Tous à poil !

Stéphane Bortzmeyer
stephane+pses@bortzmeyer.org

Pas Sage en Seine, 26 juin 2014

Un intéressant problème technique

Soit des opérations dont on veut prouver qu'elles ont lieu, ou qu'elles n'ont pas eu lieu (achats et dépenses, enregistrement d'un nom. . .) Comment créer de la confiance dans le public ?

La méthode traditionnelle est **centralisée** : un acteur « de confiance » garde trace des opérations et assure publiquement que tout s'est bien passé. L'acteur central joue normalement sa réputation et a donc intérêt à respecter les règles.

Exemples traditionnels

- Domaines de têtes via l'ICANN,
- Argent via les banques et/ou Paypal.

Confiance

N. m. : Phénomène irrationnel et difficile à justifier

- Enron, Lehman Brothers, MtGox...
- Sciences Politiques, premier cours de la première année : quand il y a du pouvoir, il n'y a plus d'honnêteté (Montesquieu l'avait mieux dit).
- Remplacer l'ICANN par Telecomix, FDN ou la Quadrature du Net ?
- Les systèmes centralisés nécessitent toute une supervision, des contre-pouvoirs, des mécanismes d'*accountability*...

Alternative : tout exposer

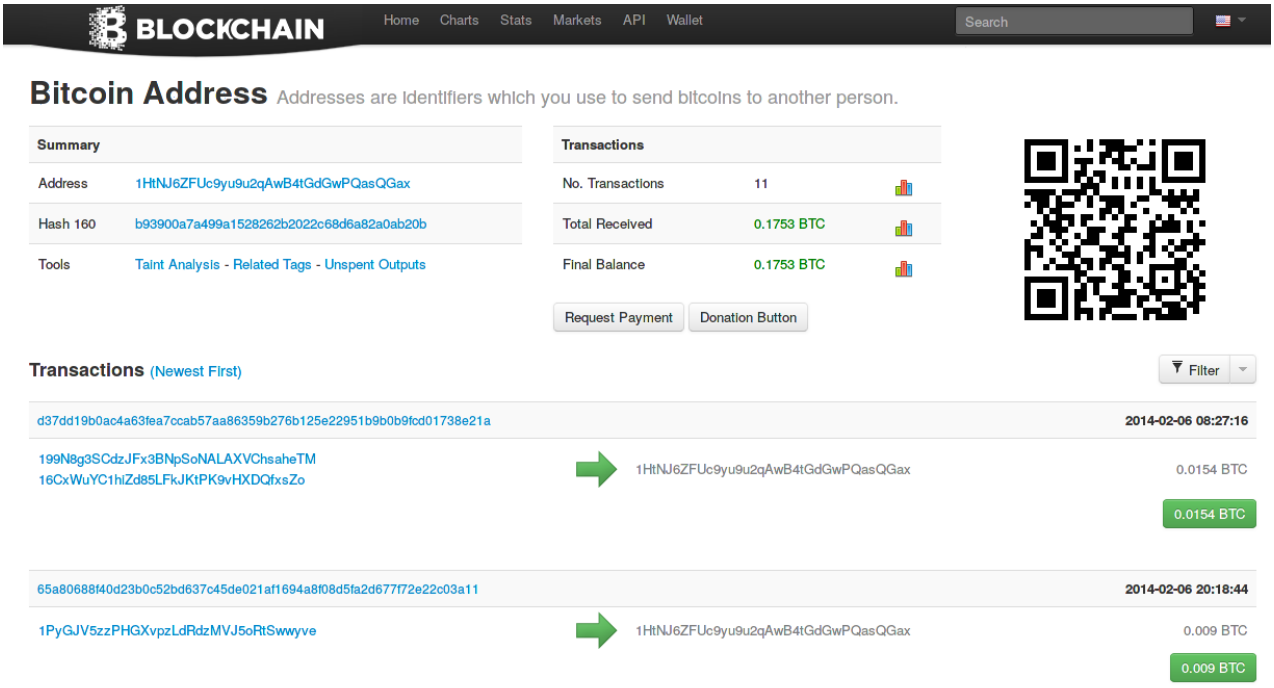
1. Si tout est public, n'importe qui **peut** vérifier (on ne dit pas que tout le monde le fera),
2. Plus besoin de confiance dans un organisme central !

Exemple : le bitcoincoin

Bien plus qu'une monnaie, Bitcoin est un système permettant la tenue d'un livre d'opérations public : tout le monde peut vérifier que les bitcoins n'apparaissent pas ou ne disparaissent pas magiquement.

Peut servir de base à bien des choses. Pour la monnaie, peut remplacer les banques ? Plutôt remplacer **certains** de leurs rôles.

Tous vos bitcoins à poil



Détails techniques

- Chacun signe ses transactions,
- Les transactions sont chaînées dans une structure de données publique, le **livre des opérations** (*blockchain*),
- Preuve de travail pour éviter l'attaque par déni de service contre le livre des opérations (il existe d'autres défenses),
- Vérification par tous les noœuds du réseau de l'intégrité du livre.

On n'est pas dans un monde idéal

- Taille des données et temps de calcul. On ne peut pas mettre le livre des opérations sur son *smartphone* !
- Pas mal de « clients légers » qui ne font pas les vérifications : ils font **confiance** (au moins, ils choisissent à qui).
- Passage à l'échelle. Bitcoin a moins d'une transaction/s, Visa en a des milliers.
- Logiciel unique : en cas de bogue ?

Tyrannie de la majorité

1. La majorité n'a pas forcément tous les droits. La transparence n'aide pas si les gens veulent fermer les yeux.
2. Bitcoin est vulnérable à l'« attaque des 51 % ». Si on a la majorité de la puissance de calcul, on contrôle le livre des opérations.
3. Twister (bien moins utilisé et donc bien plus vulnérable) a déjà fait l'objet d'une telle attaque le 18 janvier 2014
4. « L'honnêteté d'une masse indéfinie ? »

Le principe peut s'étendre à tout registre

- Il n'y a pas que le fric dans la vie : les principes de Bitcoin peuvent servir à bien autre chose.
- Twister (déjà cité) : *microblogging* avec identificateurs dans un livre des opérations public. Pas besoin d'un « silo », d'une « plateforme » pour contrôler nos identités.
- Namecoin : identificateurs uniques, parlants, sécurisés et sans aucun acteur privilégié.

Certificate Transparency

- But : lutter contre les faux certificats X.509 (Diginotar, Bercy. . .)
- Méthode : que les AC publient **tous** les certificats. Google pourra alors vérifier qu'il n'y a pas de faux certificat pour `gmail.com`
- Normalisation : RFC 6962
  `http://www.certificate-transparency.org/`
- Pas de preuve de travail donc, pour éviter la DoS, un acteur privilégié qui décide qui peut écrire (~ le choix par le navigateur des AC à mettre dans le magasin)

Tous à poil !

La transparence, une idée plus ancienne que l'informatique

Élections

Un processus transparent, contrôlable par tous

Sauf évidemment si on utilise les machines de vote, qui rendent tout opaque

Un exemple de vote complètement transparent

Usenet. . .

Vote non secret et où tout est public

`http://www.usenet-fr.net/fur/minis-faqs/vote.html`

Un dernier exemple de transparence

- Le protocole BGP est au cœur de l'Internet : il transmet les routes entre opérateurs.
- Tout routeur BGP voit toutes les annonces. Beaucoup le publient (RouteViews, RIS du RIPE, *looking glasses*. . .)
- N'importe qui peut donc voir, par exemple, que tel opérateur annonce des adresses IP qui ne lui appartiennent pas.
- Cette transparence contribue beaucoup à la résilience de l'Internet : pas de coup en traître dans le routage.

Vérification effective

- On peut appeler cela l'« effet HeartBleed ». Tout le monde pouvait vérifier OpenSSL. Personne (sauf la NSA ?) ne l'avait fait pendant deux ans.
- La solution n'est évidemment pas l'opacité, qui est bien pire.
- Mais il faut réfléchir à des mécanismes encourageant la vérification effective.
- Twister avait été piraté parce que très peu de gens avaient « donné » du temps de calcul pour les vérifications.

Vie privée

Donc, ton truc, c'est comme la NSA, on est à poil ?

Grosses différences : information (on sait que les données sont publiques) et symétrie (tout le monde a les mêmes informations).
Mais, évidemment, ce principe de la transparence n'est pas applicable aux données personnelles et/ou sensibles.
Pour Namecoin, c'est l'équivalent du whois public pour toutes les données, et avec historique.

Solutions pour la vie privée

- Bitcoin : adresses à usage unique,
- Bitcoin : systèmes de brouillage des transactions `http://bitcoinlaundry.com/`
- Bitcoin : trucs cryptographiques avancés `http://zerocash-project.org/`
- Namecoin : comme avec le whois de `.com` : mentir...
- Namecoin : des réflexions en cours `https://forum.namecoin.info/viewtopic.php?f=2&t=1694`

Conclusion

Un concept ancien, mais réactivé par des progrès récents, comme le livre des opérations Bitcoin

Une alternative aux systèmes centralisés. Mais qui n'est pas parfaite et ne convient pas à tous les cas.