Hors Série

1

Edito


Ces dernières semaines, le Bitcoin a souvent fait la une des journaux. Décrié par certains pour son utilisation massive dans les milieux mafieux, cette monnaie virtuelle est encensée par d'autres pour les nombreux avantages qu'il apporte par rapport à ses concurrents traditionnellement établis. Mais qu'est-ce que le Bitcoin ? Comment ça marche ? Quels sont les risques inhérents à sa détention et à son utilisation ? Comment s'en prémunir ? Alors, est-ce que le Bitcoin est un concept fumeux ou futur des transactions financières ?

C'est l'objet de ce hors série, dans lequel nous allons essayer de démystifier le concept Bitcoin, son fonctionnement et, sécurité oblige, présenter les risques inhérents à son utilisation ainsi que quelques recommandations pour sécuriser son capital Bitcoin s'il vous prenait un jour l'envie de vous lancer dans l'aventure. Un conseil cependant : « Bitcoin n'est qu'une expérience. N'y investissez que l'agent et le temps que vous pouvez vous permettre. »

Bonne lecture à toutes et à tous !

Sara FOMINAYA
Julien CASTAIGNE

Equipe Expertise Sécurité du SI

Bitcoin

Le Bitcoin est en quelque sorte la nouvelle monnaie électronique à la mode. Cette dernière a été mise en service en 2009 par une personne ou un groupe de personnes souhaitant garder l'anonymat et agissant sous le pseudonyme de Satoshi NAKAMOTO. Nous essayons à travers ce numéro spécial de démystifier le concept Bitcoin et de présenter les risques et quelques bonnes pratiques de sécurité relatives à l'usage de cette monnaie virtuelle.

Bitcoin, c'est quoi ?

Le Bitcoin (sigle : BTC) est une monnaie électronique distribuée aussi appelée crypto-monnaie. Par monnaie il faut entendre à la fois devise monétaire (comme l'Euro ou le Dollar) et moyen de paiement (on peut payer des produits et des services en Bitcoin).

En effet, ce n'est ni plus ni moins que le pendant électronique des pièces et billets que l'on peut avoir dans son porte-monnaie qui, pour le coup, devient complètement virtuel. Après le courrier électronique, ou la dématérialisation de la musique ou des vidéos, il semble donc que le prochain « objet » de notre vie de tous les jours à être rendu complètement numérique soit notre argent.

Pour ce faire, BTC repose à la fois sur des principes techniques (réseau de « peer to peer », cryptographie pour la signature des transactions, etc.) et économiques (masse monétaire fixe : la quantité de Bitcoin en circulation est fixe et ne dépassera jamais 21 millions de Bitcoins). Il y a différentes façons d'obtenir des Bitcoins :

- En achetant sur des places de marchés dediés, tout comme on le ferait pour une devise étrangère,
- En échangeant des BTC avec quelqu'un près de chez vous,
- En participant au protocole de validation. Lorsqu'une transaction est validée par le réseau, une prime en BTC est accordée aux participants.

Il est à noter que le Bitcoin n'est pas la seule monnaie cryptographique existante mais c'est la première à avoir vu le jour. En effet, BTC a permis d'améliorer le concept b-money imaginé en 1999 et de bitgold décrit en 2005. De même, les trois dernières années sont marquées par le développement de nouvelles crypto-monnaies (Litecoin, Peercoin, etc.) qui se positionnent sur le même segment de monnaie alternative que BTC.

RTE\FASIT\DSIT\CEESI\DIS\E²S
Centre de Compétences Sécurité
mail : RTE-DSIT-CEESI-DIS-SECURSI

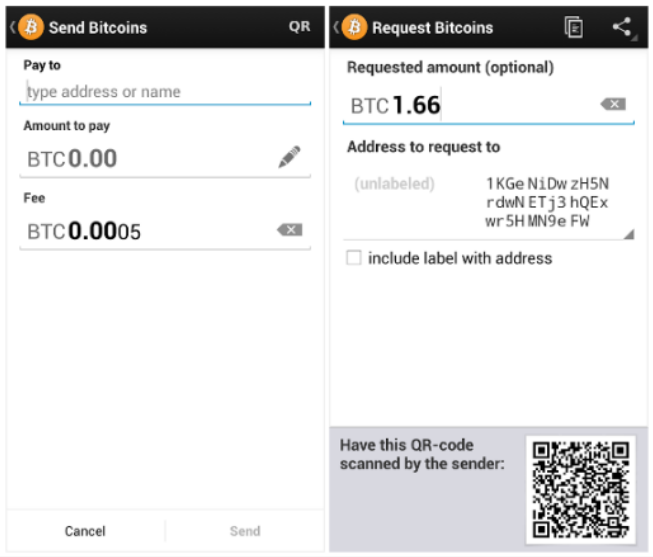
BTC : Comment ça marche ?

BTC est à la fois une devise monétaire virtuelle et un système/protocole de paiement dans cette devise. Le fonctionnement du BTC est quelque part analogue à la messagerie électronique. En effet, tout utilisateur BTC doit posséder une adresse BTC (exemple d'adresse BTC : 1FGAftzSTztFSB8LMvsrdCKTyqGY6zr3sM) qui donne accès a un porte monnaie électronique et donc les transactions s'effectuent d'une adresse BTC à une autre. Ceci, permet au système transactionnel BTC de garantir l'anonymat des acteurs de la transaction.

Le porte monnaie doit être installé sur un ordinateur ou sur un mobile. Le porte monnaie calcule son solde à partir d'une espèce de livre de comptes, qui contient toutes les transactions depuis le commencement du Bitcoin, appelé chaine de blocs. Cet historique est connu par tous les ordinateurs du réseau.

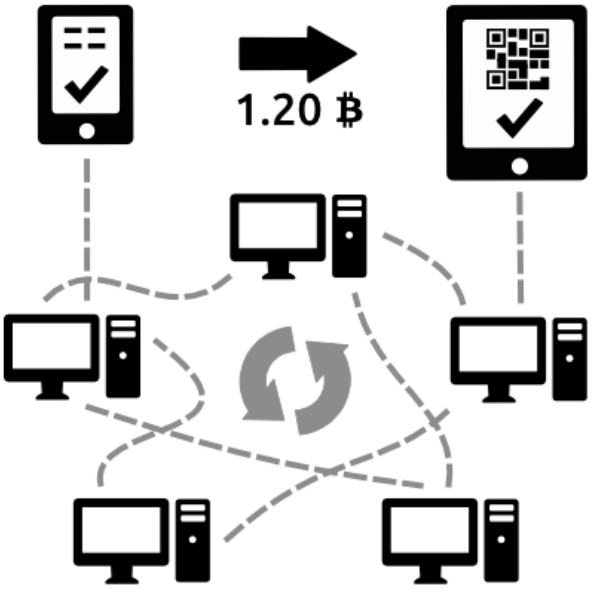
Pour accéder au porte monnaie ainsi que pour envoyer ou recevoir des Bitcoins, rien de plus simple qu'une application mobile ou un logiciel installé sur l'ordinateur. Le porte monnaie, une fois installé, créera une première adresse Bitcoin.

Une fois que l'utilisateur accède à son porte monnaie, il peut faire des paiements. Il faut introduire l'adresse d'envoi (vu la complexité des adresses Bitcoin, ce champ peut être rempli en scannant le code QR qui du bénéficiaire), le montant de la transaction et cliquer sur accepter. Les BTC seront transférés et la transaction vérifiée par le réseau.



Toute transaction en BTC est signée par l'utilisateur à l'aide d'une clé privée contenue dans le porte monnaie. Grâce à cette opération, tout le monde sur le réseau peut vérifier que la demande de transaction provient bien du propriétaire légitime du compte.

Un paiement avec Bitcoin est presque instantané. Toutefois, les Bitcoins reçus ne peuvent pas être dépensés avant que le réseau ait confirmé la transaction. Le temps de validation est d'environ 10 minutes.



BTC : validation d'une transaction

Le processus de validation, transparent aux utilisateurs, s'appelle minage. Pendant le minage, les transactions sont validées par les ordinateurs du réseau Bitcoin, appelées mineurs. Les transactions validées sont incluses dans la chaine de blocs.

Toutes les transactions qui ont eu lieu pendant les dernières 10 minutes, vont être intégrées dans un bloc de transaction. La fonction des mineurs est de calculer des fonctions mathématiques associées à ces transactions. La complexité des algorithmes exige l'utilisation de la puissance de calcul de l'ordinateur.

Tous les mineurs du réseau reçoivent la transaction et sont donc en concurrence afin d'obtenir le résultat et vérifier l'opération. Le gagnant est rétribué en échange de sa contribution avec des Bitcoins, générés par le réseau.

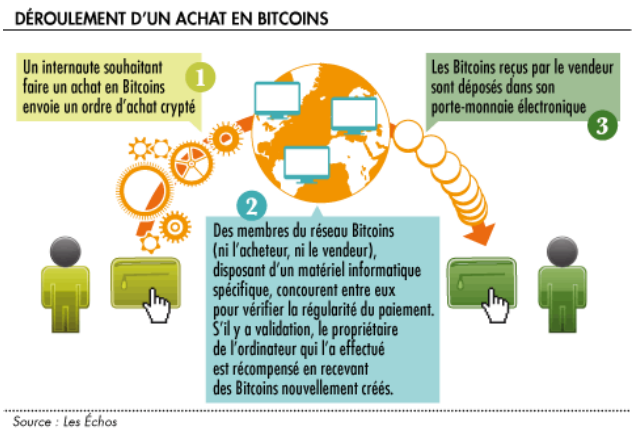
En accord avec l'algorithme, la quantité de Bitcoins générés par le réseau est fixe : dès que la limite sera atteinte, les mineurs devront être récompensés avec de l'argent provenant des frais de transaction.

Souvent, les mineurs se regroupent en coopératives de mineurs (mining pool), et le gain associé à une transaction est répartit entre tous les membres proportionnellement à leur effort de calcul.

Toute personne peut devenir un mineur de Bitcoins en utilisant un logiciel et du matériel informatique spécialisé.

Grâce au minage, le réseau confirme que les Bitcoins n'ont été envoyés à personne d'autre et sont considérés comme étant de la propriété du bénéficiaire de la transaction. C'est la solution donc au problème des attaques par double dépense (création de deux transactions pour dépenser la même chose).

RTE\FASIT\DSIT\CEESI\DIS\E²S
Centre de Compétences Sécurité
mail : RTE-DSIT-CEESI-DIS-SECURSI



Bref, le BTC s'appuie sur trois principes (chaine de blocs, clés privées et minage), permettant au système de s'affranchir de l'intégrité et de la compétence d'un émetteur central et donc d'assurer une gestion décentralisée de la monnaie.

BTC : cas pratiques

- Berlin, capitale mondiale du BTC. A Berlin, une trentaine de cafés, hôtels, restaurants et commerces du quartier de Kreuzberg acceptent le Bitcoin. Par ailleurs, le gouvernement allemand a reconnu officiellement le Bitcoin comme « monnaie privée », indépendante de l'état. Cette existence juridique permettra au gouvernement du pays de surveiller les échanges en BTC et de les taxer.
- Distributeurs de Bitcoin : A Vancouver (Canada), le premier distributeur de BTC au monde, a été installé en octobre 2013. Le principe du distributeur est d'échanger des dollars canadiens contre des Bitcoins. En Europe Stockholm a décidé, elle aussi, de se doter d'un distributeur de Bitcoins. A la fin de cette année, on estime que 40 de ces distributeurs seront opérationnels dans le monde entier.
- Sites où on peut payer en BTC. Le Bitcoin est déjà utilisé par un grand nombre de sites Internet. Aussi, les commerces physiques sont de plus en plus nombreux à proposer des transactions avec le Bitcoin, avec une augmentation de 81% en novembre 2013. Voici quelques annuaires qui regroupent les sites où le payement en Bitcoins est possible :
  - **Plans interactifs qui montrent les endroits au monde** (boutiques, bars, restaurants et d'autres commerces), où le Bitcoin est accepté : http://coinmap.org/, http://Bitcoin.travel/, http://useBitcoins.info/
  - **Portail de commande de repas en ligne** : http://corporate.takeaway.com
  - **Liste de sites internet acceptant un payement en Bitcoin** : http://www.Bitcoin.fr/post/2010/12/30/Que-faire-avec-mes-Bitcoins, leBitcoin.fr

BTC : les risques

Le BTC a plusieurs avantages, notamment :

- L'utilisateur contrôle lui-même son porte monnaie en l'absence d'une autorité centrale,
- Le BTC est parfaitement adapté à internet et peut servir pour des micros-transactions,
- Le BTC est une devise globale et neutre et donc il n'est normalement pas possible pour une quelconque autorité d'arrêter le réseau,
- Le BTC n'est pas falsifiable puisqu'il ne s'agit pas d'une monnaie fiduciaire,
- Le BTC permet d'éviter l'inflation du fait qu'il repose sur le principe d'une masse monétaire fixe (21 millions de BTC) et donc il n'est pas possible d'exercer des pratiques permettant de dévaluer la monnaie,
- Sécurité très solide du système BTC du fait qu'il repose sur une cryptographie robuste sans point central.

Depuis son origine, l'utilisation de cette crypto-monnaie affiche aussi certains risques à prendre en compte :

- Risque d'irréversibilité des transactions du fait de l'anonymat de ces dernières,
- Risques opérationnels et technologiques liés au logiciel et à l'environnement informatique,
- Risque de change par rapport aux monnaies fiduciaire et donc de volatilité liée principalement au fait que le BTC est sujet à de fortes variations de son cours,
- Risque juridique du fait de son statut de monnaie non régulée,
- Risque financier du fait du caractère hautement spéculatif des BTC,
- Risque politique puisque le BTC peut devenir un moyen de financement d'une économie parallèle et un moyen d'échapper au contrôle des états et des banques (blanchiment d'argent, transactions délictueuses, évasion fiscale, etc.)
- Risque de vol du porte-monnaie BTC,
- Etc.

D'ailleurs l'autorité bancaire européenne (EBA) a mis en garde, dans un document publié en Décembre 2013, les détenteurs des monnaies électroniques comme le BTC contre ces risques inhérents à la détention et l'utilisation de ce type de monnaie.

D'un point de vue sécurité de l'information, le logiciel de BTC, du moins dans sa conception initiale, contrairement à une idée reçue liée à la méconnaissance de la signification exacte de la cryptographie, ne chiffre aucune donnée qu'il utilise. Seul le porte-monnaie de clefs privées est susceptible d'être chiffré par l'utilisateur ou laissé à la charge du système d'exploitation comme n'importe quel autre fichier. Cependant, même en chiffrant ce fichier d'autres risques résiduels peuvent subsister, notamment :

- Perte de la clé de chiffrement et donc la perte du porte-monnaie BTC,

RTE\FASIT\DSIT\CEESI\DIS\E²S
Centre de Compétences Sécurité
mail : RTE-DSIT-CEESI-DIS-SECURSI

- Compromission du matériel informatique hébergeant le porte-monnaie BTC,
- Perte ou vol du matériel sur lequel est installé le porte-monnaie,
- Vol de BTC suite à l'exploitation d'une vulnérabilité relative à une erreur d'implémentation du porte-monnaie BTC,
- perte de BTC suite à attaque sur le réseau BTC,
- Etc.

D'ailleurs, en Octobre 2013 et selon les développeurs de Bitcoin.org, une vulnérabilité impactant les porte-monnaie électroniques des BTC générés à partir d'un client Android a été publiée. Cette vulnérabilité aurait permis le vol de BTC à cause d'un souci dans la façon dont Android génère les nombres de manière aléatoire. Dans un souci de sécurité, aucune donnée technique n'a été publiée sur la faille et une correction a été apportée par les développeurs qui ont opté pour une réinitialisation des clés de chiffrement avec un générateur de nombre aléatoire valide. De cette façon les utilisateurs n'auront qu'à envoyer leur argent de l'ancien porte-monnaie au nouveau. En outre, en novembre 2013, des chercheurs ont annoncé avoir trouvé une méthode pour mener des attaques sur le réseau BTC.

Tout ceci montre qu'il faut prendre des précautions d'utilisation de cette monnaie virtuelle qui pourrait causer un préjudice financier important à son détenteur. En particulier, quand on sait que le taux de change de cette monnaie est passé de 4,15 € en février 2011 à 659,17 € en décembre 2013.

BTC : les bonnes pratiques sécurité

Comme vous l'avez compris, il existe plusieurs niveaux de risques inhérents à la détention et l'utilisation du BTC. Pour couvrir les différents niveaux de risques, il faut mettre en place plusieurs niveaux de sécurité en commençant par la sensibilisation des utilisateurs. Dans cette perspective, l'équipe sécurité a rassemblé quelques bonnes pratiques à adopter par un utilisateur du BTC. Ainsi, la liste suivante, n'ayant pas pour vocation d'être exhaustive, regroupe un ensemble de recommandations pour se prémunir des risques de détention et d'utilisation de cette monnaie virtuelle :

- Chiffrez votre porte-monnaie avec mot de passe et gardez minutieusement votre clé de chiffrement,
- N'oubliez pas le mot de passe, car BTC ne compte pas de mécanisme de récupération de mot de passe,
- Faites des sauvegardes régulières de votre porte-monnaie,
- Privilégiez l'utilisation des « cold storage » telle une clé USB non connectée à internet ou même des « deep cold storage » telle une clé USB rangée dans un coffre fort (du monde réel) au « hot wallet » [NdT : portefeuilles connectés],
- Ne mettez pas tous vos Bitcoins sur un même porte-monnaie,
- Choisissez avec précaution votre porte monnaie en ligne. Si le site web n'est pas suffisamment sécurisé et qu'il se fait pirater, la totalité de l'argent stocké sous cette forme, sera perdue,
- Utilisez un système multi-signature pour signer les transactions. Bitcoin inclut une fonctionnalité qui permet à une transaction d'exiger la signature de plus d'une clé privée avant d'être dépensée,
- N'utilisez pas un mot de passe faible ou un mot de passe que vous utilisez sur d'autres services internet pour le chiffrement de votre porte-monnaie BTC.
- N'envoyez pas de copies non chiffrées de vos porte-monnaie sur internet,
- Vérifiez l'authenticité des sites vous proposant d'effectuer des opérations par BTC,
- Mettez à jour vos logiciels et votre système d'exploitation avec les dernières mises à jour sécurité,
- N'exécutez pas de programmes copiés sur internet dans le même environnement hébergeant votre porte-monnaie BTC.

Adopter ces quelques recommandations vous apportera un meilleur niveau de sécurité de vos BTC. Cependant, le risque zéro étant un mythe, la première règle à suivre est de redoubler de vigilance quand vous serez amenés à manipuler cette monnaie virtuelle. De plus, ayez toujours dans l'esprit que la nature totalement immatérielle de cette monnaie l'expose, fort logiquement, au risque d'être volée de manière tout aussi immatérielle

Conclusion

Le Bitcoin offre un très haut niveau de sécurité s'il est utilisé correctement. Toutefois, des failles de sécurité ont été trouvées et corrigées avec le temps dans plusieurs implémentations logicielles existantes.

Entre ceux qui pensent que le Bitcoin est un concept fumeux et ceux qui y voient un réel potentiel pour le futur des transactions financières, le Bitcoin a toutes ses chances pour s'installer dans le paysage économique mondial.

Nous nous permettons ce constat puisque le Bitcoin est une technologie contrôlée par les masses, à l'image de linux et internet, et comme le montre l'expérience et l'histoire, ces technologies prennent vie d'elle-même. De plus, cette crypto-monnaie séduit de plus en plus de particuliers et de sociétés. Elle commence à être reconnue par les autorités américaines, à l'image des déclarations faites par le patron de la banque centrale américaine, qui a salué le potentiel de la monnaie électronique et a estimé que, si des innovations de ce type pouvaient comporter des risques liés à la fraude, elles pouvaient aussi être prometteuses à long terme.

De même, pour répondre à la demande croissante d'utilisation du BTC comme moyen de paiement, un nombre croissant de boutiques physiques, de restaurants et d'autres commerces commencent à accepter ce type de paiement.

En attendant, Bitcoin voit des crypto-monnaies alternatives s'élever à ses côtés : Litecoin (créée en 2011), Namecoin (créée en 2011), Peercoin (créee en 2012) et Dogecoin (créée en décembre 2013) pourraient lui faire l'ombre avant qu'elle n'ait le temps de s'imposer totalement sur le segment de la monnaie alternative.

RTE\FASIT\DSIT\CEESI\DIS\E²S
Centre de Compétences Sécurité
mail : RTE-DSIT-CEESI-DIS-SECURSI