Les cryptomonnaies et l'état

Petit manuel concernant la bonne gestion des cryptomonnaies à destination de l’état

Crédit photo : Duncan Rawlinson

Pourquoi est-ce que nos monnaies marrantes font des sueurs froides aux états ? Parcequ’ils se disent que les gens sont des filous et que leur premier but dans la vie est de frauder l’administration fiscale. Du coup, qui dit absence de traçabilité de l’argent dit absence d’impôt.

La version officielle du discours, c’est la noble lutte contre le terrorisme, la pédophilie, la drogue ou tout autre chose vilaine à l’esprit de la majeure partie de nos concitoyens. C’est de la poudre aux yeux, puisqu’on sait fort bien que la traçabilité des cryptomonnaies majoritaires est quasi garantie, si on met de coté les services de blanchiment qui ont de toute façon une fâcheuse tendance à disparaître ou à se faire tellement petits qu’une utilisation majoritaire est peu probable.

Pour protéger sa rente, l’état accorde, via l’ACPR, des autorisations de traiter des bitcoins. Concrètement, ça doit être à peu près la même que des boites comme Western Union doivent demander. Le gros intérêt de ça, c’est qu’avant de traiter avec un client, la boite doit relever son identité, histoire que si l’argent sert à faire des crapuleries, on ait une chance de retrouver la personne.

Bon, une pièce d’identité, surtout quand elle n’est absolument pas vérifiée par la personne qui est derrière le guichet, ça engage pas à grand chose, mais si ça peut leur faire plaisir, pourquoi pas…

Par contre, là où c’est un brin chiant, c’est qu’il faut se taper l’accord de l’ACPR pour pouvoir innover un peu en matière de cryptomonnaies. Je ne l’ai pas encore demandé, mais rien qu’en lisant les formulaires, on attrape des boutons. Dans l’absolu, me concernant, je cherche à faire ça proprement. Je ne veux pas vendre des AK47 ou des sacs de poudre. Je veux juste pouvoir payer ma bière dans mon pub favori.

Toutes les cryptomonnaies se basent sur des identifiants de portefeuilles. Partant de là,

pourquoi ne pas imaginer une API permettant d'assouplir les règles ?

Scénario :

> J'ai besoin de 220mBTC, je me rend à la maison du bitcoin rue du Caire à Paris, je donne mon passeport à la dame, je lâche quelque chose comme 100 € avec ma CB et boum mon wallet est plus riche de 220mBTC. La dame a fait un scan de mon passeport comme l'ACPR lui a demandé.
>
> L'intérêt de ce scan, c'est que l'ACPR puisse demander à la dame qui a acheté ces bitcoins. Elle est donc amenée, à un moment, à venir demander ce scan à la maison du bitcoin.
>
> Partant de là, pourquoi ne pas envoyer à l'ACPR l'identifiant du wallet en indiquant qu'on a le scan de pièce d'identité à dispo ? D'une part l'ACPR a l'information sous la main qui lui permet de lutter contre le terrorisme, la pédophilie et l'évasion fiscale et en prime, elle peut constituer une API à laquelle des souscripteurs d'une convention plus légère avec l'ACPR pourront accéder et qui leur dira « oui, ce wallet là, on sait que quelqu'un sait qui c'est et tu peux traiter avec la personne qui de demande un change de monnaie sans risquer les foudres administratives ».

Du coup, le boulanger du coin pourra d'une part accepter les paiements basés sur une cryptomonnaie quelconque (ce qu'il peut théoriquement déjà faire, moyennant une sérieuse discussion avec son centre des impôts ou l'utilisation d'un mandataire qui fera la conversion en Euro pour lui) mais aussi proposer de l'échange de monnaie en toute quiétude avec les wallets des gens qui auront été vérifiés.

Je ne suis pas fana du fichage, mais cette solution a l'élégance de ne pas centraliser l'information tout en la conservant disponible « au cas où » et en garantissant à peu près son effacement dans les délais légaux puisqu'elle sera au mains des entités qui font les vérifications. Si c'est un moyen d'arriver à développer la monnaie non bancaire, ça me semble un compromis acceptable.

En allant plus loin, c'est une première piste pas idiote pour jeter les bases de la gestion de l'identité numérique de demain et avancer vers des monnaies de 3e génération qui pourront, grâce à un meilleur contrôle de l'unicité des wallets, implémenter les notions du revenu de base.

Evidemment, ça suppose que l'état ne soit pas pourri jusqu'à la moelle par le lobby bancaire. Et ça, c'est pas gagné.