Investigation sur la chaîne de blocs

Stéphane Bortzmeyer

bortzmeyer@nic.fr

La chaîne de blocs

La chaîne de blocs

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

afnic

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

afnic

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

afnic

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 abus par la **preuve de travail** ou la **preuve d'enjeu** (le pouvoir aux riches. . .)

afnic

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 abus par la **preuve de travail** ou la **preuve d'enjeu**
- Sécurité et confiance reposant sur le caractère **public** de la chaîne

afnic

Utilisation par les délinquants

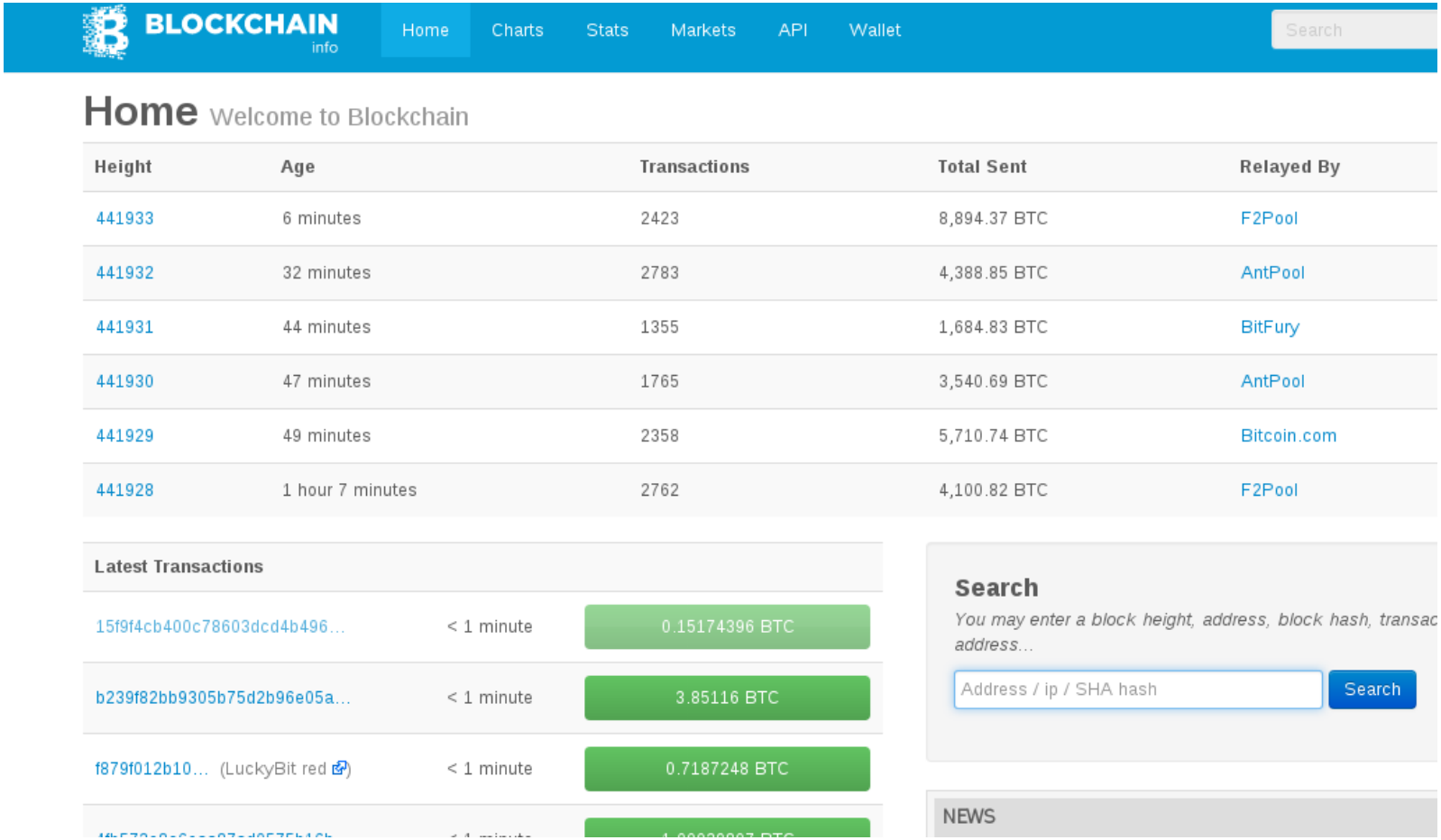
Ici un rançongiciel

Utilisations légales

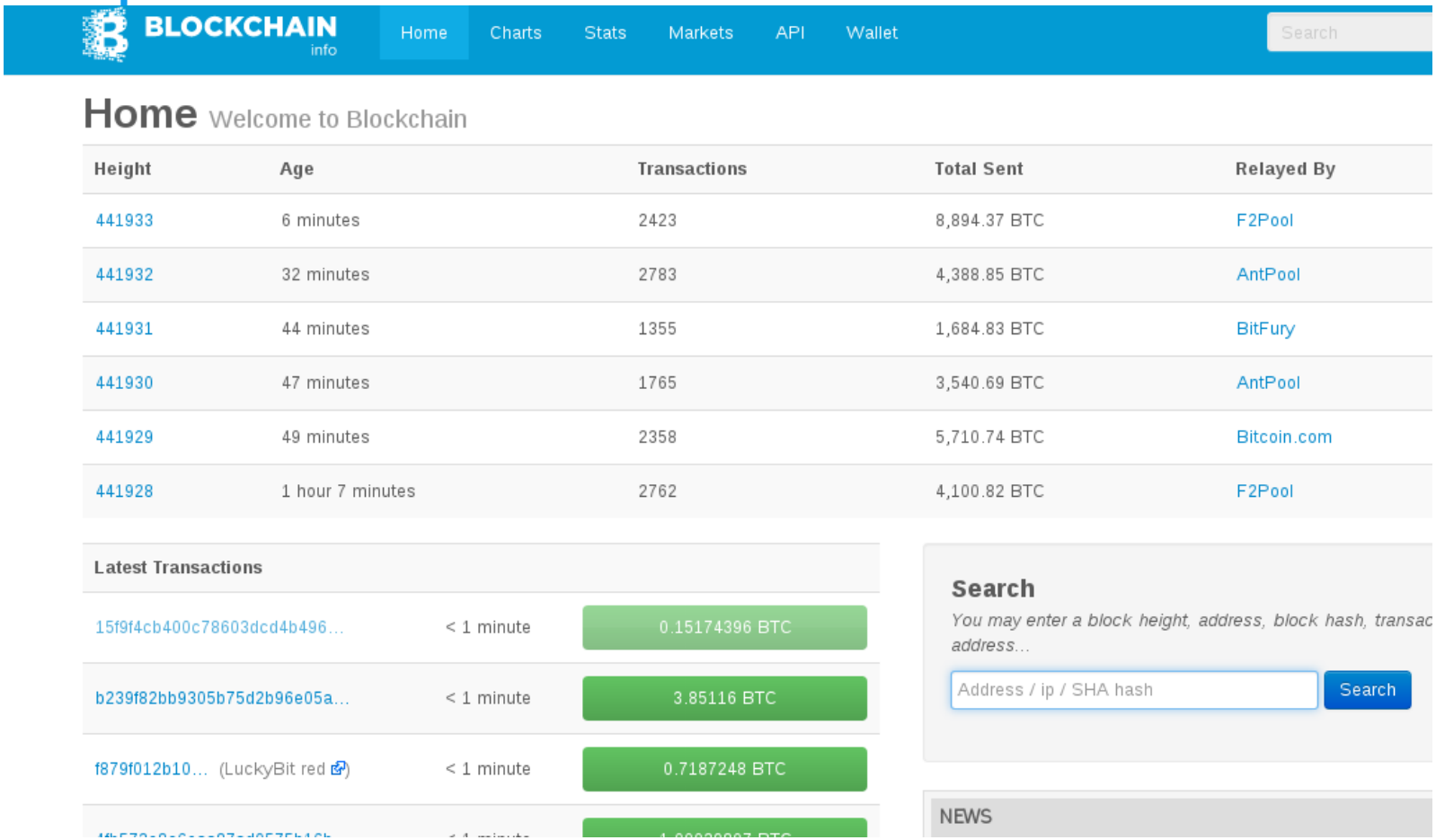
Utilisations légales

- Wikileaks (bloqué par Paypal)

Les explorateurs



Les explorateurs

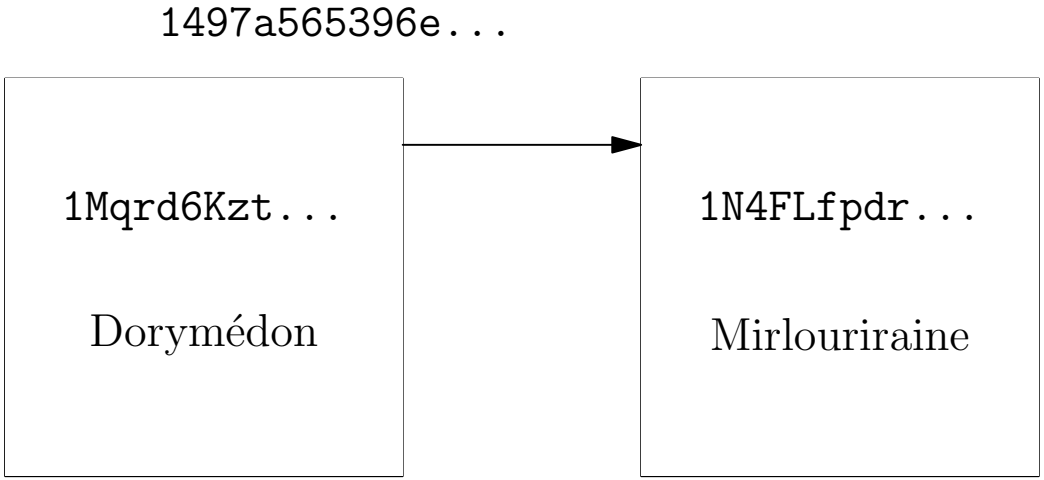


Attention, l'explorateur peut vous mentir (ou garder trace de vos requêtes) ! Utilisez plutôt un nœud complet local !

afnic

Exemple de transaction

Transfert direct. Bitcoin



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/blanchisseurs* Bitcoin, des adresses à usage unique, ou bien des chaînes plus perfectionnées

afnic

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/blanchisseurs* Bitcoin, des adresses à usage unique, ou bien des chaînes plus perfectionnées
- 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)

afnic

Et l'adresse IP ?

Et l'adresse IP ?

- Elle est celle du nœud voisin de l'explorateur, pas l'origine,

Et l'adresse IP ?

- Elle est celle du nœud voisin de l'explorateur, pas l'origine,
- Même si elle est l'origine, l'injecteur a pu passer par PushTx (ou Tor. . .)

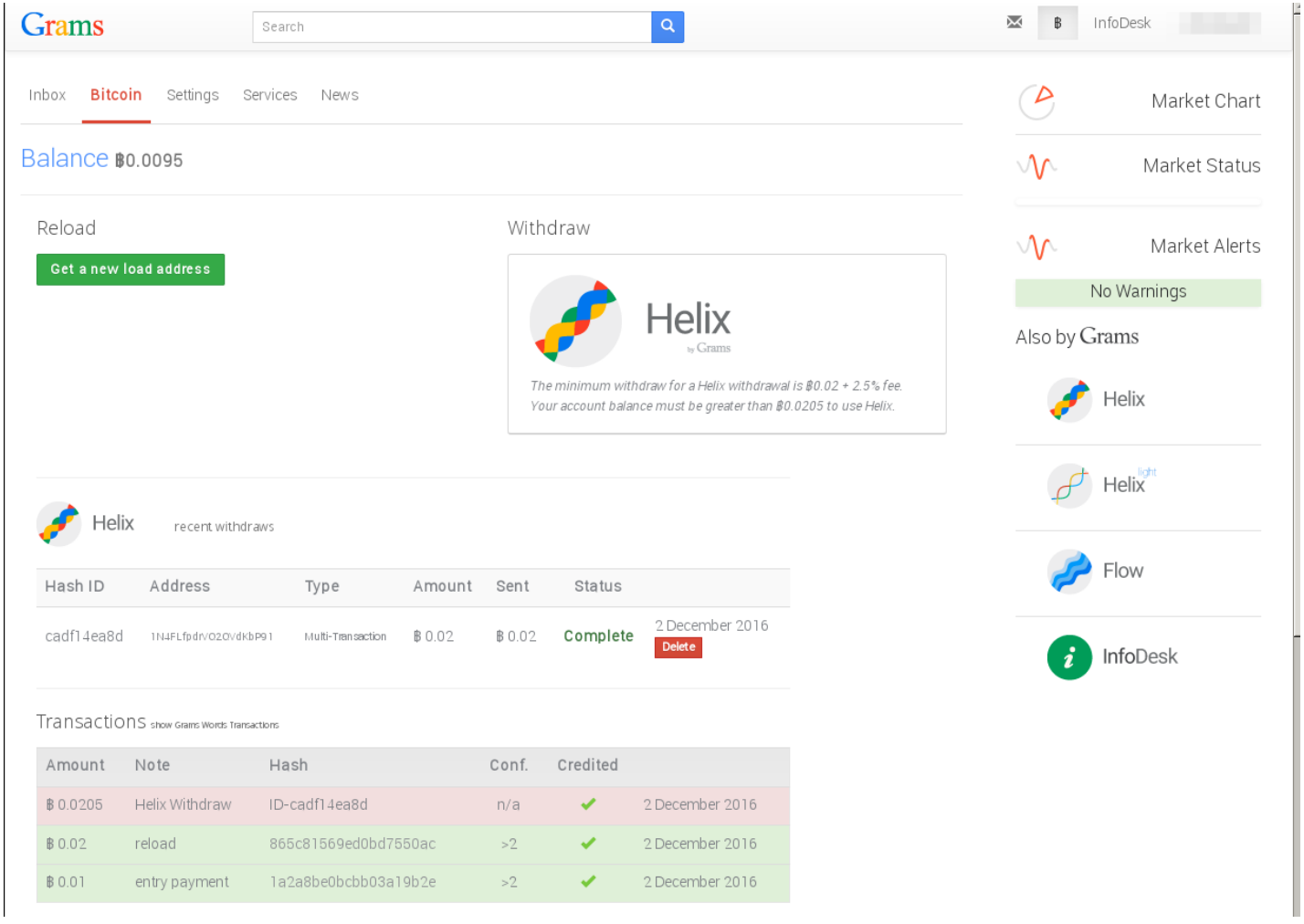
Et l'adresse IP ?

- Elle est celle du nœud voisin de l'explorateur, pas l'origine,
- Même si elle est l'origine, l'injecteur a pu passer par PushTx (ou Tor. . .)
- Et si l'attaquant contrôle beaucoup de nœuds ? (Attaque de Chainalysis)

afnic

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.

Autres mixers

Autres mixers

- BitMixer

Autres mixers

- BitMixer
- CoinMixer

Autres mixers

- BitMixer
- CoinMixer
- DarkLaunder

Autres mixers

- BitMixer
- CoinMixer
- DarkLaunder
- Peu ou pas de mixers pour Ethereum (un signe de non-succès ?)

Défaire les mixers ?

Défaire les mixers ?

- L'enchainement des transactions (le classique problème des métadonnées, un bon mixer doit ajouter des durées aléatoires),

Défaire les mixers ?

- L'enchainement des transactions,
- Les montants (un bon mixer brouille aussi cela),

Défaire les mixers ?

- L'enchainement des transactions,
- Les montants (un bon mixer brouille aussi cela),
- Méthodes *big data* sophistiquées (et pas publiées. . .),

afnic

Défaire les mixers ?

- L'enchainement des transactions,
- Les montants (un bon mixer brouille aussi cela),
- Méthodes *big data* sophistiquées,
- Beaucoup de mixers souffrent de leur activité trop faible (pas assez de bitcoins à brasser)

Les services d'investigation

- Quelques explorateurs publics comme Blockchain.info avec sa fonction *taint*

Les services d'investigation

- Quelques explorateurs publics comme Blockchain.info avec sa fonction *taint*
- Blockchain Inspector, ScoreChain, Chainalysis, Skry, Elliptic, BlockSeer, Elliptic...

Les services d'investigation

- Quelques explorateurs publics comme Blockchain.info avec sa fonction *taint*
- Blockchain Inspector, ScoreChain, Chainalysis, Skry, Elliptic, BlockSeer, Elliptic...
- Attention, comme les explorateurs, ils savent tout de votre investigation,

Les services d'investigation

- Quelques explorateurs publics comme Blockchain.info avec sa fonction *taint*
- Blockchain Inspector, ScoreChain, Chainalysis, Skry, Elliptic, BlockSeer, Elliptic...
- Attention, comme les explorateurs, ils savent tout de votre investigation,
- Logiciels fermés, preuves acceptables devant un tribunal ?

afnic

Les services d'investigation

- Quelques explorateurs publics comme Blockchain.info avec sa fonction *taint*
- Blockchain Inspector, ScoreChain, Chainalysis, Skry, Elliptic, BlockSeer, Elliptic...
- Attention, comme les explorateurs, ils savent tout de votre investigation,
- Logiciels fermés, preuves acceptables devant un tribunal ?
- Capacités exactes ? Beaucoup d'affirmations commerciales, quels résultats ? (Rarement des démos publiques.)

Défaire les investigateurs

Défaire les investigateurs

- Passer par plusieurs monnaies,

Défaire les investigateurs

- Passer par plusieurs monnaies,
- Des nouvelles chaînes comme Zcash, Dash ou Monero
  « *Confidential Transactions combine and utilize several cryptographic tricks, most notably Borromean ring signatures and Pedersen commitment schemes* »

afnic

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
- Peuvent aussi servir à casser la traçabilité

Les places de marché

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

afnic

Les places de marché

- Certains mettent leur argent sur des places de marché
- Peuvent aussi servir à casser la traçabilité
- 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)

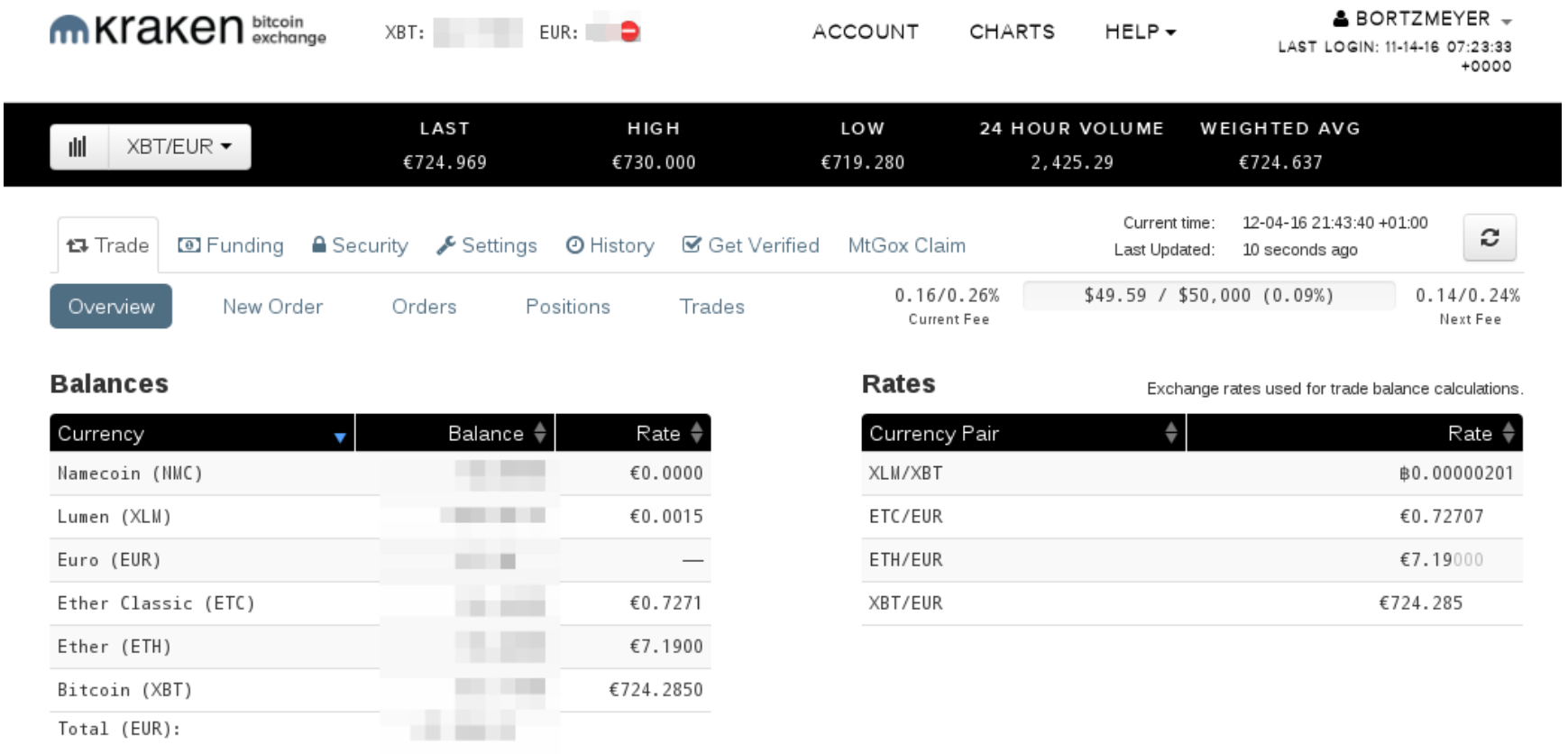
afnic

Les places de marché

- Certains mettent leur argent sur des places de marché
- Peuvent aussi servir à casser la traçabilité
- 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
- Action légale possible (arrestation d'un vendeur de drogue client de Paymium en décembre 2013, Coinbase forcé de donner son fichier au fisc en novembre 2016)

afnic

Kraken


kraken bitcoin exchange
XBT:
EUR:
ACCOUNT
CHARTS
HELP
BORTZMEYER
LAST LOGIN: 11-14-16 07:23:33 +0000
XBT/EUR
LAST
€724.969
HIGH
€730.000
LOW
€719.280
24 HOUR VOLUME
2,425.29
WEIGHTED AVG
€724.637
Trade
Funding
Security
Settings
History
Get Verified
MtGox Claim
Current time: 12-04-16 21:43:40 +01:00
Last Updated: 10 seconds ago
Overview
New Order
Orders
Positions
Trades
0.16/0.26%
Current Fee
$49.59 / $50,000 (0.09%)
0.14/0.24%
Next Fee
Balances
Currency
Balance
Rate
Namecoin (NMC)
€0.0000
Lumen (XLM)
€0.0015
Euro (EUR)
—
Ether Classic (ETC)
€0.7271
Ether (ETH)
€7.1900
Bitcoin (XBT)
€724.2850
Total (EUR):
Rates
Exchange rates used for trade balance calculations.
Currency Pair
Rate
XLM/XBT
฿0.00000201
ETC/EUR
€0.72707
ETH/EUR
€7.19000
XBT/EUR
€724.285

Une conclusion

Une conclusion

- Verra-t-on la victoire définitive des anonymiseurs ou bien celle des investigateurs ?

Une conclusion

- Verra-t-on la victoire définitive des anonymiseurs ou bien celle des investigateurs ?
- Plutôt une lutte éternelle.

Merci !

www.afnic.fr
contact@afnic.fr