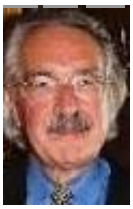
Institut Turgot

Le monde Bitcoin et l'avenir des systèmes "pair à pair": 1) comment ça marche

Par Gérard Dréan le lundi 14 juillet 2014, 15:11 - Note de synthèse - Lien permanent

- Bitcoin
- Informatique
- Innovation
- Internet
- Monnaie
- Monnaie électronique
- Réseaux
- systèmes de paiement



*Partir à la découverte de **Bitcoin**, c'est s'embarquer pour un voyage sans fin.*
En explorant les blogs, les forums et les wikis, on découvre des choses qu'on avait mal comprises ou dont on n'avait pas perçu l'importance, qui viennent corriger des opinions qu'on s'était forgées, répondre à des questions restées ouvertes ou soulever de nouvelles questions qui incitent à poursuivre l'exploration.
Dans une situation aussi dynamique, il n'est pas inutile de faire le point de temps en temps, même au risque de se répéter ou de devoir rectifier ses positions antérieures.
*Notre ami **Gérard Dréan** nous propose de revenir en détail sur le monde Bitcoin, avec deux articles dont le second concernera les conséquences sociétales de cette révolution technologique.*
Vos réactions à ce premier texte seront les bienvenues car elles permettront d'enrichir le suivant.

Dans ce monde mouvant, une question fait figure de point fixe : le phénomène bitcoin est-il le début d'une profonde révolution sociétale ou une bulle en forme de gigantesque arnaque ?
Les meilleurs esprits continuent à apporter les réponses les plus divergentes, dont un trop grand nombre repose encore sur une méconnaissance des réalités technologiques du système. En particulier, ceux qui sont plus économistes qu'informaticiens transposent trop rapidement leurs positions sur la monnaie, alors que Bitcoin est un animal complètement différent et que l'immense majorité d'entre eux est aveuglée par la croyance superstitieuse née au vingtième siècle que la monnaie est nécessairement l'affaire des États.
A l'inverse, les pronostics enthousiastes des informaticiens ignorent le plus souvent les réalités de la concurrence appliquées au domaine monétaire.

De toute façon, il semble bien qu'appliquer imprudemment à Bitcoin des connaissances acquises, que ce soit en informatique ou en économie, mène à nombre d'erreurs, tant les principes informatiques sur lesquels il repose, tout comme les mécanismes économiques qu'il met en jeu, échappent à nos cadres de réflexion habituels.
C'est pourquoi, avant toute réflexion sur ses aspects monétaires, il convient de rappeler inlassablement ce qu'est Bitcoin et dans quel contexte il évolue. Cette première partie commencera donc par quelques rappels techniques indispensables à tout jugement, et se poursuivra par une visite du milieu inhabituel où grandit Bitcoin. Dans une deuxième partie, nous explorerons les conséquences économiques et sociétales potentielles. Il serait bien sûr présomptueux de formuler un pronostic ; nous nous contenterons donc de planter le décor, de présenter les protagonistes, de rappeler les règles du jeu et d'évoquer quelques pistes.

Bitcoin et bitcoin

Le terme « bitcoin » désigne à la fois un système de paiement électronique pair à pair (Bitcoin nom propre, avec une majuscule) et l'unité de compte utilisée dans ce système (le bitcoin nom commun, avec un article et une minuscule).

Un système de paiement est un dispositif qui permet de transférer des unités de compte d'un utilisateur à un autre. Les utilisateurs peuvent accepter ces unités en échange de services ou de biens, ce qui donne à ces unités de compte un rôle de monnaie.

Au sens général, un système pair à pair est une société coopérative où chaque participant a les mêmes droits, notamment la possibilité de jouer tous les rôles et d'offrir librement ses services. Réciproquement, chacun peut librement choisir les services qu'il désire utiliser, sans qu'aucune fonction ne soit réservée par construction à certains participants. Remarquons que c'est la définition d'une société libre ou du marché libre ; ce n'est pas un hasard si les promoteurs de Bitcoin se réclament de positions libérales voire libertariennes.

En informatique, un système pair à pair est un ensemble de machines liées par un réseau de communications, où chacune est dotée des fonctionnalités correspondant à tous les rôles possibles, où chaque utilisateur peut offrir librement les services qu'il souhaite offrir et peut réciproquement choisir librement les services qu'il désire utiliser, sans qu'aucune fonction ne soit réservée autoritairement à certains participants. Chaque utilisateur peut être en même temps prestataire de services.

Un système pair à pair se caractérise donc par l'absence d'un système central auquel les participants seraient contraints de s'adresser pour certaines fonctions. Il peut être conçu de façon qu'un grand nombre de nœuds concourent à offrir les mêmes services, se contrôlent mutuellement et se portent secours en cas de besoin, assurant ainsi au système une sécurité et une inviolabilité quasi-totales.

Le système Bitcoin

Les fonctions essentielles du système Bitcoin sont réalisées par un logiciel standard téléchargeable gratuitement et qui peut être installé sur n'importe quel ordinateur, Ce logiciel permet de créer des comptes, de créer des transactions et de tenir à jour le grand livre des transactions en contrôlant la validité des transactions émises par les autres utilisateurs.

Une transaction consiste à transférer d'un utilisateur A à un utilisateur B une certaine quantité M d'unités appelées bitcoins. Cette transaction n'est légitime que si elle est émise par A, et si A a reçu préalablement M unités (au moins), ce que tout utilisateur qui le souhaite peut vérifier. Si oui, ce mouvement est enregistré de façon irréversible et publique, ce qui autorise alors B à transférer de la même façon à C tout ou partie de ces mêmes unités.

B peut accepter ce transfert comme contrepartie d'un service qu'il a rendu à A ou d'un bien qu'il lui a cédé, et de même C pourra l'accepter comme contrepartie d'un service qu'il a rendu à B ou d'un bien qu'il lui a cédé, Par cette confiance que les utilisateurs s'accordent mutuellement, l'unité de compte utilisée, le bitcoin, devient un instrument d'échange indirect, c'est-à-dire une monnaie.

Ce mécanisme psychologique n' a rien de mystérieux ni d'exceptionnel : c'est le même qui nous fait accepter un chèque, un billet de banque ou une carte de crédit. Il y a quand même une différence : cette monnaie bitcoin n'est utilisable qu'à l'intérieur du système de paiement Bitcoin, une limitation qu'il ne faut pas oublier dans toute discussion du bitcoin en tant que monnaie. C'est en somme une monnaie locale utilisée par les membres du réseau Bitcoin et eux seuls, à ce détail près que tous les internautes, soit quelques milliards d'individus sur tout le globe, peuvent devenir membres de ce réseau gratuitement, en quelques minutes et sans formalités.

Le cœur du système est formé de l'historique complet des transactions légitimes et de l'ensemble des processus informatiques qui le construisent. Dans cet historique, les transactions sont enregistrées en clair et sont lisibles par n'importe qui mais ne peuvent être ni modifiées ni effacées.

Les « comptes »

L'émetteur de chaque transaction doit pouvoir dire à qui il donne le droit d'en utiliser le montant pour le transférer à son tour à quelqu'un d'autre. Cette question est résolue par un système de signatures cryptographiques faisant appel à la cryptographie asymétrique à double clé.

Chaque utilisateur peut demander au système de créer pour lui un nombre quelconque de paires de clés, chacune des clés d'une paire permettant de crypter des messages et de décrypter les messages codés par l'autre. Une des deux, la clé publique, pourra être communiquée à des tiers, voire publiée dans un annuaire ou figurer dans des documents officiels. L'autre, la clé privée, devra être tenue secrète par son titulaire, et lui servira notamment de signature. Si j'envoie à un correspondant un message connu de ce dernier, en le cryptant par ma clé privée, il pourra vérifier que je suis bien l'auteur du message en le décryptant avec ma clé publique. Je peux ainsi signer les transactions que je crée et permettre à tous les autres utilisateurs de vérifier que j'en suis bien l'auteur.

En réalité, ce n'est pas réellement la clé publique qui est publiée, mais une version « durcie » de celle-ci, qui me servira d'identificateur et est improprement appelée « numéro de compte ». Ces identificateurs sont en réalité des nombres de 160 bits représentés sous une forme ésotérique dont voici un exemple :

« *1Lke9VyQHixh8zxteh7mENSr4wsX5N6BeN* »

Le titulaire de cet identificateur peut, pour son usage propre, le désigner par un nom symbolique de son choix (par exemple « Jules »), mais qui n'apparaîtra jamais dans le registre ou les autres fichiers publics. Ce qui est appelé « compte » dans Bitcoin n'est qu'une paire de clés qui permet de créer et d'exploiter des transactions. En particulier aucun solde n'apparaît jamais dans le registre central.

Les utilisateurs conservent généralement ces adresses, avec éventuellement d'autres informations personnelles, dans un « *wallet* » (portefeuille ou plus exactement porte-clés), qui offre aussi les fonctions de création de transactions et d'exploitation des transactions reçues. Il existe plusieurs logiciels de gestion de « *wallet* », pouvant résider sur un ordinateur partagé, sur l'ordinateur de l'utilisateur ou sur smartphone, voire sur carte magnétique. Quel que soit ce support, c'est la responsabilité de chaque utilisateur de protéger son « *wallet* » pour conserver l'anonymat en rendant impossible à un tiers d'associer son identité à ses comptes, à l'exception de celui qu'il a choisi comme clé publique. A cet effet, les « *wallets* » sont souvent protégés par des dispositifs cryptographiques perfectionnés.

Rappelons que chaque utilisateur peut avoir un nombre quelconque de « comptes », c'est-à-dire de paires de clés. Mais comme le mot « compte », le mot « *wallet* » (portefeuille en anglais) est impropre puisque c'est un simple porte-clés qui ne contient pas les bitcoins de l'utilisateur, mais seulement les clés qui lui permettent d'interagir avec le système. Nous emploierons quand même les termes français consacrés « portefeuille » et « compte ».

Les transactions

Quand il s'est créé un portefeuille et des comptes, l'utilisateur peut émettre des transactions pour transférer des bitcoins depuis un ou plusieurs de ses comptes vers un ou plusieurs autres, pouvant appartenir à un autre utilisateur. Ces transactions sont anonymes, puisque seuls les codes des portefeuilles y figurent, et que les utilisateurs peuvent conserver secrets les liens entre eux-mêmes et leurs portefeuilles, rendant ainsi impossible de remonter d'un portefeuille vers son propriétaire.

Chaque transaction est signée cryptographiquement par son émetteur, qui doit aussi spécifier à quelle(s) condition(s) un autre utilisateur peut s'en approprier le montant. Dans le cas le plus simple et le plus courant, l'émetteur indiquera un numéro de compte à créditer et demandera à l'autre utilisateur de prouver, par sa signature cryptographique, qu'il en est le titulaire.

En réalité, cette condition est définie par l'émetteur de la transaction sous la forme d'un programme (un « script de sortie ») écrit dans un langage spécifiquement adapté et qui fait partie intégrante de la transaction. L'utilisateur qui veut utiliser le montant de cette transaction dans une nouvelle transaction émise par lui devra inclure dans celle-ci un programme écrit dans le même langage qui fournira les données du script de sortie de la transaction à laquelle il fait référence.

Ces conditions peuvent être très variées. Par exemple, l'émetteur peut simplement demander la réponse à une question plus ou moins difficile, et créditer du montant indiqué le premier utilisateur qui donnera la réponse correcte ; c'est alors un concours. Ou bien l'émetteur peut demander, outre l'identification d'un destinataire, la signature d'un ou plusieurs tiers ; on obtient ainsi un compte sous séquestre. Ou encore le paiement peut être conditionné par un événement qui sera annoncé sur Internet (réussite à un examen pour une récompense, victoire d'une équipe dans une compétition pour un pari, décès pour un testament, etc.). Cette condition peut être arbitrairement complexe, ouvrant la voie à une infinité de formes de mouvements couvrant potentiellement toute une gamme de transactions financières, existantes ou nouvelles.

Une transaction complète peut regrouper des montants issus de plusieurs transactions antérieures et ventiler le montant total en plusieurs sorties, assortie chacune d'un montant et d'un script définissant la condition d'utilisation de ce montant.

Le registre des transactions

Chaque transaction est d'abord diffusée de proche en proche à tous les ordinateurs du réseau, qui vérifient tous son intégrité et sa légitimité par rapport aux transactions antérieures. D'une façon générale, le système Bitcoin applique un principe de méfiance généralisée : tout nœud du réseau est considéré *a priori* comme susceptible de frauder, et donc chaque nœud vérifie l'intégrité de tout ce qu'il reçoit des autres. Une transaction illégitime est ignorée ; une transaction légitime est rangée dans une file d'attente locale et transmise aux nœuds voisins, et ainsi de proche en proche à tout le réseau.

La suite de l'opération se passe en deux temps, La première étape consiste à assembler les transactions en « blocs » intangibles structurés de façon à faciliter les recherches ultérieures, comme si on les inscrivait à l'encre indélébile sur des pages de registre. La deuxième consiste à assembler les blocs ainsi obtenus pour créer l'historique complet (la « *blockchain* »), ce qui est analogue à la reliure inviolable des pages ainsi créées.

Dans l'étape 1, chacun des blocs est protégé par somme de contrôle, un procédé habituel en informatique. Mais ici, on impose à cette somme des conditions qui en rendent le calcul extrêmement gourmand en ressources informatiques (temps de calcul et/ou mémoire). De plus, les blocs sont conçus pour que toute modification oblige à recalculer non seulement la somme de contrôle du bloc modifié, mais aussi celle de tous les suivants dans la *blockchain*, ce qui devient vite totalement prohibitif. Parce qu'elle très lourde en temps machine, cette étape ne peut être exécutée avec succès que par des nœuds spécialisés dont les propriétaires sont récompensés par des bitcoins créés à cet effet, ce qui leur vaut le nom de « mineurs ».

L'étape 2, au contraire, est exécutée en parallèle par un grand nombre de nœuds, dont chacun tient à jour son propre exemplaire du registre des transactions. Quand un mineur parvient à assembler un bloc valide, il le transmet aux nœuds voisins qui vérifient à leur tour sa validité et celle de toutes les transactions qu'il contient avant de l'ajouter à leur *blockchain* locale et de le transmettre à leurs propres voisins qui procéderont à leur tour aux mêmes opérations. Chaque transaction est donc revérifiée un nombre incalculable de fois avant d'être définitivement inscrite dans les multiples exemplaires de la *blockchain*.

Le coût de cette opération est un très grand encombrement en mémoire. C'est pourquoi on a vu apparaître récemment des serveurs légers (*thin clients*) qui se dispensent de tenir à jour le registre complet, et font appel aux autres nœuds du réseau, appelés serveurs complets (*full nodes*), pour y avoir accès à travers un protocole sécurisé, faisant souvent appel à plusieurs dizaines de serveurs voisins, éventuellement choisis de façon aléatoire, pour se prémunir contre toute erreur ou toute fraude.

Une transaction n'est confirmée que quand elle a été incorporée à un bloc et que ce bloc a été ajouté à la *blockchain*. Afin de rendre la *blockchain* infalsifiable, la difficulté de création d'un bloc est réglée de telle façon que le calcul d'une clé de contrôle acceptable exige en moyenne 10 minutes, quelle que soit la puissance de l'ordinateur qui s'en est chargé. Le délai de confirmation d'une transaction est donc d'au moins dix minutes, voire plus si on veut s'assurer que le bloc qui la contient est lui-même confirmé par les blocs suivants et ne pourra plus jamais être modifié. On admet que si un bloc est suivi dans la *blockchain* par six blocs confirmés, donc au bout d'une heure, les transactions qu'il contient sont irrévocables.

Toutes les transactions enregistrées dans la *blockchain*, y compris les clés publiques de leurs émetteurs et de leurs bénéficiaires et les *scripts* associés, sont visibles par toutes les personnes intéressées. Bien que l'identité des utilisateurs n'y apparaisse pas, il est possible de remonter des clés publiques à l'identité de leurs possesseurs, ce qui donne certaines possibilités de contrôle et d'audit. Mais les utilisateurs soucieux de confidentialité peuvent mettre en place des procédés cryptographiques utilisant le réseau pair à pair pour entraver cette « réidentification », qui ne peut alors être réalisée qu'au prix d'une véritable enquête de police par des experts.

La structure générale du système

Au total, le système Bitcoin se compose donc de plusieurs couches :

- au centre, un réseau formé des serveurs complets fonctionnant en mode pair à pair, où un grand nombre d'intervenants (de l'ordre de 10000 en juin 2014) assurent en parallèle et indépendamment les mêmes fonctions, gèrent chacun un exemplaire local de la base de données fondamentale, se contrôlent mutuellement et se prêtent secours en cas de besoin ;
- un réseau de serveurs plus légers (probablement de l'ordre du million) qui ne se construisent pas un exemplaire local de la *blockchain,* mais font appel aux serveurs complets pour accéder aux transactions ;
- parmi tous les précédents, un certain nombre, probablement plusieurs milliers, assurent les fonctions de mineurs, la plupart regroupés en une grosse centaine de coopératives (« *pools* ») pour mettre en commun leur puissance de calcul ;
- le tout entouré de points d'entrée sous forme d'au moins autant de « *wallets* » que d'utilisateurs (plus de 3 millions en juin 2014), allant d'une simple appli sur smartphone pour un particulier à une fonction intégrée au système de gestion local pour un site marchand, une banque ou un établissement de change.

L'intégrité et la sécurité du réseau sont assurées par le réseau lui-même, Au contraire, la sécurité et l'intégrité de chaque « *wallet* », ainsi que de l'application locale dans laquelle il peut être incorporé, sont la responsabilité de l'utilisateur local. Jusqu'à présent, toutes les fraudes et violations de sécurité ont concerné les applications locales, notamment les systèmes de change, et non le système Bitcoin proprement dit dont la robustesse a été amplement démontrée par les faits.

L'évolution de Bitcoin et des systèmes de paiement pair à pair

Pour former un pronostic sur l'avenir de Bitcoin, il faut prendre en compte les perspectives d'évolution du logiciel lui-même. On assiste en effet aujourd'hui à un tel foisonnement d'initiatives et de réalisations de logiciels annexes, de corrections, de perfectionnements et d'alternatives au système Bitcoin que le contexte même de l'évolution des monnaies alternatives va se modifier en permanence.

Ces développements sont favorisés par le principe du logiciel libre, où non seulement les logiciels sont gratuits et librement utilisables, mais où le code source est lui-même public et où chacun a droit de le modifier et de distribuer ces versions modifiées. Il existe donc autour de Bitcoin toute une population de développeurs volontaires et de testeurs volontaires qui identifient les problèmes et les opportunités d'extensions, imaginent des solutions et produisent des modifications et des extensions aux systèmes existants, voire des systèmes alternatifs entièrement nouveaux.

Cette activité est structurée par toute une discipline de développement et d'intégration de nouvelles fonctions et de nouvelles versions, portée par quelques sites spécialisés (le plus important étant *GitHub*) qui fournissent les outils nécessaires à la coordination et à l'intégration d'une multitude d'initiatives décentralisées et autonomes, y compris les échanges d'idées, les discussions préalables, la gestion des développements en cours sous leurs différentes versions, les tests et l'intégration des modifications, la publication des travaux en cours, et enfin la construction, la distribution et la maintenance des systèmes opérationnels.

Les objectifs

On peut distinguer dans ces développements plusieurs types d'objectifs.

Le premier est évidemment, comme pour tout logiciel, de résoudre les problèmes courants : éliminer les dysfonctionnements constatés, fermer les failles de sécurité résiduelles, améliorer la convivialité et les performances. A plus long terme, diminuer la consommation des ressources pour permettre de traiter un très grand nombre de transactions, de réduire les temps de réponse et d'accepter dans le réseau un très grand nombre de nœuds sans outrepasser les capacités physiques des ordinateurs (problème de la « *scalability* »).

Une deuxième voie consiste à ajouter au système existant, toujours sur le mode pair à pair, de nouvelles fonctions et de nouveaux services, jusqu'à égaler puis dépasser l'offre des établissements spécialisés conventionnels. Ces développements peuvent se contenter d'exploiter la forme ouverte des transactions en définissant de nouveaux « *scripts* » qui réalisent à l'intérieur de Bitcoin des services tels que les paiements conditionnels, le « *crowdfunding* », les comptes bloqués, etc. D'autres sont plus ambitieux et visent à ajouter de nouveaux types d'interactions financières comme des offres et des demandes, le crédit, le change, les contrats de toutes sortes, etc.

Une troisième voie part du constat que les technologies de construction d'un registre indélébile ne sont pas limitées aux transactions financières, mais peuvent s'étendre à d'autres classes d'information : textes de référence, contrats, titres de propriété, brevets, droits d'accès, rapports d'expertise, ouvrages littéraires, etc... Il s'agit alors de munir de fonctions applicatives propres à ces différentes classes d'informations un système par à pair qui utilise la technologie Bitcoin comme technologie d'enregistrement définitif inviolable. Ces applications peuvent soit être indépendantes, soit couplées avec un système de paiement. Dans ce dernier cas, le système pourra gérer à la fois des biens informationnels, leur transfert entre utilisateurs et sa contrepartie monétaire, c'est-à-dire leur commerce, ainsi que celui des biens ou services dont l'accès est commandé par une information, le tout étant enregistré dans la *blockchain*.

Les résultats de ces efforts peuvent prendre la forme habituelle d'une nouvelle version du logiciel de base (la version actuelle, après 5 ans d'existence, est la version 9), ou de logiciels annexes périphériques d'utilisation facultative, notamment pour les « *wallets* » et les serveurs légers. Plusieurs équipes indépendantes développent des extensions qui viennent s'ajouter au système Bitcoin pour former une surcouche capable de traiter des transactions complexes comme le change décentralisé entre monnaies virtuelles, l'épargne ou le crédit.

Les règles du logiciel libre autorisent tout utilisateur à reprendre les idées et les développements d'un autre et à les incorporer à ses propres produits. Il est donc probable que le système Bitcoin lui-même intégrera tout ou partie des développements annexes qui sont aujourd'hui vus comme ses concurrents. A l'inverse, ces mêmes règles autorisent l'apparition de quasi-clones utilisant le même logiciel où seuls quelques paramètres sont modifiés, notamment les paramètres qui gouvernent la gestion de l'unité de compte. Certaines de ces variantes peuvent coexister avec Bitcoin sur le même réseau pair à pair en utilisant la même *blockchain*, d'autres utilisant une *blockchain* distincte.

Enfin, l'offre de nouveaux services peut se traduire soit par une surcouche ajoutant des fonctions nouvelles sans toucher au système Bitcoin existant et en continuant à utiliser ses fonctions, soit par un système alternatif entièrement nouveau, même s'il reprend des concepts voire des parties de systèmes existants.

Dans la mesure où ces systèmes appliquent à leur unité de compte et aux transactions des principes de gestion différents, ils définissent autant de « monnaies » distinctes. On recense une grosse centaine de telles « cryptomonnaies », voire beaucoup plus selon certaines sources, mais dont l'immense majorité a échoué ou a été abandonnée, et dont le décompte exact est donc sans importance pratique. Le bitcoin est le leader incontesté avec plus de 95 % de la valeur cumulée et du nombre de transactions.

Quelques exemples

Litecoin, lancé début 2011, est un quasi-clone de Bitcoin qui offre exactement les mêmes fonctionnalités, avec quelques différences dans la discipline de création des unités, et en utilisant une autre méthode de protection de la *blockchain* moins gourmande en temps machine et pouvant de ce fait soutenir un plus grand volume de transactions en offrant un meilleur temps de réponse, donc mieux approprié aux transactions de faible montant. C'est le seul à atteindre une part de marché significative, loin néanmoins derrière Bitcoin.

Ripple, lancé en 2013 et encore en cours de développement, est aussi un système pair à pair, mais radicalement différent y compris par la forme et la méthode de protection du registre des transactions. Sa fonction principale reste le paiement, mais dans toutes les monnaies présentes et imaginables, y compris le change entre toutes ces monnaies. Pour cela, il intègre dans le réseau pair à pair des « *gateways* » (portails) qui assurent en particulier l'alimentation du système en unités monétaires, dont les monnaies nationales. Les « *gateways* » sont des sortes d'institutions financières automatisées, dont ils s'efforcent de transposer les règles de fonctionnement, y compris celles qui sont imposées par la réglementation bancaire, en s'appuyant sur une formalisation des relations de confiance entre utilisateurs.

Darkcoin, lancé début 2014 et encore en cours de développement, ajoute au logiciel Bitcoin la possibilité de rendre les transactions réellement anonymes en les mélangeant de façon indéchiffrable avec d'autres transactions et en les transmettant à travers un chemin aléatoire comme le fait déjà le système TOR. Il comporte aussi de nouveaux algorithmes de construction des blocs et de la *blockchain*.

Ethereum, en cours de développement, est un projet de restructuration globale du système permettant une extension de son domaine d'application à travers une généralisation de la notion de transaction et un nouveau système de gestion du registre. Il vise à constituer un environnement général pour tous les systèmes pair à pair, et la base pour toutes sortes de transactions et de contrats complexes dont le change, le crédit, les produits dérivés, ainsi que pour de nouvelles classes de documents autres que financiers. Il prévoit en outre le support d'« entreprises autonomes distribuées », des automates fonctionnant en mode pair à pair et capables de percevoir des redevances, de verser des rémunérations et de publier des comptes, résolvant ainsi le problème de la motivation des fournisseurs de service dans un système pair à pair.

Pris séparément, et au plan strictement technique avant même toute mise en concurrence, chacun de ces projets pourra réussir ou échouer, et vivre en tant que projet indépendant ou disparaître en voyant ses fonctions plus ou moins reprises par d'autres. Mais au niveau global des systèmes pair à pair, dont Bitcoin est le prototype et la réalisation dominante, tous les problèmes courants sont et seront identifiés en permanence et rapidement résolus, y compris les failles de sécurité résiduelles. Grâce à une communauté enthousiaste et active et aux règles du logiciel libre, les critiques d'aujourd'hui seront caduques demain, et de nombreuses améliorations, certaines très significatives et susceptibles d'applications dans des domaines fondamentaux de la société, se concrétiseront à court et moyen terme.

Dans l'analyse de la concurrence avec les systèmes traditionnels, la libre circulation des idées et des morceaux de code entre les différentes réalisations, qui est la marque du logiciel libre, autorise à traiter l'ensemble comme un tout, au sein duquel différents systèmes entretiennent des relations originales de compétition et d'enrichissement mutuel qui entraînent une extraordinaire réactivité et une créativité sans précédent. A la fois concurrent et complémentaire, chacun de ces systèmes est le banc d'essai d'améliorations qui profiteront à tous les autres.

Gérard Dréan

Gérard Dréan (http://gdrean.perso.sfr.fr/) *(X54) a fait carrière dans l'industrie informatique, puis s'est tourné vers la réflexion économique. Il est l'auteur d'un "**Abrégé de L'Action Humaine (http://www.amazon.fr/product-reviews/2251390375)** " de Ludwig von Mise, ainsi que du livre **"b.a.ba d'économie" (http://gdrean.perso.sfr.fr/baba.html)***

Commentaires

1. Le jeudi 17 juillet 2014, 02:32 par BitNoob

Merci pour ce bel article qui traite de Bitcoin et des monnaies décentralisées en général.

Je dois vous avouer que j'ai hâte de lire la suite.

Je me suis bien renseigné à propos de ce protocole et je pense assez bien comprendre son fonctionnement. Preuve de travail, chaine de bloc etc.

Cependant il me reste une zone d'ombre, je précise que je ne suis absolument pas codeur. Mais ce genre d'innovation me donne clairement envie de m'y mettre.

Bref, je me demande comment fonctionne en pratique le consensus autour des régles qui régissent Bitcoin.

Pour qu'une règle change, augmentation de la taille max d'une transaction, récompense allouée à un mineur pour l'écriture d'un bloc, ajustement de la difficulté etc, il faudrait que la majorité des clients change la règle?

Si je change une règle tout seul dans mon coin, mes transactions farfelues seront rejetés par les autres noeuds. Si la majorité des noeuds (mineurs inclus) changent une règle alors ce changement sera effectif car appuyé par plus de la moitié de la puissance de calul. Qu'advient-il des clients non à jour? ils deviennent aveugles et les mineurs bredouilles?

J'espère que je fournis la réponse à ma propre question

2. Le jeudi 17 juillet 2014, 04:12 par BitNoob

Sinon en ce qui concerne des concepts que je rêverai de voir abordés en français par des libéraux, je pense :
- aux smart contrats
- à la smart property
Excellent site, proposant un ebook gratuit sur le sujet http://www.ofnumbers.com/the-guide/ (http://www.ofnumbers.com/the-guide/)

Sinon dans les projets diablement ambitieux autour des monnaies décentralisées je me permets de rajouter en plus de ceux que vous avez déjà cité :

- Counterparty : https://www.counterparty.co/ (https://www.counterparty.co/) et http://www.blockscan.com/ (http://www.blockscan.com/)
- Bitshares : http://bitshares.org/ (http://bitshares.org/)
- Next : http://www.nxtcommunity.org/ (http://www.nxtcommunity.org/)
- Maidsafe : http://maidsafe.net/ (http://maidsafe.net/)
- Storj : http://storj.io/ (http://storj.io/)
- Open Bazaar : https://openbazaar.org/ (https://openbazaar.org/) pour une petite présentation http://coinbrief.net/bitcoin-openba... (http://coinbrief.net/bitcoin-openbazaar/)
- Dark wallet : https://github.com/darkwallet/darkw... (https://github.com/darkwallet/darkwallet) et http://coinbrief.net/dark-wallet-al... (http://coinbrief.net/dark-wallet-alpha-5-release/)

3. Le jeudi 17 juillet 2014, 19:54 par Gérard Dréan

Merci de vos réactions

Sur votre question : j'en parle (rapidement) dans la deuxième partie, mais voici une présentation plus complète.
Généralement, les noeuds qui restent sur la version N du logiciel ne reconnaissent pas les blocs construits par des mineurs qui sont passés à la version N+1, et donc ne les ajoutent pas à leur blockchain. Mais ils continuent à accepter et à ajouter à leur

blockchain les blocs valides construits par le mineurs qui sont eux aussi restés à la version N. Il y a donc division des noeuds en deux populations qui utilisent deux blockchains différentes, les noeuds de chaque population pouvant communiquer et échanger entre eux, mais généralement pas avec ceux de l'autre.
A chaque fois qu'un noeud bascule de la version N à la version N+1 du logiciel, le protocole de construction de la blockchain reconstruit dans ce noeud la branche nouvelle de la blockchain et la substitue à la branche ancienne. Ce basculement est aidé par le fait que chaque noeud conserve dans une branche secondaire de la blockchain tous les blocs bien formés qu'il a reçus, y compris des mineurs de l'autre population, mais sans vérifier les transactions qu'ils contiennent,
La réalité est un tout petit peu plus compliquée à cause des cas particuliers, mais ça devrait répondre à votre question.

Merci pour les références supplémentaires. Je n'ai bien entendu pas cherché à être exhaustif, mais à donner une idée des développements les plus significatifs des principales tendances.

4. Le samedi 19 juillet 2014, 11:34 par Jo.Pizzo

Bonjour Monsieur Dréan,

J'ai eu à maintes reprises l'occasion d'écouter vos conférences dans le cadre de l'Institut Turgot et j'ai apprécié la clarté de vos exposés mais là, concernant "Bitcoin", j'ai toujours beaucoup de mal à en comprendre le fonctionnement pratique et ce, depuis le premier exposé de Philippe Herlin qui a fait connaître " l'économie " du Bitcoin.
Ainsi, pratiquement, comment les choses se passent si, je veux régler en bitcoin; à mon libraire, lui-même " connecté au système Bitcoin" , pour l'achat d'un livre de 23 Euros ?

Soyez assuré, cher Monsieur, que votre réponse intéressera une grande quantité de personnes et c'est ainsi que s'effectuera la promotion de cette monnaie " complémentaire" si ceci est la bonne expression.
Sentiments cordiaux.
J.Pizzo

5. Le samedi 19 juillet 2014, 13:25 par Gérard Dréan

@Jo Pizzo
En l'état actuel des choses, il faut évidemment que vous ayez téléchargé et installé un "wallet" de votre choix et que vous ayez créé un "compte", puis que vous vous soyez procuré au moins 0.05 bitcoin, puisque au moment où je vous réponds, 23€ c'est 0.0497 btc. Vous pouvez l'avoir fait soit en minant, mais il faudra sans doute vous être inscrit dans une coopérative minière et y avoir consacré pas mal de temps machine, soit avoir changé des euros en btc sur un site spécialisé, dont une liste figure ici : http://bitcoincharts.com/markets/cu... (http://bitcoincharts.com/markets/currency/EUR.html)
mais ça va sans doute vous prendre des jours pour obtenir les autorisations.
Ou vous avez pu vendre quelque chose à quelqu'un qui a bien voulu vous payer en bitcoins, ou enfin vous avez pu les gagner aux loteries en bitcoins qui existent.
Il faut maintenant que vous conveniez avec votre libraire de l'équivalent de 23€ en btc, puisque je ne pense pas qu'il aura déjà un tarif en btc. Avec de la chance, il consultera le site Bitcoin charts et utilisera la taux de change du jour, qui aura probablement changé depuis aujourd'hui.
Le reste est tout simple: si vous avez un "walllet" sur smartphone, vous flashez le QR code du libraire, vous entrez le nombre de btc convenu et vous cliquez.
Tout ça vous paraît bien lourd ? C'est précisément pour ça qu'il y a tant de projets qui visent à offrir le change immédiat : vous permettre, dès que vous avez installé votre "wallet", de taper 23€ et que le système pair à pair se charge du reste. Mais c'est bien loin d'être simple à réaliser.
J'aborde cette question dans la deuxième partie.