ses derniers messages sur le forum, Hal Finney partagera une citation énigmatique du film *Man of Steel* tout juste sorti, résumant bien la dimension mystérieuse entourant le créateur de Bitcoin :

> « Comment retrouver quelqu'un qui a toujours brouillé les pistes ? [...] Pour certains, c'était un ange gardien. Pour d'autres, [une énigme,] un fantôme, toujours un peu à l'écart. [...] Que représente le S ? [59] »

En mars 2014, on croira l'avoir trouvé en la personne de Dorian Prentice Satoshi Nakamoto suite à la publication d'un article de News-

week [60]. Cet ingénieur des télécommunications, citoyen américain naturalisé d'origine japonaise, vivant avec sa mère à Temple City dans la banlieue de Los Angeles, se fera harceler par la presse mais niera en bloc. On découvrira cependant que la famille de Hal Finney a habité dans la même municipalité, « à quelques pâtés de maisons de la maison familiale des Nakamoto », durant l'adolescence de Hal, ce qui attirera quelques soupçons sur ce dernier [61].

Hal Finney décèdera en août 2014 des suites de la maladie de Charcot. En tant que futuriste averti, il se fera cryogéniser par la fondation Alcor.

La communauté prend le relai

Alors que Satoshi se met progressivement en retrait, la popularité de Bitcoin augmente prodigieusement. En particulier, le prix du bitcoin évolue de manière favorable : alors qu'il n'était que de 20 centimes en décembre 2010, il atteint la parité avec le dollar le 9 février 2011 et s'y maintient pendant quelques temps. Cette hausse du prix attise l'enthousiasme de la communauté, et notamment celui de Hal Finney qui déclare avoir « vraiment de la chance d'être au début d'un nouveau phénomène potentiellement explosif [62] ».

Cette période coïncide avec l'apparition de Silk Road, une place de marché du dark web s'appuyant sur Tor et Bitcoin qui permet à ses utilisateurs d'échanger librement des produits et des services légaux et illégaux. Celle-ci est lancée à la fin du mois de janvier par un jeune Texan du nom de Ross Ulbricht, qui en fait mention sur le forum de Bitcoin en feignant d'avoir découvert le site par hasard [63].

Ross Ulbricht adhère profondément aux principes du libertarianisme, une philosophie libérale originaire des États-Unis prônant le respect impératif de la liberté individuelle, des droits de propriété et du marché. Silk Road est pour lui une incarnation de cet idéal. De ce fait, la gamme des produits et services qui peuvent être listés sur le site est restreinte et nécessite qu'aucun mal n'ait été fait à autrui : on y retrouve

ainsi de la drogue, des médicaments, des pièces de métaux précieux, mais en aucun cas des cartes bancaires volées, de la pédopornographie ou des services de tueur à gages. Dans l'ensemble, le site sert principalement à la vente de drogue illicite (dont surtout de petites quantités de cannabis), chose pour laquelle il deviendra célèbre.

La promotion de Bitcoin s'intensifie également. Le 22 mars, la première vidéo expliquant Bitcoin de manière qualitative est publiée [64]. Cette vidéo, intitulée sobrement « *What is Bitcoin?* », est produite par Stefan Thomas grâce à un financement participatif de la communauté. Elle aura un succès retentissant au fil des années en totalisant plusieurs millions de vues sur YouTube. Les vidéos de ce type se multiplieront.

Bitcoin est notamment vanté dans les cercles libertariens, où son caractère libre, anonyme et hors de portée de l'État est mis en avant. Le 16 mars 2011, une partie de l'épisode de FreeTalkLive du jour est consacrée à Bitcoin et à Silk Road. Cela attire l'attention de l'entrepreneur et activiste Roger Ver, déjà millionnaire grâce à sa société de revente de composants informatiques, Memory Dealers. Il découvre Bitcoin à la fin du mois d'avril en écoutant une rediffusion de l'épisode et est instantanément conquis : il se met à lire tout ce qu'il peut sur le sujet, achète du bitcoin et commence à l'accepter avec son entreprise. Il deviendra rapidement l'un des promoteurs les plus zélés de Bitcoin, ce qui lui vaudra le surnom de *Bitcoin Jesus* pendant un temps.

L'existence de Silk Road est révélée au grand public le 1er juin 2011 avec un article d'Adrien Chen sur Gawker [65], ce qui a pour effet d'attirer l'attention sur Bitcoin encore un peu plus, notamment en incitant les consommateurs à se procurer du bitcoin pour acheter des produits sur la plateforme.

Au cours du printemps 2011, on assiste par conséquent à une forte poussée du prix, due à l'augmentation de la demande. Après avoir stagné pendant quelques mois, celui-ci passe ainsi de 1 $ le 15 avril à plus de 32 $ le 8 juin.

Mt. Gox, la principale plateforme de change de l'époque, se retrouve sous pression. Celle-ci a alors été reprise depuis quelques mois par Mark Karpelès, un développeur français de 26 ans vivant au Ja-

pon, qui est quelque peu négligent et n'a pas su résoudre les problèmes d'implémentation de son prédécesseur. C'est ainsi qu'un incident malencontreux survient le dimanche 19 juin : un groupe de pirates accède au compte administrateur de Jed McCaleb et tente d'en extraite un maximum d'argent.

La limite de retrait journalière étant fixée à 1 000 $, les pirates cherchent à faire baisser le prix afin de retirer le plus de bitcoins possibles. Ils vendent les bitcoins de Jed McCaleb au marché ce qui provoque un krach éclair sur le cours : le prix, qui stationne ce jour-là autour des 17 $, chute à 0,01 $ en quelques minutes. C'est la panique dans la communauté, et beaucoup d'utilisateurs de Mt. Gox vendent sous le coup de l'émotion afin de conserver ce qui leur reste. La situation est rétablie dans la journée mais 2 000 bitcoins manquent à l'appel. Le 23 juin, Mark Karpelès prouve la solvabilité de l'entreprise en déplaçant 424 242 bitcoins d'une adresse à une autre [66].

Cet incident entraîne la fin de la folie spéculative sur le bitcoin et le prix se met à descendre doucement. C'est ce moment-là qu'on assiste à l'escroquerie de sortie de MyBitcoin : le 29 juillet, son fondateur anonyme, Tom Williams, disparaît avec les 154 406 bitcoins présents sur les comptes de ses clients. Suite à cet évènement, le prix baissera en flèche jusqu'à atteindre un creux local de 2 $ en novembre.

Mais cela ne décourage pas pour autant les membres de la communauté. Du 19 au 21 août 2011 a lieu la première conférence sur Bitcoin à New York, qui est organisée par Bruce Wagner, l'animateur du *Bitcoin Show*, une émission d'entretiens filmés avec les acteurs de l'écosystème [67]. La conférence revêt un caractère amateur (qui caractérise la communauté d'alors) et seules quatre présentations ont lieu : celle de Bruce Wagner ainsi que les interventions de Gavin Andresen, Jeff Garzik et Stefan Thomas. Cela permet néanmoins aux membres les plus actifs, tels que Roger Ver, Jesse Powell, Jed McCaleb, Mark Karpelès ou Charlie Lee, de se réunir en personne pour la première fois.

Le développement logiciel s'organise aussi. Jusqu'ici, il était centralisé dans les mains de Satoshi, le « dictateur bienveillant » du projet.

Mais après le départ du créateur de Bitcoin, il s'ouvre à la participation de la communauté, sous la supervision de Gavin Andresen. On voit ainsi des contributeurs talentueux commencer à s'impliquer dans l'évolution de Bitcoin comme Nils Schneider, Matt Corallo, Pieter Wuille, Jeff Garzik, Wladimir van der Laan, Luke-Jr ou encore Gregory Maxwell. Des méthodes de coordination sont rapidement mises en place comme la liste de diffusion `bitcoin-development` permettant de discuter formellement des changements à apporter [68], et le système des propositions d'amélioration de Bitcoin (*Bitcoin Improvement Proposals* ou BIP), qui décrivent publiquement ces changements [69].

L'utilisation de Bitcoin devient plus facile. On assiste à l'apparition de portefeuilles légers permettant d'utiliser Bitcoin sans avoir à télécharger et vérifier l'intégralité de la chaîne. Ces derniers utilisent la vérification de paiement simplifiée décrite par Satoshi Nakamoto dans la section 8 du livre blanc. Celle-ci est mise en œuvre par Mike Hearn au sein de sa bibliothèque logicielle *bitcoinj* programmée en Java, qui permet entre autres une meilleure compatibilité avec les applications sur les téléphones multifonctions fonctionnant sous Android. Le premier portefeuille pour mobile, le *Bitcoin Wallet for Android*, est lancé par Andreas Schildbach en mars 2011. Celui-ci montre que l'usage direct de Bitcoin dans la vie de tous les jours est possible. Du côté ordinateur, Thomas Voegtlin crée Electrum en novembre 2011, présenté comme un portefeuille qui permet à l'utilisateur de récupérer ses fonds par le biais d'une phrase mnémotechnique. Cette pratique sera plus tard standardisée et adoptée largement dans l'écosystème.

Ce développement décentralisé est également source de tensions. Sans son fondateur, le projet ne dispose plus d'un meneur incontestable : certes Gavin Andresen possède le contrôle du dépôt, mais n'a pas l'autorité technique suffisante pour imposer toutes ses vues aux autres développeurs. Les décisions sont prises relativement collectivement, ce qui pose la question de la gouvernance de Bitcoin : qui décide d'apporter un changement au protocole ?

À la fin de l'année 2011 et au début de l'année 2012, le premier débat technique en l'absence de Satoshi a lieu. Le groupe de développeurs

est alors encore très restreint mais cela suffit pour créer un conflit à propos de l'amélioration de la programmabilité des transactions, qui permettrait notamment de créer des comptes multisignatures. On s'en souviendra comme la « bataille pour P2SH [70] ».

De par sa nature informatique, Bitcoin constitue un système de monnaie programmable qui permet à l'utilisateur d'imposer des conditions au blocage et au déblocage des fonds. Il dispose pour cela d'un mécanisme de scripts reposant sur des instructions logiques appelées codes opérations. Cependant, ces scripts sont compliqués à gérer. Il s'agit donc de trouver un moyen simple pour l'utilisateur d'envoyer des fonds vers un script défini préalablement par le récipiendaire. C'est l'idée derrière la proposition faite par Nicolas van Saberhagen d'ajouter un nouveau code opération appelé `OP_EVAL`. Cette proposition souffre néanmoins d'un problème de récursivité, ce qui provoque rapidement l'apparition de deux propositions concurrentes : *Pay to Script Hash* (P2SH) proposé par Gavin Andresen et `OP_CHECKHASHVERIFY` (CHV) proposé par Luke-Jr.

Une tension émerge entre les deux propositions, ce qui crée le débat. Amir Taaki, qui ne soutient ni l'une ni l'autre, appelle à la discussion et déclare le 29 janvier 2012 :

> « Ma crainte c'est qu'un jour Bitcoin soit corrompu. Développeurs : considérez cet examen supplémentaire comme une opportunité de construire une culture d'ouverture. [71] »

Finalement, c'est P2SH qui est choisi pour être intégré à Bitcoin sur l'ordre de Gavin Andresen. Cette intégration sera réalisée, non sans difficulté, le 1er avril 2012.

Dans un même temps, la popularisation de Bitcoin se poursuit. Le 28 février, un russo-canadien du nom de Vitalik Buterin, âgé de seulement 18 ans, co-fonde le *Bitcoin Magazine* avec Mihai Alisie, un développeur roumain. Ce média, d'abord uniquement disponible en version web, est distribué en édition papier à partir de mai. Le jeune Vitalik y écrit de nombreux articles documentant l'actualité de

l'époque. Par la suite, de nombreux sites d'information spécialisés verront le jour comme CoinDesk ou CoinTelegraph.

Le 24 avril 2012, un jeu de hasard en ligne nommé SatoshiDICE est lancé par l'entrepreneur américain Erik Voorhees [72]. Le site repose sur un fonctionnement très simple : le joueur envoie des bitcoins à une adresse spécifique et il a une probabilité prédéfinie de recevoir une récompense qui correspond à un multiple du montant envoyé (il a par exemple une chance sur deux de recevoir un peu moins de deux fois sa mise). Le procédé est instantané et aisément vérifiable, ce qui attire de nombreux parieurs.

En tant que libertarien convaincu vivant dans le New Hampshire, Erik Voorhees voit en SatoshiDICE une manière d'échapper à la réglementation. Le 20 août, il réalise même une IPO pour son entreprise sur la plateforme roumaine MPEx. Il revendra la plateforme le 17 juillet 2013 pour 126 315 bitcoins, soit 12,4 millions de dollars au moment de l'acquisition.

Le succès de SatoshiDICE provoque une augmentation significative du nombre de transactions sur la chaîne, qui triple en quelques mois. Cette activité provenant du site est remarquée et dérange certains développeurs qui la qualifient de « spam [73] ».

À la moitié de l'année 2012, Bitcoin est ainsi complètement lancé et prêt à être découvert par un public plus large.

L'amorçage organique de Bitcoin

Les premières années de Bitcoin ont été déterminantes pour son succès. Il a en effet pu grandir dans la discrétion et connaître une croissance organique et prudente, à l'abri de l'opportunisme et de la propagande de notre monde.

Bitcoin a été proposé en 2008 par Satoshi Nakamoto, qui l'a mis en œuvre en janvier 2009. Les débuts ont été difficiles, à tel point qu'il a fallu attendre neuf mois avant que le bitcoin n'acquière un

prix ! Satoshi s'est dévoué pleinement à son œuvre sans jamais profiter personnellement de sa fortune accumulée. En disparaissant en 2011, il a finalement laissé la communauté s'approprier le projet.

Bitcoin a été façonné dans un creuset mêlant cypherpunks, anarchistes, libertariens et autres amoureux de la liberté. Il s'est construit en opposition au système étatico-bancaire traditionnel, où règnent la censure et les renflouements publics. C'est pourquoi le message derrière Bitcoin est si radical et que tant de gens se sont pris de passion pour lui.

Entre 2010 et 2012, les premiers cas d'utilisation de Bitcoin ont émergé. Financement de projets politiquement sensibles, jeu d'argent en ligne, achat de drogues à distance, envois de fonds à l'étranger : il s'agissait d'usages à la limite de légalité, voire complètement illégaux, qui démontraient toute l'efficacité du bitcoin en tant que monnaie incensurable et relativement anonyme. Cependant, cette tendance a été rapidement tempérée comme on a pu le constater durant les années qui ont suivi.

Notes

1. Certains partent du principe que Satoshi Nakamoto serait un pseudonyme utilisé par un groupe d'individus. Néanmoins, nous supposerons ici qu'il n'y avait qu'une seule personne derrière les messages et le code attribués au créateur de Bitcoin, sans pour autant nier que cette personne a pu se faire aider.

2. Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, 09/11/2008 01:58:48 UTC : `https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html`.

3. Satoshi a également réservé le nom de domaine Netcoin.org au même moment, ce qui laisse à penser qu'il n'a pas encore finalisé son choix concernant le nom de son modèle. – Or Weinberger sur Twitter, 23/09/2022 08:54 UTC : `https://twitter.com/orweinberger/status/1573234325046558720`.

4. Gwern Branwen, *Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails*, 17 mars 2014 : `https://gwern.net/doc/bitcoin/2008-nakamoto`.

5. Les archives de la liste de diffusion de Metzdowd sont disponibles publiquement à l'adresse `https://www.metzdowd.com/pipermail/cryptography/`. Les cypherpunks présents en 2008 étaient, entre autres : John Gilmore, Hal Finney, James A. Donald, Robert Hettinga, Zooko Wilcox-O'Hearn, Len Sassaman.

6. Satoshi Nakamoto, *Bitcoin P2P e-cash paper*, 31/10/2008 18:10:00 UTC : `https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html`.

7. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

8. « Nous avons vraiment, vraiment besoin d'un tel système, mais si je comprends bien votre proposition, il ne semble pas pouvoir s'adapter à la taille requise. » – James A. Donald, *Re: Bitcoin P2P e-cash paper*, 02/11/2008, 23:46:23 UTC : `https://www.`

metzdowd.com/pipermail/cryptography/2008-November/014814.html

9. « Les méchants contrôlent couramment des fermes de machines zombies de 100 000 unités ou plus. Les personnes que je connais qui gèrent une liste noire de machines zombies émetteuses de spam me disent qu'elles voient souvent un million de nouveaux machines zombies par jour. C'est la même raison pour laquelle hashcash ne peut pas fonctionner sur l'Internet d'aujourd'hui : les gentils ont une puissance de calcul nettement inférieure à celle des méchants. » – John Levine, *Re: Bitcoin P2P e-cash paper*, 03/11/2008 13:32:39 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014817.html.

10. « Je pense que le vrai problème avec ce système est le marché des bitcoins. Les preuves de travail informatiques n'ont pas de valeur intrinsèque. » – Ray Dillinger, *Re: Bitcoin P2P e-cash paper*, 06/11/2008 05:14:37 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014822.html.

11. Hal Finney, *Re: Bitcoin P2P e-cash paper*, 07/11/2008 23:40:12 UTC : https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html.

12. Hal Finney, *Bitcoin and me*, 19/03/2013 20:40:02 UTC : https://bitcointalk.org/index.php?topic=155054.msg1643833#msg1643833.

13. Satoshi a écrit à James A. Donald : « Je t'ai envoyé les fichiers principaux. (disponibles sur demande pour le moment, publication complète bientôt) » – Satoshi Nakamoto, *Re: Bitcoin P2P e-cash paper*, 17/11/2008 17:24:43 : https://www.metzdowd.com/pipermail/cryptography/2008-November/014863.html.

14. Hal Finney sur Twitter, 11/01/2009 3:33 UTC : https://twitter.com/halfin/status/1110302988.

15. Cette première transaction entre Satoshi et Hal avait pour identifiant f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 et a été confirmée dans le bloc 170 le 12 janvier à 3:30.

16. L'identifiant de la transaction reçue par Dustin (en P2IP) était d71fd2f64c0b34465b7518d240c00e83f6a5b10138a7079d1252858fe7e6b577.

17. Satoshi Nakamoto, *Bitcoin v0.1 released*, 08/01/2009 19:27:40 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html.

18. Hal Finney, *Re: Bitcoin v0.1 released*, 11/01/2009 02:22:01 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html.

19. Satoshi Nakamoto, *Bitcoin v0.1 released*, 16/01/2009 16:03:14 UTC : https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html

20. Satoshi Nakamoto, *Bitcoin open source implementation of P2P currency*, 11 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

21. Satoshi Nakamoto, *Re: Bitcoin open source implementation of P2P currency*, 18 février 2009 : https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:9562.

22. Mike Hearn, *Questions about BitCoin*, 11/04/2009 22:46 UTC : https://plan99.net/~mike/satoshi-emails/thread1.html.

23. Martti Malmi, *P2P Currency could make the government extinct?*, 09/04/2009 17:49:47 UTC : https://web.archive.org/web/20150927195115/https://board.freedomainradio.com/topic/17233-p2p-currency-could-make-the-government-extinct/.

24. Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, Harper Paperbacks, 2016, p. 29.

25. Archive de la page web de Bitcoin : https://web.archive.org/web/20090511173000/http://bitcoin.sourceforge.net/.

26. « J'ai trouvé la première transaction connue de bitcoins en USD dans mes sauvegardes de courriel. J'ai vendu 5 050 BTC pour 5,02 $ le 12-10-2009. » – Martti Malmi sur Twitter, 15/01/2014 : https://twitter.com/marttimalmi/status/423455561703624704. L'identifiant de la transaction était 7dff938918f07619abd38e4510890396b1cef4fbeca154fb7aafba8843295ea2.

27. NewLibertyStandard, *Re: New Exchange Service: "BTC 2 PSC"*, 19/01/2010 08:06:15 UTC : https://bitcointalk.org/index.php?topic=15.msg111#msg111.

28. Satoshi Nakamoto, *New icon/logo*, 24/02/2010 21:24:23 UTC : https://bitcointalk.org/index.php?topic=64.msg504#msg504.

29. Satoshi Nakamoto, *Re: Ummmm... where did my bitcoins go?*, 18/05/2010 20:06:46 UTC : https://bitcointalk.org/index.php?topic=125.msg1149#msg1149.

30. Satoshi Nakamoto, *Re: A few suggestions*, 12/12/2009 17:52:44 UTC : https://bitcointalk.org/index.php?topic=12.msg54#msg54

31. Satoshi Nakamoto, mai 2010, propos rapportés par Nathaniel Popper : https://www.reddit.com/r/Bitcoin/comments/36vnmr/heres_what_satoshi_wrote_to_the_man_responsible/.

32. Laszlo Hanyecz, *Pizza for bitcoins?*, 18/05/2010 00:35:20 UTC : https://bitcointalk.org/index.php?topic=137.msg1141#msg1141.

33. L'identifiant de la transaction de la pizza entre Laszlo Hanyecz et Jeremy Sturdivant était a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d.

34. Gavin Andresen, *Get 5 free bitcoins from freebitcoins.appspot.com*, 11/06/2010, 17:38:45 UTC : https://bitcointalk.org/index.php?topic=183.msg1488#msg1488.

35. Satoshi Nakamoto, *Re: Get 5 free bitcoins from freebitcoins.appspot.com*, 18/06/2010, 23:08:34 UTC : https://bitcointalk.org/index.php?topic=183.msg1620#msg1620.

36. James A. Donald, *Re: [bitcoin-list] New User*, 30/06/2010 22:29:16 : https://web.archive.org/web/20131016002646/http://sourceforge.net/p/bitcoin/mailman/bitcoin-list/?viewmonth=201006. – Dans un autre courriel, James A. Donald ajoutait : « Je ne voulais pas paraître si négatif. Si nous y arrivons, c'est une grande victoire pour la liberté – mais c'est un long périple, et je suis occupé par un autre projet. ».

37. teppy, « *Bitcoin Releases Version 0.3* », *Slashdot*, 11 juillet 2010 : https://news.slashdot.org/story/10/07/11/1747245/Bitcoin-Releases-Version-03.

38. Gwern Branwen, *2014 Jed McCaleb MtGox interview*, 16 février 2014 : https://www.gwern.net/docs/bitcoin/2014-mccaleb.

39. Jed McCaleb, *Re: New Bitcoin Exchange*, 18/07/2010 02:53:07 UTC : https://bitcointalk.org/index.php?topic=444.msg3891#msg3891.

40. Le 13 août 2010, le ferme de minage d'ArtForz était constituée de 6 cartes graphiques ATI Radeon HD 5770 ; à la fin, elle se composait de 24 ATI Radeon HD 5970. – Tim Swanson, *How ArtForz changed the history of Bitcoin mining*, 20 avril 2014 : https://www.ofnumbers.com/2014/04/20/how-artforz-changed-the-history-of-bitcoin-mining/.

41. Jeff Garzik, *Strange block 74638*, 15/08/2010, 18:08:49 UTC : https://bitcointalk.org/index.php?topic=822.msg9474#msg9474

42. Satoshi Nakamoto, *Development of alert system*, 22/08/2010 23:55:06 UTC : https://bitcointalk.org/index.php?topic=898.msg10722#msg10722. – Après avoir servi entre 2012 et 2015, ce système d'alerte a été progressivement désactivé pour finir par être définitivement supprimé du logiciel en 2017 (https://bitcoin.org/en/alert/2016-11-01-alert-retirement).

43. Marek Palatinus, *Cooperative mining*, 27/11/2010, 13:45:41 UTC : https://bitcointalk.org/index.php?topic=1976.msg24844#msg24844.

44. « Nous ne voulons pas mettre l'aspect "anonyme" au premier plan. (J'avais l'intention de modifier la page d'accueil) "Les développeurs s'attendent à ce que cela se traduise par une monnaie stable par rapport à l'énergie et hors de portée de tout État." – Je ne fais certainement pas ce genre de provocation ou d'affirmation. » – Satoshi Nakamoto, *Re: Slashdot Submission for 1.0*, 05/07/2010 21:31:14 UTC : https://bitcointalk.org/index.php?topic=234.msg1976#msg1976.

45. L'histoire de Bradley Manning (devenu Chelsea Manning après une transition de genre) est narrée par Andy Greenberg dans son ouvrage *This Machine Kills Secrets* publié en 2012.

46. Amir Taaki, *Wikileaks contact info?*, 10/11/2010 12:49:16 UTC : https://bitcointalk.org/index.php?topic=1735.msg21271#msg21271.

47. ShadowOfHarbringer, *Re: Wikileaks contact info?*, 10/11/2010 13:28:00 UTC : https://bitcointalk.org/index.php?topic=1735.msg21283#msg21283.

48. Wladimir van der Laan, *Re: Wikileaks contact info?*, 04/12/2010 08:57:41 UTC : https://bitcointalk.org/index.php?topic=1735.msg26737#msg26737.

49. Satoshi Nakamoto, *Re: Wikileaks contact info?*, 05/12/2010 09:08:08 UTC, https://bitcointalk.org/index.php?topic=1735.msg26999#msg26999

50. Satoshi Nakamoto, *Re: PC World Article on Bitcoin*, 11/12/2010 23:39:16 UTC, https://bitcointalk.org/index.php?topic=2216.msg29280#msg29280.

51. Le contrôle du site a été cédé à un individu utilisant le pseudonyme Cøbra tandis que la charge du forum a été donnée à Michael Marquardt (theymos). Les deux personnes co-gèrent ces deux plateformes.

52. Gavin Andresen, *Development process straw-man*, 19/12/2010 16:41:39 UTC : https://bitcointalk.org/index.php?topic=2367.msg31651#msg31651.

53. Satoshi Nakamoto, *Re: Holding coins in an unspendable state for a rolling time*

window, 23/04/2011 13:40 UTC : https://plan99.net/~mike/satoshi-emails/thread5.html.

54. Allie Jones, « *Former Coworker Regrets Helping Reveal Identity of Bitcoin's Founder* », *The Wire*, 6 mars 2014, archive : https://web.archive.org/web/20140309041730/http://www.thewire.com/technology/2014/03/bitcoin-founders-coworker-regrets-doxxing-him/358878.

55. « WikiLeaks accepte désormais les dons anonymes en bitcoin sur 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v » – WikiLeaks sur Twitter, 14/06/2011 23:12 UTC : https://twitter.com/wikileaks/status/80774521350668288.

56. Ce montant a été retrouvé grâce au Patoshi Pattern, mis en lumière par Sergio Lerner en 2013 dans un article intitulé *The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius* (https://bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/). L'estimation utilisée ici est celle de Whale Alert publiée en 2020 : https://whale-alert.medium.com/the-satoshi-fortune-e49cf73f9a9b.

57. Un message provenant de son compte du compte de Satoshi sur le forum de la Fondation P2P a été publié le 7 mars 2014 pour nier son association à Dorian Nakamoto (https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008:Comment:52186), et un courriel d'opposition à Bitcoin XT a été envoyé le 15 août 2015 à la liste de diffusion de développement depuis son adresse satoshi@vistomail.com (https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-August/010238.html).

58. Parmi les candidats pour être la figure de Satoshi Nakamoto, ceux qui reviennent le plus souvent sont : Nick Szabo, Hal Finney, Adam Back, Len Sassaman.

59. Hal Finney, *Re: Another *Potential* Identifying Piece of Evidence on Satoshi*, 15/06/2013 01:23:42 UTC : https://bitcointalk.org/index.php?topic=234330.msg2479328#msg2479328.

60. Leah McGrath Goodman, « *The Face Behind Bitcoin* », *Newsweek Magazine*, 6 mars 2014 : https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html.

61. Andy Greenberg, « *Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius* », *Forbes*, 25 mars 2014 : https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/.

62. Hal Finney, *Re: Parity Party*, 11/01/2011 21:17:04 UTC : https://bitcointalk.org/index.php?topic=2734.msg37307#msg37307.

63. La première mention publique de Silk Road par Ross Ulbricht remonte au 27 janvier 2011 sur le forum de *The Shroomery*, un site consacré aux champignons hallucinogènes, où il prétendait être tombé par hasard sur la place de marché. – Ross Ulbricht, *anonymous market online?*, 27/01/2011 22:28 UTC : https://www.shroomery.org/forums/showflat.php/Number/13860995.

    Ross Ubricht a réitéré cette manœuvre sur le *Bitcoin Forum*, où il a écrit le 29 janvier : « Quelqu'un a-t-il déjà visité Silk Road ? C'est un peu comme un amazon.com anonyme. Je ne pense pas qu'il y ait de l'héroïne sur ce site, mais ils vendent d'autres choses. Ils utilisent essentiellement bitcoin et tor pour négocier des transactions anonymes. » – Ross Ulbricht, *Re: A Heroin Store*, 29/01/2011 19:44:51 UTC, https://bitcointalk.org/index.php?topic=175.msg42670#msg42670.

64. WeUseCoins, *What is Bitcoin?* (vidéo), 22 mars 2011 : https://www.youtube.com/watch?v=Um63OQz3bjo.

65. Adrian Chen, « *The Underground Website Where You Can Buy Any Drug Imaginable* », *Gawker*, 1er juin 2011 : https://www.gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

66. L'identifiant de la transaction de preuve de solvabilité de Mt. Gox en 2011 était 3a1b9e330d32fef1ee42f8e86420d2be978bbe0dc5862f17da9027cf9e11f8c4.

67. La chaîne Youtube de Bruce Wagner se trouve à l'adresse https://www.youtube.com/@vlogwrap. Les vidéos des présentations à la conférence peuvent y être retrouvées.

68. Jeff Garzik, *[Bitcoin-development] Preparing 0.3.23-rc1 release*, 12/06/2011 02:23:58 UTC : https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-June/000000.html.

69. Le système des BIP a été initialement proposé le 19 septembre 2011 par Amir Taaki sous le nom de *Bitcoin Enhancement Proposals*, en référence directe aux *Python Enhancement Proposals* (PEP) dont il s'est inspiré. (Amir Taaki, *[Bitcoin-development] Bitcoin Enhancement Proposals (BEPS)*, 19/09/2011 00:31:55 UTC, https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2011-September/000554.html)

70. Pete Rizzo, Aaron van Wirdum, « *The Battle For P2SH: The Untold Story Of The First Bitcoin War* », *Bitcoin Magazine*, 4 décembre 2020 : https://bitcoinmagazine.com/technical/the-battle-for-p2sh-the-untold-story-of-the-first-bitcoin-war.

71. Amir Taaki, *The Truth behind BIP 16 and 17 (important read)*, 29/01/2012 03:54:08 UTC : https://bitcointalk.org/index.php?topic=61705.msg719790#msg719790.

72. Erik Voorhees, *SatoshiDICE.com - The World's Most Popular Bitcoin Game*, 24/04/2012 02:17:31 UTC : https://bitcointalk.org/index.php?topic=77870.msg865877#msg865877.

73. Matt Corallo, *Huge increase in satoshidice spam over the past day*, 13/06/2012 23:21:47 UTC : https://bitcointalk.org/index.php?topic=87444.msg961132#msg961132.

Notes supplémentaires

Chapitre 1

(page 2) « Satoshi Nakamoto se met à travailler sur Bitcoin au printemps 2007 » : https://bitcointalk.org/index.php?topic=13.msg46#msg46, https://www.metzdowd.com/pipermail/cryptography/2008-November/014863.html.

(page 2) « il rentre en contact avec Adam Back » : Adam Back, *Re: Introduce yourself :)*, 18/04/2013 11:27:49 UTC : https://bitcointalk.org/index.php?topic=15672.msg1873483#msg1873483.

(page 5) « Hal et Ray réalisent alors un examen minutieux du code » : Ray Dillinger, *If I'd Known What We Were Starting*, 20 septembre 2017 : https://www.linkedin.com/pulse/id-known-what-we-were-starting-ray-dillinger/.

(page 5) « Après avoir échangé avec Satoshi » : https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf.

(page 6) « Dustin Trammell communique aussi avec Satoshi par courriel, et reçoit 25 bitcoins de sa part le 15 janvier » : http://web.archive.org/web/20131204164149/http://www.dustintrammell.com/files/Satoshi_Nakamoto.zip.

(page 10) « Certains individus minent en continu » : Ludovic Lars, *Les premiers mineurs de Bitcoin*, 19 juin 2022 : https://journalducoin.com/analyses/premiers-mineurs-bitcoin/.

(page 11) « Les prix sont publiés quotidiennement sur son site » : https://web.archive.org/web/20091229132610/http://newlibertystandard.wetpaint.com/page/Exchange+Rate.

(page 11) « Satoshi annonce la sortie de la version 0.2 du logiciel » : Satoshi Nakamoto, *Bitcoin 0.2 released!*, 16/12/2009 22:45:36 UTC : https://bitcointalk.org/index.php?topic=16.msg73#msg73.

(page 11) « Au début de l'année 2010, le bitcoin est désigné comme une "cryptomonnaie" » : https://web.archive.org/web/20100106082749/http:

//www.bitcoin.org/

(page 12) « NLS propose que le bitcoin [...] adopte le sigle boursier BTC et le symbole du baht thaïlandais » : NewLibertyStandard, *Bitcoin Currency Symbol ℬ*, 05/02/2010 01:48:53 UTC : https://bitcointalk.org/index.php?topic=41.msg238#msg238.

(page 13) « NLS ouvre un magasin en ligne où il propose à la vente des timbres et des autocollants » : Liberty Swap Variety Shop, https://web.archive.org/web/20100414172623/http://newlibertystandard.wetpaint.com/page/Specialty+Shop.

(page 13) « D'autres services acceptant le bitcoin apparaissent » : https://web.archive.org/web/20100517040312/http://www.bitcoin.org:80/trade.

(page 13) « la première partie de poker mettant en jeu des bitcoins est organisée » : Kai Sedgwick, *Bitcoin History Part 14: The 1,000 BTC Poker Game*, 9 août 2019 : https://news.bitcoin.com/bitcoin-history-part-14-the-1000-btc-poker-game/.

(page 14) « Après avoir acheté des bitcoins à NLS » : https://blockchair.com/bitcoin/transaction/faf172f5dc06b0ae03268555dddcd65be47e9a8a8bb44a122b12bfaf735f9a81?o=1

(page 14) « celui-ci programme début mai un logiciel de minage qui s'adapte aux cartes graphiques » : Laszlo Hanyecz, *Generating Bitcoins with your video card (OpenCL/CUDA)*, 10/05/2010, 14:03:57 UTC : https://bitcointalk.org/index.php?topic=133.msg1103#msg1103.

(page 15) « un jeune Californien du nom de Jeremy Sturdivant accepte l'échange sur la messagerie instantanée IRC » : Bitcoin Who's Who, *A Living Currency*, 22 mai 2015 : https://www.bitcoinwhoswho.com/jercosinterview; archive : https://web.archive.org/web/20150528074728/http://bitcoinwhoswho.com/jercosinterview/.

(page 15) « un développeur américain de 44 ans, nommé Gavin Andresen, découvre Bitcoin par le biais d'un article publié sur InfoWorld » : Neil McAllister, *Open source innovation on the cutting edge*, 24 mai 2010 : https://www.infoworld.com/article/2627013/open-source-innovation-on-the-cutting-edge.html?page=3.

(page 16) « jusqu'à sa fermeture deux ans plus tard » : Gavin Andresen, *Bitcoin Faucet Hacked*, 2 mars 2012 : https://gavintech.blogspot.com/2012/03/bitcoin-faucet-hacked.html.

(page 17) « Le réseau tient le coup malgré la montée en charge » : Gavin Andresen, *Re: Scalability*, 14/7/2010, 04:22:49 UTC : https://bitcointalk.org/index.php?topic=286.msg2745#msg2745.

(page 17) « Parmi les personnes qui découvrent Bitcoin grâce à Slashdot, il y a Jed

McCaleb » : The Ripple Blog, *Interview with Jed McCaleb, inventor of the Ripple protocol and co-founder of OpenCoin*, 17 avril 2013 : https://web.archive.org/web/20130428155220/https://ripple.com/blog/interview-with-jed-mccaleb-inventor-of-the-ripple-protocol-and-co-founder-of-opencoin/.

(page 17) « la plateforme de change Mt. Gox [...] est lancée et annoncée officiellement sur le forum par Jed » : Jed McCaleb, *New Bitcoin Exchange*, 18/07/2010 01:57:19 UTC : https://bitcointalk.org/index.php?topic=444.msg3866#msg3866.

(page 18) « Satoshi s'empresse d'inclure la correction dans la mise à jour 0.3.6 » : Satoshi Nakamoto, **** ALERT *** Upgrade to 0.3.6*, 29/07/2010 19:13:06 UTC : https://bitcointalk.org/index.php?topic=626.msg6451#msg6451.

(page 18) « il publie un correctif créant une chaîne alternative ne contenant pas la transaction incriminée » : Satoshi Nakamoto, *Version 0.3.10 - block 74638 overflow PATCH!*, 15/08/2010 23:48:22 UTC : https://bitcointalk.org/index.php?topic=827.msg9590#msg9590.

(page 18) « la chaîne correcte devient plus longue que l'autre le lendemain à 8 heures 10 du matin » : Satoshi Nakamoto, *Re: overflow bug SERIOUS*, 16/08/2010 12:59:38 UTC : https://bitcointalk.org/index.php?topic=823.msg9734#msg9734.

(page 19) « il a grossi à tel point qu'il devient difficile de diriger le mouvement » : Pete Rizzo, « *The Last Days of Satoshi: What Happened when Bitcoin's Creator Disappeared* », *Bitcoin Magazine*, 26 avril 2021 : https://bitcoinmagazine.com/technical/what-happened-when-bitcoin-creator-satoshi-nakamoto-disappeared.

(page 20) « PayPal gèle le compte de WikiLeaks » : *PayPal statement regarding WikiLeaks*, 3 décembre 2010 : https://web.archive.org/web/20101206112350/https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks/.

(page 21) « met en péril la survie financière de l'ONG » : Le 24 octobre 2011, un communiqué de WikiLeaks (*Banking Blockade*, 24/10/2011 13:00 UTC, https://wikileaks.org/Banking-Blockade.html) a indiqué que le blocus financier a fait disparaître de ses 95 % des revenus.

(page 21) « un article est publié sur PC World pour mettre en avant la possibilité d'un usage de Bitcoin par WikiLeaks » : Keir Thomas, *Could the Wikileaks Scandal Lead to New Virtual Currency?*, 11 décembre 2010, 00:30 : https://www.pcworld.com/article/499375/could_wikileaks_scandal_lead_to_new_virtual_currency.html.

(page 21) « Il vendra ses 55 000 bitcoins pour s'acheter un appartement près de Helsinki » : Martti Malmi sur Twitter, 18/12/2020 12:22 UTC : https://twitter.com/marttimalmi/status/1339908783187832834.

(page 22) « Gavin annonce qu'il a été invité par la CIA » : Gavin Andresen, *Gavin will visit the CIA*, 27/04/2011 19:00:26 UTC : https://bitcointalk.org/index.php?topic=6652.msg97181#msg97181.

(page 22) « Cette visite se passe le 14 juin » : Gavin Andresen sur Twitter, 14/06/2011 23:55 UTC : https://twitter.com/gavinandresen/status/80785477342478336.

(page 24) « en aucun cas des cartes bancaires volées, de la pédopornographie ou des services de tueur à gages » : Capture du *Seller's Guide* du 18/9/2012 (GX-120), https://antilop.cc/sr/exhibits/GX-120_Redacted.pdf : « Ne pas mettre en vente les objets dont le but est de nuire ou de frauder, comme les objets ou les informations volés, les cartes de crédit volées, la fausse monnaie, les informations personnelles, les assassinats et les armes de toutes sortes. Ne pas mettre en vente les objets liés à la pédophilie. »

(page 24) « une partie de l'épisode de FreeTalkLive du jour est consacrée à Bitcoin et à Silk Road » : https://soundcloud.com/freetalklive/ftl2011-03-16.

(page 24) « commence à l'accepter avec son entreprise » : Roger Ver, *Re: Earn 131BTC or 12-13BTC for getting shops/organisations to accept Bitcoin!*, 26/04/2011 08:00:52 UTC : https://bitcointalk.org/index.php?topic=4667.msg95746#msg95746.

(page 25) « son fondateur anonyme, Tom Williams, disparaît avec les 154 406 bitcoins présents sur les comptes de ses clients » : shotgun, *mybitcoin down or just me?*, 29/07/2011 22:41:36 UTC : https://bitcointalk.org/index.php?topic=32900.msg411251#msg411251.

(page 26) « Le premier portefeuille pour mobile [...] est lancé par Andreas Schildbach en mars 2011 » : Andreas Schildbach, *Bitcoin Wallet for Android*, 11/03/2011 21:25:51 UTC : https://bitcointalk.org/index.php?topic=4384.msg64142#msg64142.

(page 26) « Thomas Voegtlin crée Electrum en novembre 2011 » : Thomas Voegtlin, *[Electrum] a brainwallet in twelve words*, 10/11/2011 01:06:59 UTC : https://bitcointalk.org/index.php?topic=51397.msg612674#msg612674.

(page 28) « il réalise même une IPO pour son entreprise sur la plateforme roumaine MPEx » : Erik Voorhees, *S.DICE - SatoshiDICE 100% Dividend-Paying Asset on MPEx*, 20/08/2012 04:14:43 UTC : https://web.archive.org/web/20121024050433/https://bitcointalk.org/index.php?topic=101902.0.

(page 28) « Il revendra la plateforme le 17 juillet 2013 pour 126 315 bitcoins, soit 12,4 millions de dollars au moment de l'acquisition » : Erik Voorhees, « *SatoshiDice Sold for $12.4 Million* », *Bitcoin Magazine*, 28 juillet 2012 : https://bitcoinmagazine.com/markets/satoshidice-sold-12-4-million.