Questions de sécurité de la chaîne de blocs

Stéphane Bortzmeyer
stephane@bortzmeyer.org

RéSIST, Toulouse, 6 décembre 2016

La chaîne de blocs

La chaîne de blocs

- Un livre des opérations, **public**, pair-à-pair, idéalement immuable, et sécurisé par la **cryptographie**

La chaîne de blocs

- Un livre des opérations, **public**, pair-à-pair, idéalement immuable, et sécurisé par la **cryptographie**
- Surtout connue par Bitcoin mais il existe des dizaines d'autres chaînes, très différentes, parfois spécialisées comme Namecoin pour les noms de domaine

La chaîne de blocs

- Un livre des opérations, **public**, pair-à-pair, idéalement immuable, et sécurisé par la **cryptographie**
- Surtout connue par Bitcoin mais il existe des dizaines d'autres chaînes
- De très nombreuses applications, pas seulement l'argent

La chaîne de blocs

- Un livre des opérations, **public**, pair-à-pair, idéalement immuable, et sécurisé par la **cryptographie**
- Surtout connue par Bitcoin mais il existe des dizaines d'autres chaînes
- De très nombreuses applications
- Protection contre les Sybils et les généraux byzantins par la **preuve de travail** ou la **preuve d'enjeu** (le pouvoir aux riches. . .)

La chaîne de blocs

- Un livre des opérations, **public**, pair-à-pair, idéalement immuable, et sécurisé par la **cryptographie**
- Surtout connue par Bitcoin mais il existe des dizaines d'autres chaînes
- De très nombreuses applications
- Protection contre les Sybils et les généraux byzantins par la **preuve de travail** ou la **preuve d'enjeu**
- Sécurité et confiance reposant sur le caractère **public** de la chaîne

Minage

Minage

- La preuve de travail demande. . . du travail (trouver un condensat inférieur à une certaine valeur)

Minage

- La preuve de travail demande. . . du travail
- Ce travail est fait par les **mineurs**

Minage

- La preuve de travail demande. . . du travail
- Ce travail est fait par les **mineurs**
- Chez Bitcoin, entreprises commerciales spécialisées et matériels spécialisés

Les dangers du bitcoin

LE SCAN > LES INSOLITES

Pour illustrer les dangers du «darknet», Bernard Debré se fait livrer de la drogue

Par Marc de Boni | Mis à jour le 29/06/2016 à 09:53 / Publié le 28/06/2016 à 17:03

Bernard Debré, député LR de Paris

200 commentaires

Ça attaque le cerveau. . .

Le portefeuille de M. Michu

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique** (avec courbes elliptiques),

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant
- Il faut donc prendre soin de la clé privée

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant
- Il faut donc prendre soin de la clé privée
- Deux risques : copie de la clé par un tiers, et perte de la clé

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant
- Il faut donc prendre soin de la clé privée
- Deux risques : copie de la clé par un tiers, et perte de la clé
- Premier cas : vous stockez votre clé sur une machine MS-Windows (donc infestée de logiciels malveillants)

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant
- Il faut donc prendre soin de la clé privée
- Deux risques : copie de la clé par un tiers, et perte de la clé
- Premier cas : vous stockez votre clé sur une machine MS-Windows
- Deuxième cas : le type qui jette par négligence son disque dur « contenant » 7 500 bitcoins

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant
- Il faut donc prendre soin de la clé privée
- Deux risques : copie de la clé par un tiers, et perte de la clé
- Premier cas : vous stockez votre clé sur une machine MS-Windows
- Deuxième cas : le type qui jette par négligence son disque dur
- Solutions pour le premier cas : stockage hors-ligne (« *cold storage* »), HSM, hygiène informatique

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant
- Il faut donc prendre soin de la clé privée
- Deux risques : copie de la clé par un tiers, et perte de la clé
- Premier cas : vous stockez votre clé sur une machine MS-Windows
- Deuxième cas : le type qui jette par négligence son disque dur
- Solutions pour le premier cas : stockage hors-ligne, HSM, hygiène informatique
- Solutions pour le deuxième cas : sauvegardes, *paper wallet*

Le portefeuille de M. Michu

- La chaîne utilise de la cryptographie **asymétrique**,
- La preuve que je détiens ces bitcoins, c'est que j'arrive à signer une transaction les dépensant
- Il faut donc prendre soin de la clé privée
- Deux risques : copie de la clé par un tiers, et perte de la clé
- Premier cas : vous stockez votre clé sur une machine MS-Windows
- Deuxième cas : le type qui jette par négligence son disque dur
- Solutions pour le premier cas : stockage hors-ligne, HSM, hygiène informatique
- Solutions pour le deuxième cas : sauvegardes, *paper wallet*
- Solutions dans les deux cas : **notariat**, un organisme de confiance qu'on choisit

La gestion de clés, c'est dur

[Extrait de la FAQ d'Electrum, un portefeuille Bitcoin] « *I have forgotten my password [...] Is there any way I can recover my password ?* » $\longrightarrow$ « *No, you cannot recover your password* »

La gestion de clés, c'est dur

[Extrait de la FAQ d'Electrum, un portefeuille Bitcoin] « *I have forgotten my password [...] Is there any way I can recover my password ?* » $\longrightarrow$ « *No, you cannot recover your password* »

- Mais n'est-ce pas pareil avec ma banque ?

La gestion de clés, c'est dur

[Extrait de la FAQ d'Electrum, un portefeuille Bitcoin] « *I have forgotten my password [...] Is there any way I can recover my password ?* » $\longrightarrow$ « *No, you cannot recover your password* »

- Mais n'est-ce pas pareil avec ma banque ?
- Non, car il y a un recours (venir AFK dans l'agence avec ses papiers)

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue
- Si on a 51 % de puissance de calcul, on décide quelle sera la plus longue

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue
- Si on a 51 % de puissance de calcul, on décide quelle sera la plus longue
- « Bitcoin est une hashocratie »

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue
- Si on a 51 % de puissance de calcul, on décide quelle sera la plus longue
- « Bitcoin est une hashocratie »
- Le problème est aggravé par la trop forte concentration des mineurs

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue
- Si on a 51 % de puissance de calcul, on décide quelle sera la plus longue
- « Bitcoin est une hashocratie »
- Le problème est aggravé par la trop forte concentration des mineurs

D'un autre côté :

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue
- Si on a 51 % de puissance de calcul, on décide quelle sera la plus longue
- « Bitcoin est une hashocratie »
- Le problème est aggravé par la trop forte concentration des mineurs

D'un autre côté :

- Grâce au caractère public de la chaîne, l'attaque se voit

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue
- Si on a 51 % de puissance de calcul, on décide quelle sera la plus longue
- « Bitcoin est une hashocratie »
- Le problème est aggravé par la trop forte concentration des mineurs

D'un autre côté :

- Grâce au caractère public de la chaîne, l'attaque se voit
- Elle entrainerait une scission définitive. Destructive, mais moins qu'une tricherie cachée.

L'attaque des 51 %

- En cas de bifurcation (deux chaînes apparaissent), que faire ?
- Les mineurs choisissent la chaîne la plus longue
- Si on a 51 % de puissance de calcul, on décide quelle sera la plus longue
- « Bitcoin est une hashocratie »
- Le problème est aggravé par la trop forte concentration des mineurs

D'un autre côté :

- Grâce au caractère public de la chaîne, l'attaque se voit
- Elle entrainerait une scission définitive. Destructive, mais moins qu'une tricherie cachée.
- Les chaînes plus petites que Bitcoin sont encore plus vulnérables

Bogue dans la chaîne

Bogue dans la chaîne

- Les logiciels ont des bogues

Bogue dans la chaîne

- Les logiciels ont des bogues
- Que faire si on détecte qu'une bogue a permis d'inscrire dans la chaîne ce qu'il n'aurait pas fallu ?

Bogue dans la chaîne

- Les logiciels ont des bogues
- Que faire si on détecte qu'une bogue a permis d'inscrire dans la chaîne ce qu'il n'aurait pas fallu ?
- Le cas s'est produit pour Bitcoin en 2010 (un bête *overflow*, 186 milliards de bitcoins « volés ») Il a fallu revenir en arrière et annuler des transactions

« Mon code n'a pas de bogues »

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme
- Dans Ethereum, ces programmes sont écrits dans un langage de Turing : tout est possible (donc, y compris écrire des bogues)

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme
- Dans Ethereum, ces programmes sont écrits dans un langage de Turing
- Que faire en cas de bogue ? Après tout, l'erreur n'est pas dans la chaîne. Intéressant problème de gouvernance

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme
- Dans Ethereum, ces programmes sont écrits dans un langage de Turing
- Que faire en cas de bogue ? Après tout, l'erreur n'est pas dans la chaîne.
- Les compilos aussi ont des bogues (faille Solidity/Ethereum du 1 novembre)

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme
- Dans Ethereum, ces programmes sont écrits dans un langage de Turing
- Que faire en cas de bogue ? Après tout, l'erreur n'est pas dans la chaîne.
- Les compilos aussi ont des bogues
- Exemple de The_DAO en 2016 (qui a mené à la scission entre Ethereum et Ethereum Classic)

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme
- Dans Ethereum, ces programmes sont écrits dans un langage de Turing
- Que faire en cas de bogue ? Après tout, l'erreur n'est pas dans la chaîne.
- Les compilos aussi ont des bogues
- Exemple de The_DAO en 2016
- Bien sûr des analyseurs statiques comme Oyente

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme
- Dans Ethereum, ces programmes sont écrits dans un langage de Turing
- Que faire en cas de bogue ? Après tout, l'erreur n'est pas dans la chaîne.
- Les compilos aussi ont des bogues
- Exemple de The_DAO en 2016
- Bien sûr des analyseurs statiques comme Oyente
- Demain, n'utiliser que des langages fonctionnels, et faire des preuves formelles ?

« Mon code n'a pas de bogues »

- Les transactions Bitcoin sont l'exécution d'un programme
- Dans Ethereum, ces programmes sont écrits dans un langage de Turing
- Que faire en cas de bogue ? Après tout, l'erreur n'est pas dans la chaîne.
- Les compilos aussi ont des bogues
- Exemple de The_DAO en 2016
- Bien sûr des analyseurs statiques comme Oyente
- Demain, n'utiliser que des langages fonctionnels, et faire des preuves formelles ?
- « Si le Web a survécu à PHP et JavaScript, Ethereum peut survivre aux bogues de The DAO »

Pièges du langage Solidity

Pièges du langage Solidity

- Les fonctions (comme `send`) peuvent échouer mais tester le code de retour n'est pas obligatoire

Pièges du langage Solidity

- Les fonctions (comme `send`) peuvent échouer mais tester le code de retour n'est pas obligatoire
- Un contrat (programme) peut en appeler un autre mais **c'est dans une autre transaction**

Pièges du langage Solidity

- Les fonctions (comme `send`) peuvent échouer mais tester le code de retour n'est pas obligatoire
- Un contrat peut en appeler un autre mais **c'est dans une autre transaction**
- Pas de distinction compte/contrat : on croit envoyer de l'argent à un compte, on appelle son code !

Pièges du langage Solidity

- Les fonctions (comme `send`) peuvent échouer mais tester le code de retour n'est pas obligatoire
- Un contrat peut en appeler un autre mais **c'est dans une autre transaction**
- Pas de distinction compte/contrat : on croit envoyer de l'argent à un compte, on appelle son code !
- Si votre fonction n'est pas **réentrante**, votre état peut changer pendant une transaction !

Une chaîne où rien n'est caché

Une chaîne où rien n'est caché

- Contrairement à ce que racontent certains médias, Bitcoin ne garantit pas votre anonymat

Une chaîne où rien n'est caché

- Bitcoin ne garantit pas votre anonymat
- Les adresses Bitcoin sont pseudonymes, pas anonymes (Forte traçabilité, nécessaire pour que la chaîne fonctionne)

Une chaîne où rien n'est caché

- Bitcoin ne garantit pas votre anonymat
- Les adresses Bitcoin sont pseudonymes, pas anonymes (Forte traçabilité, nécessaire pour que la chaîne fonctionne)
- Tout le monde peut voir toutes les transactions

Une chaîne où rien n'est caché

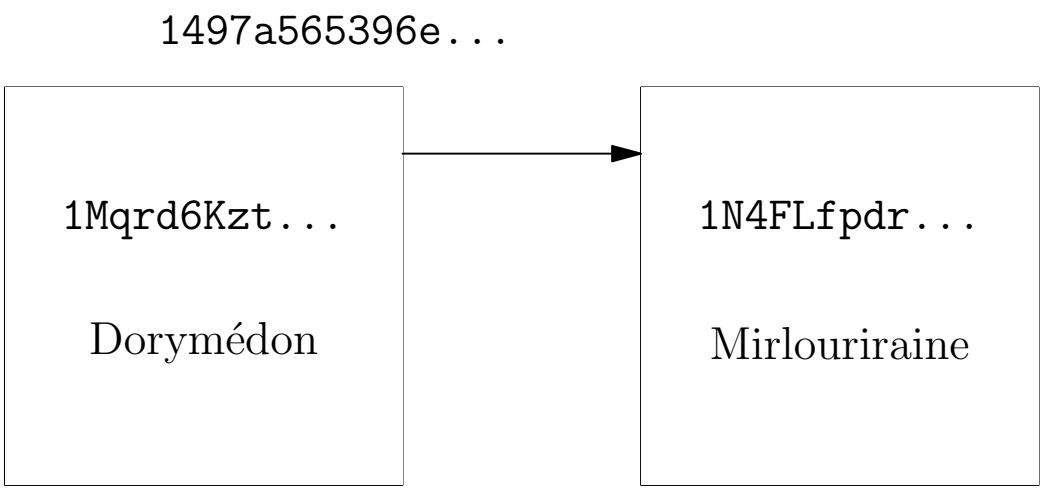
- Bitcoin ne garantit pas votre anonymat
- Les adresses Bitcoin sont pseudonymes, pas anonymes (Forte traçabilité, nécessaire pour que la chaîne fonctionne)
- Tout le monde peut voir toutes les transactions
- Solutions : les *mixers/tumblers* Bitcoin, des adresses à usage unique, ou bien des solutions comme Zcash

Une chaîne où rien n'est caché

- Bitcoin ne garantit pas votre anonymat
- Les adresses Bitcoin sont pseudonymes, pas anonymes (Forte traçabilité, nécessaire pour que la chaîne fonctionne)
- Tout le monde peut voir toutes les transactions
- Solutions : les *mixers/tumblers* Bitcoin, des adresses à usage unique, ou bien des solutions comme Zcash
- Ne mettez pas de données privées dans la chaîne (bogue du numéro de téléphone dans la chaîne, projets de votes éléctroniques stockés dans la chaîne)

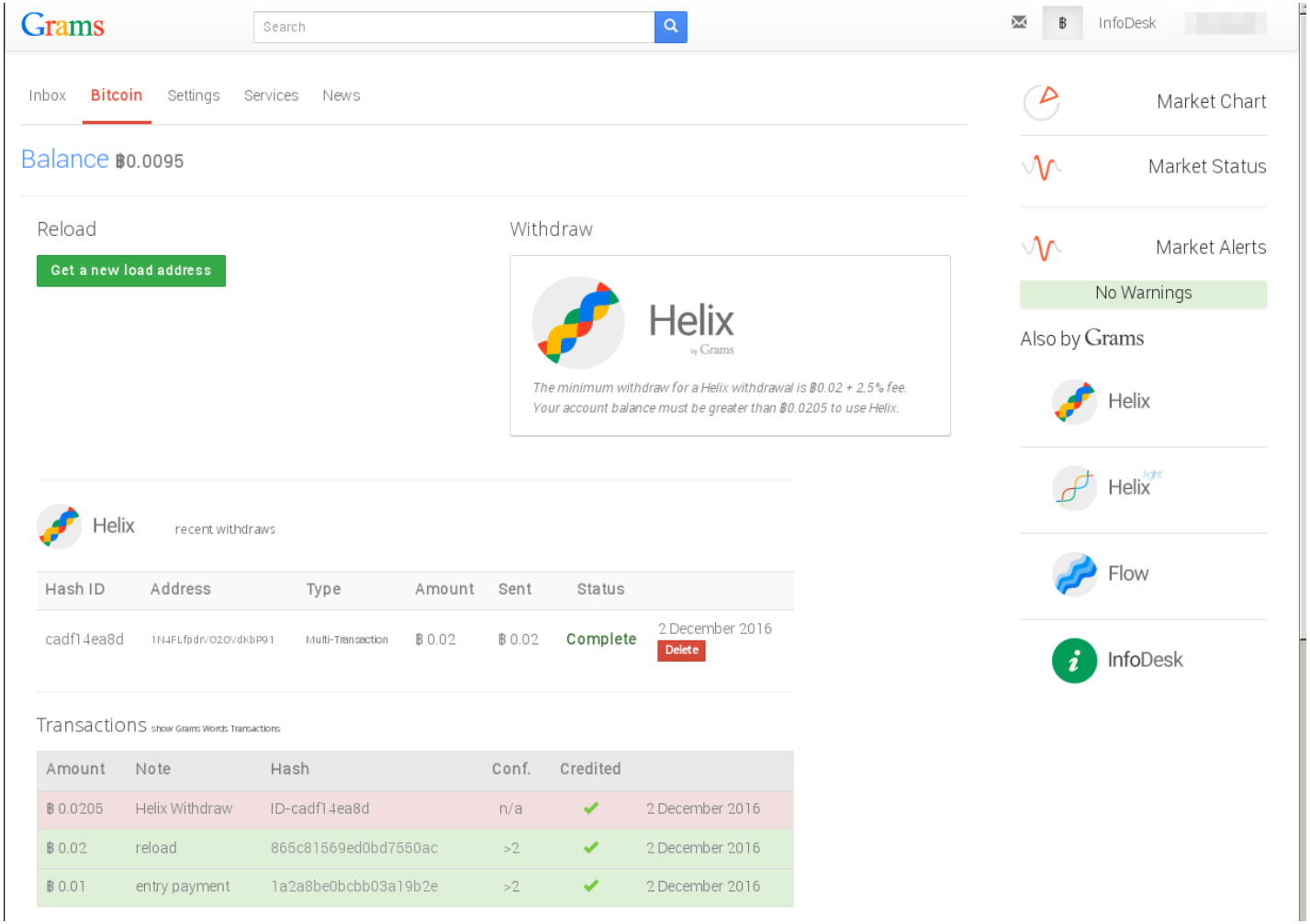
Exemple de transaction

Transfert direct. Bitcoin



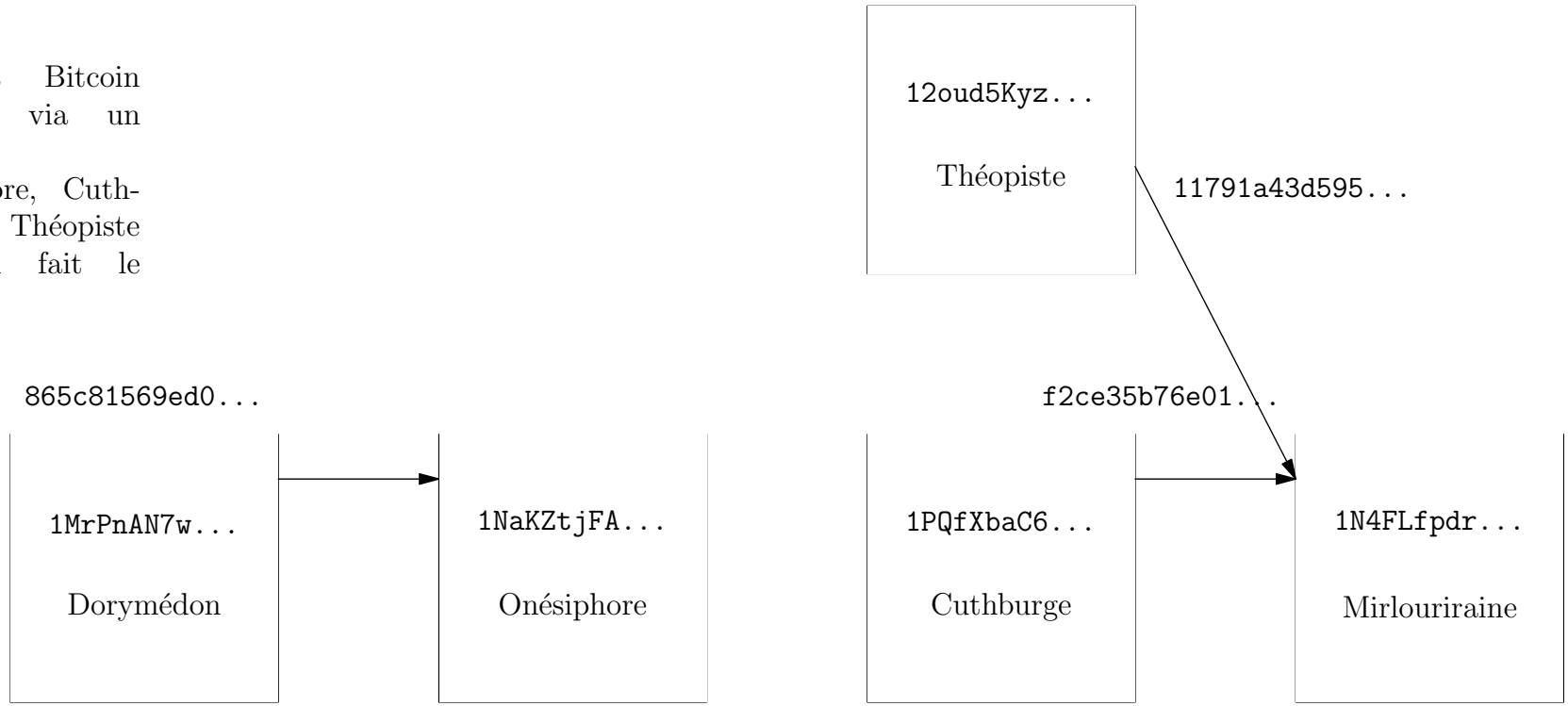
Transaction avec mixer

Grams / Helix `http://www.grams7enufi7jmdl.onion/`



Transfert indirect

Transfert Bitcoin indirect, via un mixer.
Onésiphore, Cuthburge et Théopiste sont en fait le mixer.



Les places de marché

Les places de marché

- Pour échanger contre des monnaies fiat, ou pour spéculer, ou encore pour garder son argent, certains mettent leur argent sur des places de marché comme Paymium ou Kraken

Les places de marché

- Certains mettent leur argent sur des places de marché
- Ces places ne sont **pas** la chaîne de blocs. Elles ressemblent plutôt à une banque (KYC, régulation, dépendance vis-à-vis d'un tiers. . .)

Les places de marché

- Certains mettent leur argent sur des places de marché
- Ces places ne sont **pas** la chaîne de blocs. Elles ressemblent plutôt à une banque
- Pas mal de bogues et de piratages dans le passé (MtGox)

Liberté, Immuabilité, Vie privée

Les trois grands défis de la sécurité de la chaîne de blocs pour les prochaines années

Liberté, Immuabilité, Vie privée

Les trois grands défis de la sécurité de la chaîne de blocs pour les prochaines années

- Liberté : est-ce que ça va rester pair-à-pair ou bien est-ce qu'on n'aura plus que des chaînes contrôlées ?

Liberté, Immuabilité, Vie privée

Les trois grands défis de la sécurité de la chaîne de blocs pour les prochaines années

- Liberté : est-ce que ça va rester pair-à-pair ou bien est-ce qu'on n'aura plus que des chaînes contrôlées ?
- Immuabilité : bien sûr, l'immuabilité totale est impossible. Mais est-ce qu'on va avoir certaines garanties ou bien une réécriture permanente de l'histoire ?

Liberté, Immuabilité, Vie privée

Les trois grands défis de la sécurité de la chaîne de blocs pour les prochaines années

- Liberté : est-ce que ça va rester pair-à-pair ou bien est-ce qu'on n'aura plus que des chaînes contrôlées ?
- Immuabilité : bien sûr, l'immuabilité totale est impossible. Mais est-ce qu'on va avoir certaines garanties ou bien une réécriture permanente de l'histoire ?
- Vie privée : va t-on voir la traçabilité prendre complètement le pas sur la vie privée ?