Monnaies virtuelles
Le cas Bitcoin : Paradoxes et processus d'une crypto-monnaie

Voici la première partie de cet article consacré aux bitcoins. La seconde partie, qui paraîtra dans le prochain numéro, traitera des risques et rapports à la cybercriminalité et au blanchiment.

Avec l'essor d'internet comme vecteur d'échanges et la croissance des activités de commerce électronique, le concept de monnaie virtuelle s'est développé, au point de vouloir s'imposer comme substitut aux monnaies classiques et électroniques. Dans un contexte de défiance envers le système monétaire traditionnel et pensant à la protection de leurs données nominatives bancaires, les internautes sont tentés d'y recourir, ce qui n'est pas sans risque non plus. Parmi les monnaies virtuelles, le Bitcoin est vu comme la plus répandue dans la sphère internet au point d'être accepté par certains acteurs du monde réel en permettant sa convertibilité. Fondé sur des protocoles et une architecture crypto-informatique complexes, il souffre toutefois d'incertitudes et de dérives, comme tout système naissant.

L'auteur se propose d'évoquer le besoin de confiance et de stabilité face aux crises contemporaines, puis les monnaies sous leurs différentes formes, avant d'aborder le statut juridique du Bitcoin, ses principes et son fonctionnement, pour en indiquer les paradoxes et en mesurer la portée dans un espace d'échanges ouverts à tous, y compris à la cybercriminalité et au crime organisé. Dans une seconde publication, il montrera les enjeux et les risques en l'absence de régulation et de garanties, et les besoins en matière de sécurité et d'encadrement, pour tenter de conclure.

CONFIANCE ET STABILITÉ DES MONNAIES ET CRISES CONTEMPORAINES

De l'étalon or aux monnaies fiduciaires

La confiance en la majorité des monnaies reposait sur l'étalon or pour développer le commerce international. La Première Guerre mondiale puis la crise de 1929 ont réduit la capacité des États, dont la balance commerciale était fortement déficitaire, à maintenir les réserves d'or nécessaires à la création de monnaies. L'or était alors exporté à l'étranger, comme ce qui fut le cas pour les États-Unis. Les accords de Bretton Woods[1] de 1944 ont permis la mise en place d'un système où le dollar prenait une dimension internationale en restant la seule monnaie convertible en or. En contrepartie de leur émission, les autres monnaies devenaient convertibles en dollars en remplacement de l'or. C'est en 1971 que les États-Unis ont suspendu la convertibilité du dollar avec l'or, en particulier pour leur permettre de financer la guerre du Vietnam.

En présence d'un système monétaire international largement fiduciaire, les besoins de plus en plus importants de l'économie mondiale à disposer de dollars ont paradoxalement contribué à une perte de confiance en cette monnaie, invitant à une réforme du système monétaire. À ceci s'est ajouté le flottement des monnaies[2] qui a introduit un risque nouveau au vu de produits financiers complexes, comme les produits dérivés et les fonds spéculatifs, capables d'engendrer une crise systémique. Les prémisses sont visibles dans la crise monétaire et bancaire, depuis 2007, avec le spectre d'une grave dépression et face à cela, le besoin d'une régulation mondiale effective.

De la stabilité par des réformes

La crise financière mondiale amorcée en 2007 a pour origine le dégonflement de bulles de prix, avec des pertes importantes des établissements financiers provoquées par la crise des «subprimes». Elle est associée à une crise de liquidité, voire de solvabilité, tant au niveau des banques que des États, entraînant une raréfaction du crédit aux entreprises et un frein à l'investissement. La crise financière de l'automne 2008 qui s'ensuit provoque la chute des cours des marchés boursiers et la faillite d'établissements financiers. Pour éviter une crise systémique, les États ont dû intervenir, provoquant un creusement de leur dette publique et parfois même une autre crise, comme en Islande et en Irlande, et une récession et un recul du produit intérieur brut mondial dès 2009. Si aujourd'hui les États-Unis sont toujours au cœur du système, la périphérie est occupée par les pays asiatiques, notamment la Chine, avec des taux de change volontairement sous-évalués permettant la croissance par l'exportation, mais au détriment de la demande intérieure.
Tandis que la variation des cours monétaires et l'effondrement des marchés boursiers sont au cœur des

crises, l'enjeu relève de l'organisation d'un environnement mondial efficace stable. Ceci devrait conduire à de profondes réformes de la part des États[3] et à la mise en place de règles à respecter par les institutions financières et monétaires. Le but est d'éviter les conséquences économiques et sociales de nouvelles crises qui ne manqueront pas d'apparaître sans cela.

STATUT DES MONNAIES ET DU BITCOIN EN PARTICULIER

La monnaie et ses caractéristiques

Si le développement des nouvelles technologies a pu laisser penser à la disparition de la monnaie[4], celle-ci est pourtant répandue partout, comme le pressentait R. Libchaber en 1998. Malgré tout, elle reste dépourvue de définition juridique claire. D'un côté, les juristes s'attachent aux droits et obligations qu'entraîne son usage pour caractériser ce qui est ou non une monnaie[5] ; considérant que si une monnaie est un moyen de paiement, la réciproque n'est pas nécessairement vraie. De l'autre, les économistes s'orientent vers les fonctions monétaires et leurs effets pour la définir en distinguant l'unité de compte[6] mesurant la valeur d'un bien quelconque, le moyen de paiement permettant d'acquérir ce bien, et la réserve de valeur pouvant être conservée pour être échangeable à tout moment.

Parmi la masse monétaire[7], il faut distinguer les différentes formes de monnaie : fiduciaire[8] : espèces papier et métalliques, scripturale, pour plus de 90 % de la monnaie en circulation : chèque, titre interbancaire de paiement (TIP), carte de paiement ou de crédit, dépôt sur un compte bancaire matérialisé par une écriture[9], électronique : chargée dans un portemonnaie électronique, et plus récemment virtuelle, comme c'est le cas de Bitcoin.

La monnaie sous ses formes traditionnelles

La monnaie fiduciaire repose sur la garantie de l'institution financière centralisatrice qui l'émet. Cette forme s'est généralisée et son cours dépend de la confiance[10] qui lui est accordée en tant que moyen ayant force légale[11] d'échange et de paiement. Elle s'inscrit dans un ensemble où les différentes formes de monnaies[12] répondent à des règles strictes définies par la loi[13].

La monnaie scripturale repose sur les dépôts bancaires[14] opérés sur les comptes courants. Elle est matérialisée par une écriture en compte géré par informatique. Elle circule par des transferts entre comptes par divers moyens, comme les cartes de paiement, les virements ou les chèques. Elle fournit aux banques l'essentiel des ressources affectées aux prêts et peut être transformée en monnaie fiduciaire : billets ou pièces ou chargée dans un portefeuille électronique.

Le virement électronique assure à son tour la circulation à grande vitesse des monnaies à travers le monde, permettant les transactions de placement ou d'achat au service de la mondialisation. En revanche, parce qu'elle ne bénéficie pas de la même force légale que la monnaie fiduciaire, elle peut se voir refusée par un créancier ou en tant que moyen de paiement.

La monnaie sous ses formes nouvelles

La monnaie électronique repose sur des unités électroniques d'un émetteur enregistrées dans un portefeuille électronique d'un porteur ; en général, une carte à microcircuit. Elle représente un système de paiement composé d'un émetteur[15], de porteurs-consommateurs et d'un réseau de commerçants. Lorsque le porteur transfère les unités électroniques de sa carte vers le vendeur, l'opération n'engendre aucun mouvement sur les comptes bancaires respectifs de ces derniers. Les mouvements ont lieu lorsque l'émetteur convertit ces unités, ou lors du transfert par virement bancaire sur le compte du vendeur ou de l'achat d'unités par le porteur. Il s'agit de savoir si ce nouveau moyen de paiement constitue une nouvelle forme juridique de monnaie.

Si la monnaie électronique était une nouvelle forme juridique de monnaie, elle devrait réunir des fonctions particulières nouvelles d'unité de compte, d'incorporation dans un instrument monétaire, et d'utilisation comme moyen de paiement. Si la logique de son système de paiement présente plusieurs originalités par rapport aux solutions classiques, l'unité de compte légale est la même : euro, dollar, etc., et la monnaie électronique n'a pas une valeur autonome, indépendamment de la valeur de la créance sur une somme qu'elle représente. D'un point de vue juridique, chaque unité électronique est un titre de créance incorporé dans un instrument électronique accepté comme un moyen de paiement dont le succès dépend largement de la confiance des utilisateurs et de la surveillance prudentielle[16].

La monnaie électronique n'est donc pas une nouvelle forme de monnaie, mais seulement un titre de créance et un instrument d'une nature juridique particulière, créé comme tel et non par la dématérialisation d'une forme antérieure sur support papier.

On notera que ces divers moyens de paiement fiduciaires, scripturaux et électroniques ne sont pas uniformes, ni par leur nature, ni par leur régime

Les différentes formes de monnaie

Fiduciaire Scripturale Electronique Virtuelle

juridique et que la définition d'une monnaie ne peut se réduire à la seule fonction représentant une unité de compte[17] : euro, Bitcoin, etc. Elle nécessite[18] aussi une fonction d'échange incorporée dans un instrument monétaire pour être utilisée à tout moment : billets de banque[19], pièces métalliques et monnaie scripturale, et une fonction de circulation par des moyens de paiement qui facilitent les transactions commerciales et servent à transférer des fonds, par tradition ou par des écritures en compte : billets de banque, chèques, cartes bancaires, virements.

Le statut du Bitcoin en tant que monnaie

Le Bitcoin a été créé en 2009 par Satoshi Nakamoto[20], pour remplir les trois fonctions essentielles attachées à une monnaie : l'enregistrement d'une unité de compte virtuelle sur support numérique, la conservation d'une valeur pour être utilisé à tout moment, et la facilitation des transactions commerciales. Sous cet angle, le Bitcoin aurait l'apparence d'une monnaie. Pourtant, il ne peut être qualifié de monnaie ayant cours légal puisqu'il est possible de le refuser en paiement sans contrevenir aux dispositions de l'Art. R642-3 du CP. Par ailleurs, si sa mise en circulation ne viole pas le monopole d'émission de monnaies ayant cours légal par les banques centrales, il ne répond pas à la définition de la monnaie électronique au sens du code monétaire et financier[21] et n'est pas émis contre une remise de fonds[22]. Enfin, contrairement à la monnaie électronique, le Bitcoin ne dispose pas de garantie légale de remboursement à sa valeur nominale[23].

Du point de vue de son statut, le Bitcoin est une monnaie virtuelle, différente de la monnaie électronique, sans garantie et sans cours légal. Dépourvu de cadre réglementaire et de statut légal il ne serait donc pas une monnaie au sens de la loi.

En France, les activités relevant des monnaies virtuelles et notamment de Bitcoin sont soumises à un agrément. Celui-ci est uniquement délivré par la Banque de France et l'ACPR[24] et exclusivement réservé aux prestataires de services de paiement, faute d'agir dans l'illégalité[25]. D'autres pays n'ont pas autant de prudence, comme l'Allemagne, le Luxembourg et notamment États-Unis, qui ont choisi de fournir des licences Bitcoin pour permettre aux entreprises de se développer. En revanche, les transactions en Bitcoins sont interdites en Russie et en Chine.

Pour que Bitcoin, - fondé sur la crypto-technologie pour exercer un contrôle différent sans autorité centrale et de façon anonyme - puisse être un véritable modèle alternatif crédible au service de l'économie numérique, il lui faut démontrer qu'il est le mieux adapté à la nouvelle économie et qu'il présente les propriétés de sécurité, de fiabilité, de stabilité, de légalité et d'éthique. Ceci sous-tend qu'il ne soit pas seulement une aubaine pour certains et pour d'autres, un moyen d'évasion fiscale ou favorable aux vocations criminelles. Il faudra donc s'interroger sur les potentialités offertes par Bitcoin aux cybercriminels[26] et au crime organisé et sur les moyens pour y faire face.

Premier paradoxe relevant du système Bitcoin

La création d'un tel système ex nihilo, déconnecté de l'économie, n'est ni sans paradoxes, ni sans effets. Le risque juridique lié à un statut de monnaie non régulée ne peut être ignoré, du fait de son potentiel d'usage dans le cadre de circuits illicites et criminels, même s'il n'a pas été créé dans cette attention ; à l'opposé d'être un outil transactionnel dans le cadre de circuits légaux. Non sans noter que des billets de banque sont aussi vus en quantité dans nombre d'affaires criminelles, le Bitcoin apparaît néanmoins comme un moyen de paiement répandu pour les échanges liés à des activités de marché noir ou criminelles (ex. extorsion de fonds, chantage, demandes de rançon, achats illicites, etc.), pour des motifs qui tiennent à l'anonymat, à la distance et à l'extraterritorialité[27], pour tenter d'échapper aux poursuites.

Si des solutions de paiement en ligne se développent en marge du système bancaire (ex. PayPal), l'introduction de monnaies virtuelles comme le Bitcoin relève d'un moyen beaucoup plus radical. Le Bitcoin a aussi quelques raisons d'inquiéter les banques sur le marché du crédit. L'une d'elles est liée au crédit participatif ou «crowdfunding» qui vient se substituer aux prêts bancaires en direction des entreprises. L'emprunt direct auprès des détenteurs de Bitcoins se fait par la mise en relation de prêteurs et d'emprunteurs disséminés dans le monde entier, au travers d'une plateforme dédiée. Pour les prêteurs, si les taux sont plus attractifs que ceux des marchés, leur investissement présente un risque de défaillance de l'emprunteur[28] auquel s'ajoute un risque de change lié à une évolution défavorable du cours du Bitcoin.

Si les activités du réseau Bitcoin sont associées à l'achat et à la vente de biens ou de services, elles relèvent aussi de «trading» par le biais de plateformes spécialisées. Il est maintenant proposé des options binaires par des courtiers : si l'évolution du cours du Bitcoin est favorable à l'acheteur, ce dernier perçoit la valeur du sous-jacent augmentée d'une fraction de l'écart constaté avec le cours et dans le cas contraire, il perd le capital investi. Il est aussi possible d'acheter des contrats sur différence ou CFD[29]. Dans ce cas, le dépôt d'un faible montant engage un volume important de contrats, ce qui peut générer un profit important ou des pertes substantielles qu'il faudra financer en cas d'anticipation erronée. Dans ces conditions, l'origine des fonds est difficile à déterminer du fait de flux engendrés et de l'opacité des mouvements financiers sans réel contrôle. D'abord vu comme moyen de paiement, le Bitcoin s'introduit visiblement aussi dans le monde de la finance. En France, la plateforme Bitcoin Central bénéficie d un accord avec le prestataire de services Aqoba pour permettre des opérations[30] sur des comptes de paiement en unités Bitcoins[31].

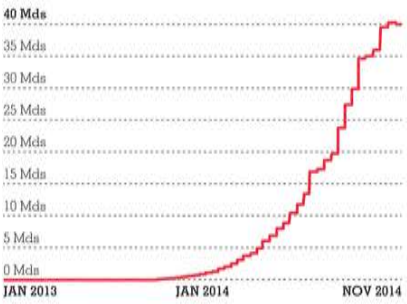
Le paradoxe est d'abord lié à la présence de Bitcoins dans des produits financiers sophistiqués qui ne sont en fait que des répliques de ceux déjà utilisés et fondés sur des

monnaies légales et ensuite, au fait que la communauté Bitcoin, après avoir cherché à s'écarter du système bancaire et monétaire traditionnel et de la réglementation, a maintenant besoin des banques et d'une certaine régulation, pour apparaître plus sûr et largement admis[32].

Second paradoxe relevant du système Bitcoin

Pour créer de nouveaux Bitcoins, les utilisateurs doivent générer un code dont la taille augmente, ce qui nécessite des opérations dont le nombre est drastiquement croissant. Au fur et à mesure de ce «mining», les moyens informatiques à mettre en œuvre deviennent de plus en plus importants, au point d'être gigantesques, ceci jusqu'à la limite prévue de 21 millions de Bitcoins.
Pour l'ensemble des moyens et activités au niveau mondial, il est observé une difficulté en forte croissance d'une année sur l'autre, de l'ordre de 40 milliards fin 2014 contre 900 millions une année auparavant, comme suit :

Mesure de la difficulté
(Données : blockchain.info)



Cette asymétrie rend le système inégalitaire. Elle favorise clairement, d'abord les créateurs et les premiers adeptes, lesquels pouvaient créer des Bitcoins avec très peu de puissance informatique, et ensuite ceux qui seraient à même de dépenser de plus en plus pour finalement ne créer que quelques Bitcoins ! Ce principe devrait induire la rareté de mise en circulation avec pour conséquence l'augmentation de la valeur des Bitcoins, qui seraient stockés plutôt que d'être dépensés, avec pour effet de renforcer cette rareté jusqu'à empêcher les échanges et rendre la devise inutile. C'est aussi une des raisons de la fluctuation de la valeur du Bitcoin et un risque important en cas de ventes massives. Cette inégalité est démontrée par les faits. Un petit groupe de privilégiés, dont les créateurs, possèdent suffisamment de Bitcoins pour contrôler l'intégralité du système. Selon D. Ron et A. Shamir (2013), au niveau mondial, si 97% des comptes ne possèdent pas plus de 10 Bitcoins, 78 comptes en détiennent plus de 10 000.

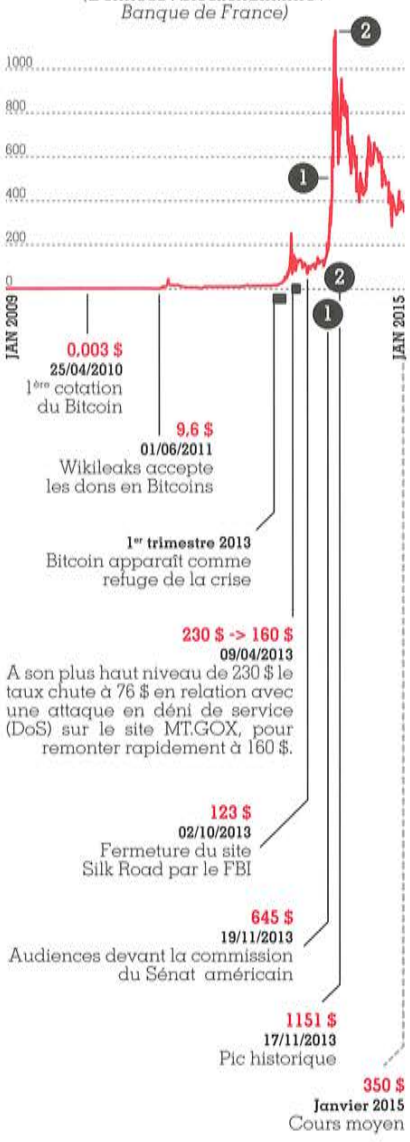
Par ailleurs, des transactions importantes relèveraient du compte de Satoshi Nakamoto, le créateur déclaré du système, lequel disposerait de près 980 000 Bitcoins, soit plus de 330 millions d'Euros au 12/12/14.

Enfin, l'étude des distributions montre que la plupart des Bitcoins restent dormants au regard d'adresses qui n'ont jamais participé à la moindre transaction. De plus, certaines d'entre elles pourraient être liées au masquage de l'existence de transactions et des relations entre elles.
Le paradoxe est lié à cette asymétrie, dont le principe même entraîne les inégalités, contrairement à l'intention initiale de servir l'économie numérique, du fait de sa détention par peu de personnes qui accumulent et concentre des richesses, à l'opposé des valeurs d'une monnaie virtuelle circulante qui serait à même de contribuer à l'économie en finançant l'innovation et en valorisant des activités mal rémunérées. Bitcoin se présentait comme une alternative au monopole bancaire et le voilà en réalité empreint d'une mainmise par ses créateurs !

Caractère spéculatif du système Bitcoin

La forte volatilité du taux de change du Bitcoin offre une opportunité de gains ou entraîne un risque de pertes, par une activité financière spéculative.
Cette dernière reste cependant marginale par rapport aux autres, tout en suscitant le développement de produits et d'instruments financiers à fort effet de levier en misant sur des écarts anormaux. Ceci se traduit par de forts gains ou de fortes pertes[33], au vu du graphe de l'historique des variations de taux de change, depuis sa création jusqu'à fin 2014.

Cours du Bitcoin en dollars
(Données : blockchain.info / Banque de France)



Si, comme les monnaies classiques, les variations de cours du Bitcoin sont liées à des événements généraux, parce qu'il peut être considéré comme un refuge temporaire, d'autres sont propres à son écosystème et notamment aux décisions prises par les États à son égard. Pourtant, si dans le cas de krachs boursiers, il est facile de déterminer la cause de fortes variations, la nature du protocole Bitcoin ne facilite pas le diagnostic, pas plus que la détection d'une tentative de manipulation du cours, piste qu'il serait quasiment impossible de valider.

De telles variations apparaissent de façon détaillée sur l'année 2014, avec des périodes de tendances haussières et baissières et notamment une certaine persistance à la baisse au second semestre.

Fluctuation du marché en dollars
(Données : blockchain.info & évenements)

1. **15/01/2014** Le sénat français organise une audition sur les enjeux liés aux monnaies virtuelles de type Bitcoin
2. **06/02/2014** Bitcoin déclaré illégal en Russie après la Chine fin 2013
3. **11/02/2014** Le réseau Bitcoin est victime d'une attaque massive sur de nombreuses plate-formes de change
4. **16/02/2014** Le sénateur américain J. Manchin demande l'interdiction du Bitcoin aux États-Unis, en raison de sa volatilité et des risques d'utilisation à des fins illégales, notamment pour du blanchiment
5. **24/02/2014** La plate-forme d'échange MT.GOX subit une perte record de 744 408 Bitcoins, (équivalent à 250 millions d'euros). Le site en situation de crise ferme temporairement. Le Bitcoin perd plus de 38 % de sa valeur au 1TR 2014
6. **13/05/2014** Ouverture de la «Maison du Bitcoin» à Paris

BITCOIN : SYSTÈME DE CRYPTO-MONNAIE INFORMATIQUE

Le Bitcoin est un système de crypto-monnaie informatique décentralisé[34]. En fonctionnant en réseau pair-à-pair sur internet de façon totalement distribuée, la gestion est répartie sur l'ensemble des nœuds du réseau Bitcoin, pour ne pas dépendre de la résilience d'un seul émetteur ou d'une autorité centrale, mais seulement de la robustesse des mécanismes et algorithmes cryptographiques employés et de la sécurité de chacun. En l'absence d'infrastructure centralisée, la tenue des comptes et de leurs montants et l'assurance des transactions sont attribuées à un ordinateur différent présent sur le réseau Bitcoin. Celui-ci est choisi de façon aléatoire toutes les dix minutes afin que personne ne puisse contrôler ce réseau.

Le "mining" qui lui est associé est nécessaire d'une part, pour la création de Bitcoins et d'autre part, pour la confirmation des transactions. Les Bitcoins possédés par les utilisateurs sont stockés dans des portefeuilles électroniques ("electronic wallets"). Chaque portefeuille Bitcoin est un fichier lié à une adresse Bitcoin, généré de façon unique par un logiciel client.

Principes informatiques et cryptographiques sous-jacents

Le système Bitcoin exerce un pouvoir de transformation et de gestion de sa masse monétaire. Il permet ainsi des transactions pour le paiement d'un bien ou d'un service dont le prix est exprimé en Bitcoins sans intermédiaire bancaire, lesquels peuvent être échangés contre des devises (ex. euros) en passant par un bureau de change en ligne ou par un distributeur automatique.

Les Bitcoins circulent d'une adresse Bitcoin à une autre par un message de transaction signé numériquement. Lors d'une transaction[35], l'authenticité du payeur et la disponibilité des fonds sont d'abord vérifiés. Dès lors que la chaîne de signatures authentiques permet de remonter le montant de la transaction[36], celle-ci sera répertoriée dans la "blockchain", une base de données apparentée à un "registre comptable" public dont la taille est croissante[37]. Chaque ajout relève d'un nouveau bloc lié à une signature basée sur son précédent, de façon à garantir l'ordre chronologique des transactions en toute neutralité[38]. Il a par ailleurs été montré que l'interopérabilité entre des blockchains multiples est d'ores et déjà possible par des chaînes latérales[39] greffées, sans difficulté technique et économique, pour éviter des pénuries de liquidité et les fluctuations du marché liées aux techno-devises.

La cryptographie et l'informatique ont un rôle crucial. La cryptographie est utilisée pour permettre l'authentification et la non-répudiation déjà décrites, grâce à la signature des transactions et aux fonctions de hachage. La crypto-sécurité[40] du système est fondée sur l'algorithme ECDSA[41] qui assure la génération des clés appariées, publique et privée, ainsi que la vérification des transactions en s'appliquant sur le condensé - généré par une fonction de hachage irréversible (ex. SHA-256 sur 256 bits) - de chaque message et adresse Bitcoin dérivés[42]. Vu leur taille[43], c'est le microordinateur sinon un autre objet numérique de l'utilisateur qui mémorise ces données. La preuve de propriété d'un Bitcoin repose sur la connaissance de la clé privée et de la sécurité de celle-ci. Lors de la production de Bitcoins, les machines volontaires du réseau participent au "mining" et doivent pour cela résoudre un bloc de calcul avec la preuve également basée sur de telles fonctions cryptographiques.

Cependant, le système n'assure pas la confidentialité des données transmises sur le réseau. Toutes les transactions sont en clair, et l'anonymat n'est protégé que par le fait que le logiciel n'utilise aucune donnée personnelle de l'utilisateur. Par conséquent, l'identité d'un utilisateur peut être dévoilée si son adresse IP est traçable ou révélée suite à une analyse méthodique de la base de données des transactions blockchain.

Les principaux fichiers concernent les portefeuilles, les options de configuration, les blocs actuels concaténés et indexés, les adresses IP pour faciliter la connexion au réseau Bitcoin, ainsi que des informations pour la reconnaissance des pairs. Les fichiers les plus critiques wallet.dat[44] relèvent des portefeuilles ("wallets") et des clés cryptographiques associés aux Bitcoins possédés. Leur disparition ou leur corruption se traduirait par la perte définitive de ces Bitcoins.

Par défaut, les portefeuilles sont enregistrés sous forme chiffrée par l'algorithme AES (Advanced Encryption Standard) à l'aide d'un premier mot de passe utilisateur[45]. Une seconde phase est nécessaire de façon à chiffrer les clés privées, si la mention "double encryption" est indiquée. Le portefeuille dispose alors d'un condensé SHA 256 pour vérifier la validité du second mot de passe.

Processus de production de Bitcoins

La production de Bitcoins relève de participants, dénommés "mineurs", qui se livrent au "mining" en ayant recours à des moyens informatiques pour réaliser des calculs mathématiques de plus en plus exigeants en efficacité et ouverts à la concurrence de ces mineurs.

Pour que les opérations soient rentables, les profits devront être supérieurs aux dépenses résultant des investissements informatiques et en énergie. Or au fur et à mesure de la production, les premiers calculs ont exigé les moyens ordinaires du processeur d'unité centrale (CPU), puis la puissance de calcul des cartes graphiques (GPU) et celle de plusieurs cartes électroniques composées de plusieurs circuits logiques programmables pouvant atteindre chacune jusqu'à 750 MégaHashs/s. Aujourd'hui, les mineurs en concurrence seront maintenant amenés à utiliser la technologie ASIC pour former des "extracteurs" avec des modules près de 10 000 fois plus efficaces[46], s'ils veulent augmenter leur chance de succès devant le nombre de tentatives. Pour cette raison, en 2013 sont apparues de véritables "fermes" spécialement équipées en ASIC[47] pour ces opérations pour générer une puissance de calcul encore 7 000 fois supérieure[48]. Étant donné que la solution tient du hasard, sans des investissements importants ou un contrat de services, y compris en mode cloud, avec une société spécialisée dans le "mining" ou encore, la coopération entre mineurs pour mettre leurs moyens en "pools", il peut s'écouler jusqu'à des mois voire des années sans aucun gain. Cette puissance de calcul s'accompagne aussi de demandes très importantes en énergie, pour l'alimentation et le refroidissement, peu respectueuses de l'environnement.

L'investissement des mineurs n'étant pas garanti en retour[49], cette activité n'est attractive que pour les plus tenaces. En effet, si la production de Bitcoins est limitée et plutôt stable, du fait de la difficulté croissante déjà soulignée, cette dernière augmente aussi en fonction du nombre de mineurs en concurrence, là encore, la somme à se partager chaque mois se dilue dans ce nombre, tandis que la valeur même du Bitcoin fluctue.

Processus de transaction en Bitcoins

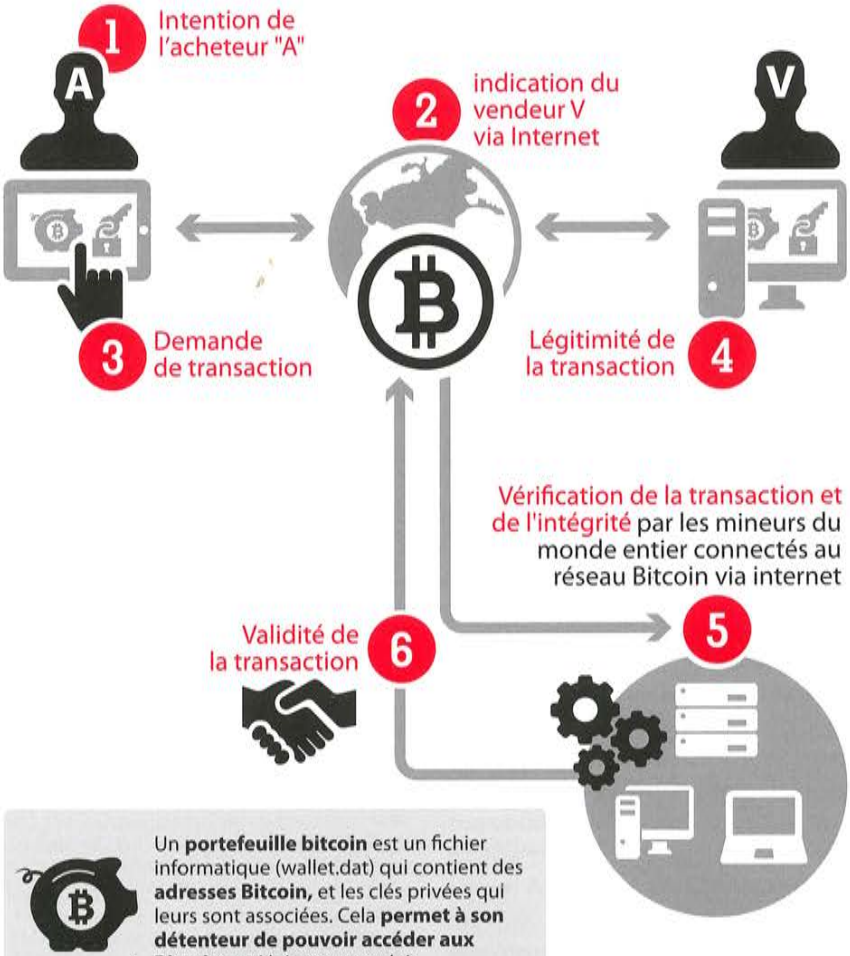
Lorsqu'un objet numérique, microordinateur ou dispositif mobile, cherche à se connecter au réseau Bitcoin, il lui faut d'abord trouver l'un ou l'autre pair connecté. Il a recours à une liste d'adresses internet IP statiques intégrées au logiciel Bitcoin dont il est équipé. Lorsque la base de données de l'ensemble des transactions effectuées depuis le début, connue sous le nom de "blockchain", est téléchargée, le logiciel entre dans sa phase transactionnelle. Il communique en continu avec d'autres objets du réseau Bitcoin, avec lesquels il échange des informations sur les adresses IP de ce réseau et sur les transactions qui apparaissant au fur et à mesure des échanges de Bitcoins.

Pour transmettre des Bitcoins, le dispositif utilisé doit signer la transaction correspondante faisant référence en entrée à une transaction précédente dont le montant de sortie est suffisant.

La clé privée doit correspondre à la clé publique avec laquelle a été créée l'adresse Bitcoin en sortie de cette transaction précédente. Il doit pour cela disposer de ses clés privées maintenues localement en toute sécurité enregistrées dans un fichier wallet.dat. Ce fichier confidentiel doit être conservé et sauvegardé en toute sécurité par l'utilisateur.

Principe de Bitcoin

L'acheteur (A) achète des **biens ou des services** via internet à un **vendeur (V)** qui accepte les Bitcoins. Tous deux sont **membres du réseau Bitcoin** et disposent d'un logiciel «client» et d'un **portefeuille Bitcoin** enregistré sur leur ordinateur, tablette ou smartphone.



Un **portefeuille bitcoin** est un fichier informatique (wallet.dat) qui contient des **adresses Bitcoin,** et les clés privées qui leurs sont associées. Cela **permet à son détenteur de pouvoir accéder aux Bitcoins** qui lui sont rattachés.

Une **paire de clés** : publique et privée, **en usage unique** est en mesure de **mieux préserver la sécurité et l'anonymat.**

LÉGENDE DÉTAILLÉE EN PAGE 63

La perte de ce fichier entraînerait la perte définitive des Bitcoins correspondants, restant dans la blockchain sans pouvoir changer d'adresse et donc sans jamais pouvoir être utilisés.

Quand il est connecté à un nœud, ce dernier reçoit une nouvelle transaction, il la valide localement au vu des transactions antérieures, l'enregistre dans le lot des transactions en attente, puis la transmet aux nœuds voisins qui réalisent le même traitement. L'opération se reproduit de proche en proche, jusqu'à ce que tous les nœuds soient informés de cette transaction.

Pour être validée, cette dernière devra pouvoir être intégrée à la blockchain, formée de la suite des blocs de transactions. L'incorporation de ce bloc de transactions nécessitera cependant une validation globale.

Dans un premier temps, certains nœuds du réseau associés aux mineurs tentent de construire chacun un nouveau bloc en regroupant des transactions récentes prises dans le lot des transactions en attente[50], en vérifiant la validité de chacune, en ajoutant des données tel que d'horodatage et en rendant l'ensemble vérifiable par l'ajout d'un condensé qui servira d'identificateur unique du bloc, — calculé par une fonction cryptographique irréversible de hachage (ex. SHA-256) —.

Quand un mineur est arrivé à construire un bloc valide dans cet intervalle, il le diffuse aux nœuds du réseau et pour ce service, il sera rémunéré par l'attribution de Bitcoins[51]. Pour cela, chaque nœud qui reçoit le bloc validé essaie d'ajouter ce nouveau bloc à sa version locale du registre en revérifiant que chaque transaction est nouvelle et valide par rapport à sa propre version et que ce nouveau bloc peut se greffer à l'extrémité actuelle. Si c'est le cas, les transactions contenues dans ce nouveau bloc deviennent valides, ce qui crédite la rémunération du mineur qui a créé ce bloc.

Le bloc en question sera ensuite rediffusé aux nœuds voisins jusqu'à sa transmission à l'ensemble du réseau[52].

Processus d'achat et de vente de Bitcoins

Il est possible de se procurer des Bitcoins en procédant à la vente de devises (ex. euros) en se connectant sur un site dédié qui constitue une place de marché (ex. Paymium). Après ouverture d'un compte auprès d'un prestataire[53] et inscription sur ce site au préalable, la première étape est la réalisation d'un virement bancaire suffisant sur le compte à approvisionner pour se voir proposer des devises à la vente. La seconde consiste à voir à quels prix les Bitcoins sont proposés en consultant le carnet d'ordres. L'étape finale relève de l'exécution du passage d'ordre, partiel ou total, selon les conditions limites ou celles du marché et la devise indiquées par l'acheteur. Le paiement en Bitcoins se fera simplement en indiquant l'adresse destinataire dans un formulaire de retrait des fonds, tandis que l'échange de Bitcoins contre des devises se fera par un simple ordre de vente associé à un compte bancaire.

Il devient réalisable de recourir à un distributeur automatique de Bitcoins (BTM)[54]. Bien que marginal[55], le développement géographique et en nombre de tels distributeurs[56] marque cependant la popularité de Bitcoin et développe la capacité de cette technologie à entrer sur le marché du paiement. Si les BTM ne remplacent pas les distributeurs automatiques dans les monnaies usuelles, leur usage pose déjà des questions en lien avec le blanchiment et la sécurité des portefeuilles électroniques présentés, comme il sera vu par après.

Daniel GUINIER
Docteur ès Sciences
Certifications CISSP, ISSMP, ISSAP en sécurité des SI et MBCI en gestion des crises
Expert en cybercriminalité et crimes financiers près la Cour Pénale Internationale de La Haye

Notes

(1) Voir Chavagneux C. (2004) et C. de Boissieu et J.-H. Lorenzi (2008).

(2) Avec des valeurs de change de 1 euro pour 0,8 dollar en 2000 à 1,6 en 2008, pour atteindre à la baisse 1,21 fin 2014.

(3) Ce qui n'est pas nouveau - voir : M. Allais (1999) : La crise mondiale d'aujourd'hui. Pour de profondes réformes des institutions financières et monétaires.

(4) Voir R. W. Rahn (1999).

(5) Colloque «Droit et monnaie» (1988) avec J. M. Servet et la conclusion par J. Carbonnier.

(6) Le remplacement du Franc par l'Euro, en tant qu'unité monétaire de la zone Euro à laquelle la France appartient, a été défini par le règlement CE n° 974/98 du 3 mai 1998.

(7) La quantité de valeurs convertibles en liquidités susceptibles d'être utilisables comme moyen de paiement d'une zone économique donnée. Elle est supérieure à 12 000 milliards de dollars et en évolution constante du fait de la capacité qu'ont les banques centrales à faire varier le taux directeur et la quantité de liquidités mises en circulation, en autorisant les banques à prêter plus qu'elles n'ont de fonds en dépôt.

(8) Les banques centrales produisent la monnaie fiduciaire et les banques commerciales, la monnaie scripturale sous la tutelle des premières.

(9) La monnaie confiée aux banques sous forme de dépôt est devenu un réservoir de monnaie, du fait de la sécurité offerte pour la conservation de l'épargne et des facilités de paiement du système bancaire. Par ailleurs, les écritures sont gérées par l'informatique.

(10) Du Latin «fiducia». Le régime monétaire dans lequel les banques sont dispensées d'échanger le papier monnaie contre du métal précieux correspond à l'adoption du «cours forcé» qui met fin à un système basé sur l'étalon or. Ainsi, l'euro, le dollar et le yen sont des monnaies fiduciaires, comme la majorité des monnaies d'autres pays. Lorsque la monnaie n'était pas constituée d'un métal de valeur, elle était cependant convertible en ce métal précieux. A cet effet, un billet de banque était alors une reconnaissance de dette de la banque émettrice qui s'engageait à l'échanger contre une certaine quantité d'or. Actuellement, elle est assise sur la seule confiance des agents économiques envers l'organisme qui l'émet, en billets comme en pièces.

(11) Le refus à leur valeur nominale de pièces ou des billets de banque ayant cours légal est une infraction pénale (en droit français : Art. R642-3 du CP), alors que, sous forme de billets de banque ou de pièces, la valeur matérielle est inférieure à la valeur nominale, contrairement à l'or qui est une référence en la matière, ou à d'autres éléments d'échange précieux.

(12) Avec une quasi-monnaie comme l'eurodollar, il est possible de s'affranchir de la règlementation de la zone d'origine, permettant ainsi la mise en circulation d'une masse de monnaie dérivée considérable.

(13) La loi impose notamment le paiement par chèque, carte ou virement, pour les traitements et salaires mensuels au-delà de 1 500 € par mois (Art. L.143-1 Code du travail), pour les achats de biens ou de services de plus de 3 000 €, non fractionné ou hors acompte, de biens ou de services, ou d'enchères, par un particulier résident et non commerçant, sinon à 750 € entre commerçants (Art. L. 112-6 Code monétaire et financier (CMF)). De plus, la loi interdit le transport de plus de 10 000 € en numéraire. Toute infraction à ces dispositions est sujette à une amende partagée de 750 à 15 000 €. (Art. L. 161-1 CMF et Art. 1749 CGI).

(14) En pratique, les montants déposés sont prêtés par la banque sans l'avis du déposant et en cas de faillite, sous réserve de la garantie

donnée par l'Etat, les dépôts seraient perdus.

(15) L'émetteur, en tant qu'intermédiaire dans des opérations de transfert de fonds, gère un moyen de paiement et doit avoir, en vertu de L'Art. 1 de la loi bancaire, un statut d'établissement de crédit.

(16) Voir directive 2009/110/CE du 16/09/09 du Parlement européen et du Conseil, concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE. Voir également, conférence EFE sur la lutte contre le blanchiment, Paris le 03/12/14, au vu de l'apparition de phénomènes de blanchiment ou de fraude fiscale, dus à des nouveaux moyens de paiement : cartes prépayées, monnaies virtuelles, etc.

(17) Autrement-dit, une unité standard permettant la mesure la valeur des flux et stocks de biens, de services et d'actifs.

(18) Banque de France (1999), sur la nature juridique de la monnaie électronique, p. 48.

(19) Le billet de banque remplissant les fonctions d'instrument monétaire et de moyen de paiement.

(2) Pseudonyme utilisé par une personne ou un groupe de programmeurs.

(21) Art. L315-1 du Code monétaire et financier et directive 2007/64/CE.

(22) Art. 4.15 de la directive 2007/64/CE du 13 novembre 2007 qui définit les fonds comme : «les billets de banque et les pièces, la monnaie scripturale et la monnaie électronique au sens de l'Art. 1, par. 3b), de la directive 2000/46/CE».

(23) BdF (2013) : Banque de France Focus, n° 10, 5 déc.

(24) L'Autorité de contrôle prudentiel et de résolution est une autorité administrative indépendante dont la mission et le champ de compétences sont définies par l'Art. L612-1 du Code monétaire et financier, avec pouvoir de sanction.

(25) Au cours du premier démantèlement d'une plateforme illégale en France, deux personnes ont été mises en examen: l'administrateur du site, poursuivi notamment pour «exercice illégal de la profession de banquier» et «blanchiment d'argent», ainsi que le fournisseur des Bitcoins. Cette plateforme échangeait des euros ou des dollars contre des Bitcoins, moyennant des taux de commission très élevés, entre 35% à 50% sans aucun agrément. Malgré cela, le site connaissait un fort succès avec 2 750 transactions enregistrées de novembre 2013 à juillet 2014, soit l'équivalent d'un million d'euros.

(26) Voir D. Guinier (2014), tandis que des «hackers» sont en devenir à différents stades et motivations.

(27) La compétence d'un droit délimité au vu d'un territoire d'un pays étant inadaptée à la cybercriminalité sans frontières, une adaptation du droit et des règles de procédures comme de la jurisprudence sont attendus. Voir M. Quéméner (2015).

(28) Sans aucune protection par un fond mutualisé du système bancaire, pour le premier, et sans surveillance de la plateforme et de ses méthodes par une autorité de tutelle, pour le second. Les investisseurs peuvent alors recourir à des fonds nécessitant des opérations d'arbitrage de façon homologue aux systèmes financiers existants, avec un fort risque de change en plus.

(29) Les CFD (Contract for difference) sont interdits aux Etats-Unis, mais autorisés sous conditions en France.

(30) L'Autorité de contrôle prudentiel et de résolution (ACPR) rappelle : «Dans le cadre d'une opération d'achat / vente de Bitcoins contre une monnaie ayant cours légal, [...] lorsqu elles sont réalisées en France, ces transactions doivent être effectuées par l'intermédiaire d un prestataire en services de paiements (c'est-à-dire un établissement de crédit, un établissement de paiement ou un établissement de monnaie électronique)».

(31) Après que Le Monde ait titré «Avec Bitcoin, payer et vendre sans les banques» dans un article de nov. 2012, décrivant le fonctionnement de Bitcoin, suite à un long travail de lobbying, il était annoncé le 06/12/12 le partenariat entre Aqoba et Paymium, de façon à permettre aux Bitcoins de transiter légalement au sein du système bancaire.

(32) Voir E. Galston (2014) et M. A. Cusumano (2014).

(33) Alors que le marché ForEX a été associé à des agissements douteux et qu'un rapport de l'AmF fait état de plaintes émanant essentiellement de plaignants crédules et vulnérables démarchés par des entités sans aucun agrément.

(34) Tandis que le Bitcoin (BTC) est la devise qui relève de ce dernier.

(35) Comportant son montant en Bitcoins et les adresses électroniques du payeur et du destinataire.

(36) Ceci permet notamment d'assurer la même somme associée à une transaction n'est pas dépensée plus d'une fois.

(37) De l'ordre de 26 Go fin décembre 1014 contre deux fois moins une année auparavant.

(38) En 2014, le nombre total de transactions au niveau mondial oscille entre 50 000 et 100 000 par jour en impliquant moins de 100 millions de dollars

(39) Voir A. Back et al. (2014). En cas de rupture cryptographique ou de conception malveillante dans une chaîne latérale, les dommages seraient confinés à cette seule chaîne latérale.

(40) Voir D. Guinier (2000a, b et 2006), SGDN (2007), S. Nakamoto S. (2008), et C. Percival et S. Josefsson (2012).

(41) L'algorithme de signature fondé sur les courbes elliptiques de Koblitz : ECDSA pour Elliptic Curve Digital Signature Algorithm a été montré comme sûr en 2001 et publié en tant que norme ANSI X9.62. Il repose sur la difficulté de calculer le logarithme discret d'un grand nombre entier avec des clés d'une taille de 256 bits, offrant une sécurité comparable à celle d'un système RSA sur 3072 bits fondé sur la difficulté de factorisation de très grands nombres, à condition de changer la valeur de k à chaque création de signature pour ne pas permettre l'obtention de la clé privée.

(42) La fonction de hachage usuellement utilisée est SHA-256 sur 256 bits, avec un algorithme en deux passes, tandis que RIPEMD-160 sur 160 bits est requise pour la création d'adresse avec condensés de plus faible taille.

(43) Une adresse Bitcoin est composée de 34 octets et la clé privée, de 50 octets.

(44) Il contient en particulier un identifiant unique utilisé comme clé primaire dans la base de données blockchain.info, une clé attribuée de façon aléatoire comme preuve de propriété du portefeuille (laquelle servira à chiffrer les clés privées), l'adresse Bitcoin ainsi que la clé privée, chiffrée ou non, etc.

(45) Celui-ci sert de clé de chiffrement, codé en base 64. Par ailleurs, la norme ISO 10126 donne les spécifications de l'algorithme PBKDF'2 en mode CBC.

(46) Par ex., chaque module Achilles Labs AM-6000, compatible avec le logiciel CGMiner, d'un coût de l'ordre de 2900 $, délivre 6000 GigaHashs/s (SHA-256 double passe) soit 2073 MegaHashs/s/$. Ceci nécessite une puissance électrique de 3800 W, soit 0,63W/GigaHash calculé, ce qui se traduit par 1579 MegaHashs/Joule, en termes de dépense en énergie.

(47) ASIC, pour Application Specific for Integrated Circuit, est un circuit intégré spécifique intégrant tous les éléments actifs nécessaires à la réalisation des fonctions d'une application ; dont le hachage dans ce cas.

(48) GHash.IO dispose d'une puissance de calcul de 41 millions de GigaHashs/s. Voir https://en.bitcoin.it/wiki/GHash.IO.

(49) Voir le calculateur en temps réel «Bitcoin mining calculator» : http://www.alloscomp.com/bitcoin/calculator.

(50) Le calcul exigé, rendu extrêmement difficile, permet une cadence décentralisée à intervalle quasi-constant d'environ dix minutes, la production de blocs valides adaptée pour maintenir cet intervalle constant, quelle que soit la puissance de calcul du réseau Bitcoin.

(51) En plus des frais de transaction redistribués, ce montant attribué est en diminution (actuellement de 25 Bitcoins).

(52) Une correction d'incohérence, prévue dans le protocole de construction de la blockchain, sera rendue nécessaire lorsque des nœuds différents ont accepté des blocs différents, ce qui aboutirait alors à des versions différentes de ce registre, du fait de différentes latences : communication, calculs, etc.

(53) Auprès d'un prestataire de paiement, dûment agréé selon la réglementation française.

(54) BTM (Bitcoin Teller Machine) par analogie à ATM (Automated Teller Machine) ou automate de libre-service.

(55) http://www.coindesk.com/7-charts-show-year-growth-bitcoin-atms/.

(56) En 2014, plus de 64 de ces distributeurs BTM sont localisés dans plus de 20 pays européens, dont 30% aux Pays-Bas et au Royaume-Uni. Concernant la Finlande 6 sur 7 sont à Helsinki qui comporte 11% de la population nationale pour 86% de détenteurs de Bitcoins. Les villes Helsinki (6), Londres (6) et Prague (4) étant les mieux pourvues.

Légende détaillée du schéma page 61

Portefeuilles : *fichiers wallet.dat contenant les adresses Bitcoin de A donnant accès aux Bitcoins et clés privées de chacune d'elles : Ex. 25M2vDxzVavhm9Me5VJ1QrEab3PxT5i627 C'est aussi l'empreinte cryptographique d'une clef publique.*

Création d'adresse et des clés de : *V crée une nouvelle adresse et transmet à A la clé publique générée. Il conserve la clé privée pour prouver qu'il est le destinataire.*

Demande de transaction : *Indication de transfert de Bitcoins au logiciel client depuis une des adresses de A vers la nouvelle adresse générée par le vendeur V et signature du message de transaction en appliquant la clé privée ad hoc de A sur le condensé.*

Légitimité de la transaction : *Toute entité connectée au réseau peut utiliser la clé publique correspondante de A pour vérifier que la demande émane d'un compte légitime.*

Vérification de la transaction et d'intégrité : *A partir du logiciel client Bitcoin et de la blockchain à jour, les «mineurs» connectés au réseau apportent une preuve de travail d'environ 10 mn en cherchant avec leur puissance de calcul une variable aléatoire («nonce») qui, ajoutée au bloc lié à la transaction, aura pour résultat un condensé SHA-256 faible débutant par un certain nombre de zéros (ex. 000000000000f3be6... De telle façon que la nouvelle valeur de «hash» calculée soit liée à l'ensemble des transactions précédentes, au nouveau bloc de transaction et à cette variable.*

Validation de la transaction : *chaque nœud recevant le bloc issu du «mining» essaie de l'ajouter à sa version locale de la blockchain en revérifiant que chaque transaction est nouvelle et valide par rapport à sa propre version et que ce nouveau bloc peut se greffer à l'extrémité actuelle. Le bloc sera ensuite rediffusé aux nœuds voisins jusqu'à sa transmission à l'ensemble du réseau Bitcoin.*