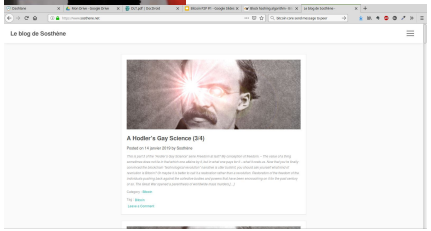
Bitcoin P2P

Wasabi Wallet

Pourquoi Wasabi ?

1. Une implémentation accessible de CoinJoin
2. Une interface pédagogique pour bien cerner les bonnes pratiques de confidentialité
3. L'occasion d'évoquer à nouveau les bases

www.sosthene.net
@Sosthene@bitcoinhackers.org



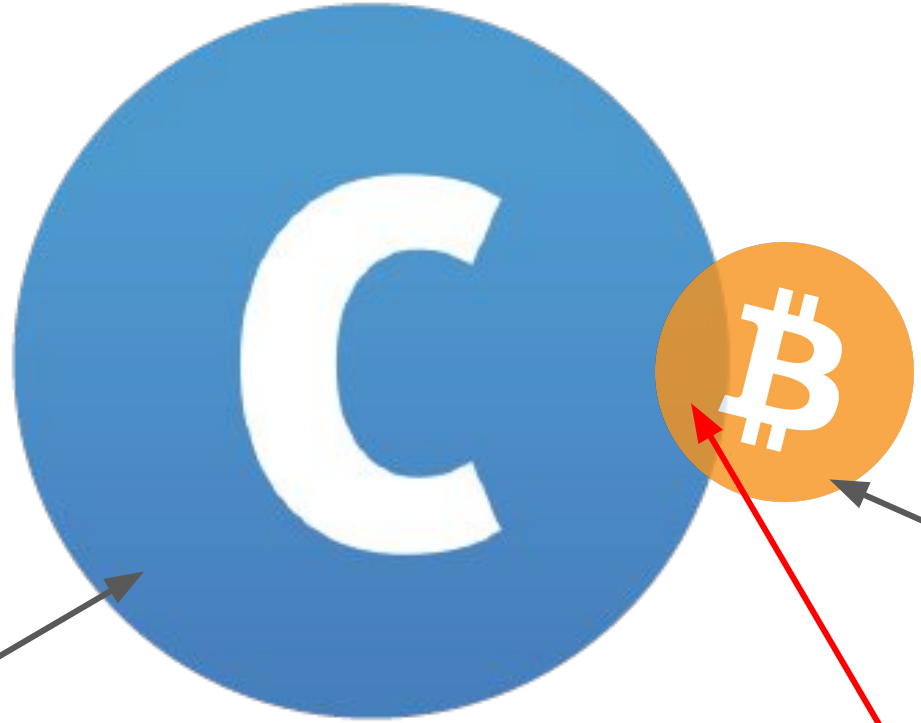
Le problème: anatomie d’une transaction

https://gist.github.com/BobleChinois/6d1541205c596936006cf6864cb2e25e

Le modèle de confidentialité de Bitcoin est certes très perfectible, mais pas aussi nul qu’on le dit souvent :

- Il n’y a aucun lien déterminé entre 2 adresses, même issues du même wallet
- Il n’y a aucun lien déterminé entre les inputs ou les outputs d’une transaction
- C’est un système pseudonyme qui garantit une confidentialité en fait plutôt correcte s’il est utilisé de façon intelligente
- Pour désanonymiser un utilisateur de Bitcoin, il est essentiel de pouvoir s’appuyer sur des éléments extérieurs à la blockchain

Le problème: *Data Fusion*



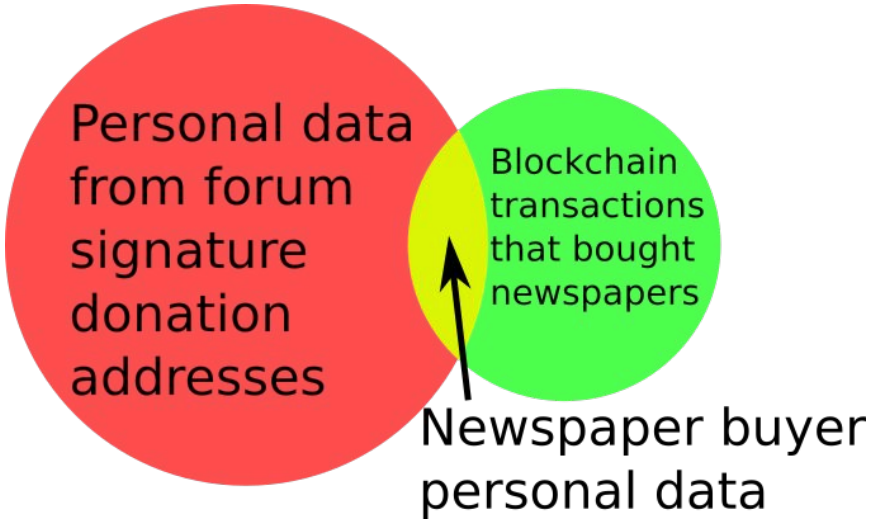
KYC/AML
Metadata
Trafic analysis
rattachent les
transactions à une
identité

Analyse de blockchain
crée des clusters de
transactions

REKT !

Exemple: rééducation d'un mal-pensant

- Alice met une adresse de donation en signature sur un forum
- Elle achète *La Grève* au marché noir avec la somme récoltée
- La police de la pensée examine la transaction, retrouve l'adresse de donation dans les outputs de la transaction précédente
- Par une simple recherche Google, l'adresse est retrouvée en signature de plusieurs centaines de posts sur un forum
- La police examine son profil/les metadata/contacte l'administrateur du forum pour l'identifier
- Alice est arrêtée et envoyée en camp de rééducation



Source : https://en.bitcoin.it/wiki/Privacy

Principales hypothèses

- **Common-input-ownership heuristic** : tous les inputs d'une transaction appartiennent à la même entité.
- **Change address detection** : parmi les outputs, l'un correspond à la "monnaie", et appartient à la même entité que les inputs.
- **Exact payment amount** : Si une transaction consomme l'intégralité d'un ou de plusieurs UTXO sans générer de monnaie, le destinataire du paiement est identique au payeur (paiement à soi-même).

Genèse: le post de G. Maxwell sur Bitcointalk

- Principe de base: dans une transaction bitcoin, les inputs peuvent être ajoutés par différentes entités indépendamment, et ensuite signés par tous.
- Si chacun apporte un ou plusieurs inputs et les outputs correspondants, un observateur extérieur ne peut pas relier un output à un input.
- Le protocole pourrait être décentralisé, mais fonctionne très bien de façon centralisée (le serveur ne peut pas voler les inputs)
- Avantages: simple, peu coûteux, complètement réalisable avec la façon dont Bitcoin fonctionne aujourd'hui
- Inconvénients: le serveur peut être un SPOF, consomme beaucoup de places sur la blockchain

(https://bitcointalk.org/index.php?topic=279249.0)

Problèmes pour implémenter CoinJoin

1. Les communications de tous les participants doivent passer exclusivement par un réseau anonymisé (typiquement, Tor).
2. Si un participant est désanonymisé, cela réduit le set d'anonymité de tous les autres.
3. Les montants des outputs doivent être les mêmes, sans quoi l'analyse des montants permet de les lier aux inputs.
4. Il faut que même le serveur ne puisse pas faire le lien entre les inputs et les outputs.
5. Comment coordonner un nombre suffisant d'utilisateurs qui ne se connaissent pas ?

Limites de Wasabi

- Le serveur reste un SPOF: on peut imaginer qu'un attaquant en prenne le contrôle et fournisse tous les participants d'un round auquel participe la cible, ce qui aura effectivement pour effet de réduire à néant son set d'anonymité
- Vous êtes dépendant des autres participants: s'ils se désanonymisent tous par la suite, votre anonymity set redevient effectivement "1"
- Les UTXO peuvent être désanonymisés si vous faites n'importe quoi avec
- Wasabi essaie de briser l'analyse de chaîne, mais ne peut rien contre les vecteurs d'attaque exogènes, il n'est efficace que si vous prenez d'autres mesures (ne pas utiliser de services imposant un KYC, bonne OPSEC, navigation internet avec Tor…)

Autres implémentations de CoinJoin

- JoinMarket : modèle plus décentralisé mais aussi moins intuitif avec des *makers* et des *takers* qui paient les premiers pour obtenir la liquidité nécessaire à un CoinJoin
- Coinshuffle++ : pas d'implémentation fonctionnelle (à ma connaissance)