Et si le Bitcoin revenait au premier plan sur internet

Publié le vendredi 30 janvier 2015
Voir en ligne : https://www.france-science.org/Et-si-le-Bitcoin-revenait-au,4425.html

Mardi 27 Janvier 2015, se tenait à Washington, DC une conférence "*State of the net*" réunissant des membres du gouvernement américain, des industriels et des représentants d'entreprises du secteur privé pour faire un point sur l'internet aujourd'hui. De nombreux sujets ont été abordés comme la cyber-sécurité avec la récente attaque des studios SONY ou encore le discours du président Obama. Un autre sujet s'est invité au premier plan et a suscité de nombreuses questions. Il s'agissait du Bitcoin.

Nous acceptons les bitcoins
Crédits : Tang Yann Song

Le Bitcoin [1] est l'une des monnaies virtuelles les plus connues aujourd'hui. Fred Ehrsam, co-fondateur de la société Coinbase, était présent comme conférencier principal lors de cette conférence et a dénombré les avantages du Bitcoin mais a surtout annoncé tous les nouveaux domaines d'utilisation et d'application de cette monnaie. Sa société, CoinBase, propose une solution de porte-monnaie électronique qui permet d'acheter des Bitcoins et de réaliser des achats en toute légalité. De grandes entreprises comme le géant Expedia acceptent dorénavant le Bitcoin comme moyen de paiement. Le Bitcoin devient de jour en jour le leader des crypto monnaies loin devant le Litecoin, le Dogecoin ou encore l'Aurora. On constate que les mentalités évoluent et s'écartent de l'ancienne vision criminelle de l'utilisation du Bitcoin.

Ce moyen de paiement s'ouvre donc peu à peu à tous les utilisateurs du net et rentre peu à peu dans les moeurs. Il apparaît aussi comme une possible nouvelle option à de nombreuses applications. Alex Fowler, co-fondateur de Blockstream a énuméré certaines d'entre elles : il pourrait être utilisé pour voter, sécuriser un document, vérifier une identité et bien d'autres applications.

La crypto monnaie comme elle est aussi appelée, utilise un algorithme ECDSA [2] (*Elliptic Curve Digital Signature Algorithm*) qui permet de signer et vérifier les transactions sur le même principe que l'algorithme plus connu, l'algorithme RSA. La différence se situe dans le fait que la complexité de l'algorithme RSA réside dans la difficulté de factoriser un grand nombre premier alors que celle de l'ECDSA réside dans la complexité de factoriser le logarithme discret. La sécurité de l'algorithme ECDSA est comparable à celle de l'algorithme RSA et permet de préserver l'identité de son utilisateur. Elle permet aussi d'intégrer d'autres informations à l'intérieur du Bitcoin qui seront protégées par ce même algorithme.

Dans toutes ces discussions il a été rappelé par l'audience que cette monnaie virtuelle n'est ni régulée par une autorité ni disponible en grande quantité dans le temps et donc que sa valeur peut-être très variable.

Sources :

- [1] "La crypto monnaie bitcoin pourrait participer…" - BE Etats-Unis 369 - Xavier Lavayssière - 16/05/2014 http://www.bulletins-electroniques.com/actualites/75929.htm
- [2] "ECDSA, la technologie clé du Bitcoin" - http://www.e-ducat.fr/bitcoin-2/securite-signatures-ecdsa/

Pour en savoir plus, contacts :

Le site internet de la conférence "state of the net" : http://www.stateofthenet.org/

Code brève
ADIT : 77732

Rédacteurs :

- Privel Hinkati, Attaché scientifique adjoint - Washington, DC, deputy-ntics@ambascience-usa.org ;
- Retrouvez toutes nos activités sur le site de la MST de l'Ambassade de France aux Etats-Unis : http://france-science.org.