

afnic

Investigation sur la chaîne de blocs

Stéphane Bortzmeyer

bortzmeyer@nic.fr

afnic

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

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

Utilisation par les délinquants

Ici un rançongiciel

Ransom ID 27843956. Your files are encrypted you must pay \$150 USD in Bitcoins to unlock them. Your software programs will not function properly.
If you try to delete this program you will loose all your files.
No matter what you do you. The files will remain encrypted until you pay.
If you need assistance in purchasing Bitcoins or unlocking your files.
send us a message thru the chat.
Visit: <http://76896.eu5.org/chat.html>
There is a file on your desktop named Payment_Instructions with the same information in case you try something funny and need our help getting your files back.
Every hour we will delete files until you pay. Depending on the amount of files your ransom can double to \$300 after 24 hours or triple to \$450 after 48 hours.
Instructions:
1. Go to www.LocalBitcoins.com, Register and purchase Bitcoins.
2. Copy the Bitcoins address below and send the coins to that address from your localbitcoins profile.
3. Click below that you paid.
4. Our system will recognize the payment instantly and unblock all your files.
If you try to tamper with this program all files you will loose yout files your computer you run the risk five. If you need help contact us thru the chat...

58:53

3 files will be deleted.

View encrypted files

Send \$150 worth of Bitcoin here!

1EYc872qXXMgS1EG3koSp5urMBWygGjA

I made a payment, now give me back my files!

1. Go to www.LocalBitcoins.com. Register and purchase coins.
2. Send coins to the address specified on the left.
3. Click the confirm button to confirm you paid.
4. Files are unlocked instantly.

Utilisations légales

Utilisations légales

- Wikileaks (bloqué par Paypal)

Les explorateurs



BLOCKCHAIN
info

Home

Charts

Stats

Markets

API

Wallet

Search

Home Welcome to Blockchain

Height	Age	Transactions	Total Sent	Relayed By
441933	6 minutes	2423	8,894.37 BTC	F2Pool
441932	32 minutes	2783	4,388.85 BTC	AntPool
441931	44 minutes	1355	1,684.83 BTC	BitFury
441930	47 minutes	1765	3,540.69 BTC	AntPool
441929	49 minutes	2358	5,710.74 BTC	Bitcoin.com
441928	1 hour 7 minutes	2762	4,100.82 BTC	F2Pool

Latest Transactions

15f9f4cb400c78603dcd4b496...	< 1 minute	0.15174396 BTC
b239f82bb9305b75d2b96e05a...	< 1 minute	3.85116 BTC
f879f012b10... (LuckyBit red )	< 1 minute	0.7187248 BTC
4e772c2c...	< 1 minute	1.0000000 BTC

Search

You may enter a block height, address, block hash, transaction address...

NEWS

6 / 18

Les explorateurs

 **BLOCKCHAIN**
info

Home Charts Stats Markets API Wallet

Search

Home Welcome to Blockchain

Height	Age	Transactions	Total Sent	Relayed By
441933	6 minutes	2423	8,894.37 BTC	F2Pool
441932	32 minutes	2783	4,388.85 BTC	AntPool
441931	44 minutes	1355	1,684.83 BTC	BitFury
441930	47 minutes	1765	3,540.69 BTC	AntPool
441929	49 minutes	2358	5,710.74 BTC	Bitcoin.com
441928	1 hour 7 minutes	2762	4,100.82 BTC	F2Pool

Latest Transactions

15f9f4cb400c78603dc4b496...	< 1 minute	0.15174396 BTC
b239f82bb9305b75d2b96e05a...	< 1 minute	3.85116 BTC
f879f012b10... (LuckyBit red ⚡)	< 1 minute	0.7187248 BTC
...	< 1 minute	...

Search

You may enter a block height, address, block hash, transaction address...

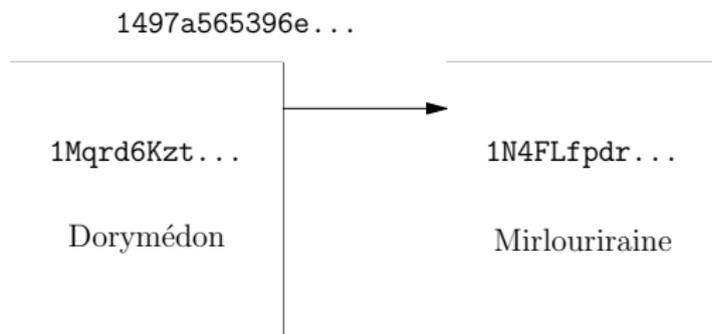
NEWS

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



Exemple de transaction

Transfert Bitcoin
direct.



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

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 électroniques stockés dans la chaîne)

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)

Transaction avec mixer

Grams / Helix <http://www.grams7enufi7jmdl.onion/>

The screenshot shows the Grams Helix web interface. At the top, there is a search bar and navigation links for 'Inbox', 'Bitcoin', 'Settings', 'Services', and 'News'. The main content area displays the user's 'Balance' as 0.0095. Below this, there are sections for 'Reload' (with a 'Get a new load address' button) and 'Withdraw' (featuring the Helix logo and a warning that the minimum withdrawal is 0.02 with a 2.5% fee). A 'recent withdraws' section contains a table with one entry: a complete transaction of 0.02 sent to address 114P... on December 2, 2016. A 'Transactions' section at the bottom shows a list of recent transactions, including a Helix withdrawal, a reload, and an entry payment, all dated December 2, 2016. On the right side, there are widgets for 'Market Chart', 'Market Status', 'Market Alerts', 'No Warnings', and 'Also by Grams' (listing Helix, Helix, Flow, and InfoDesk).

Balance $\text{\$}0.0095$

Reload

Get a new load address

Withdraw

Helix
by Grams

The minimum withdraw for a Helix withdraw is $\text{\$}0.02 + 2.5\%$ fee
Your account balance must be greater than $\text{\$}0.0205$ to use Helix.

recent withdraws

Hash ID	Address	Type	Amount	Sent	Status	
cadf14ea8d	114P...02D...043P61	Helix-Transaction	$\text{\$}0.02$	$\text{\$}0.02$	Complete	2 December 2016

Transactions show latest most transactions

Amount	Note	Hash	Conf.	Credited	
$\text{\$}0.0205$	Helix Withdraw	ID-cadf14ea8d	n/a	✓	2 December 2016
$\text{\$}0.02$	reload	865c81569ed0bd7550ac	>2	✓	2 December 2016
$\text{\$}0.01$	entry payment	1a2a8be0cb03a19b2e	>2	✓	2 December 2016

Market Chart

Market Status

Market Alerts

No Warnings

Also by Grams

Helix

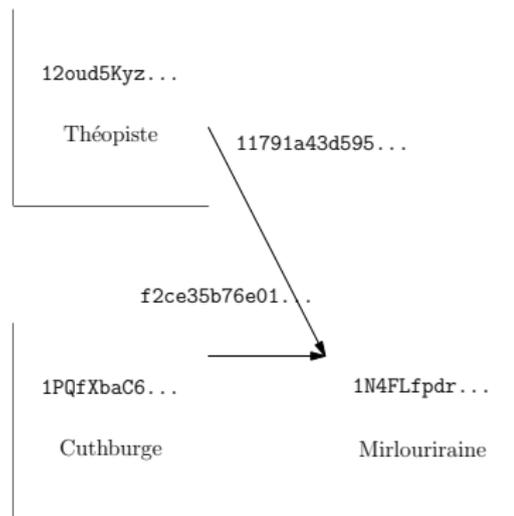
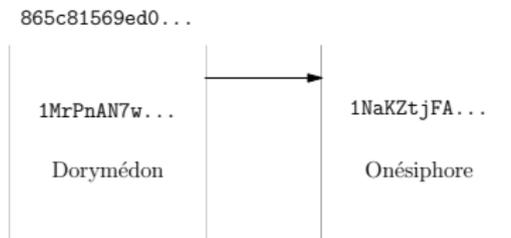
Helix

Flow

InfoDesk

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

Défaire les mixers ?

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

Défaire les mixers ?

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

Défaire les mixers ?

- L'enchaînement 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 ?

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 investisseurs

Défaire les investisseurs

- 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* »

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. . .)

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)

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)

XBT/EUR ▾	LAST	HIGH	LOW	24 HOUR VOLUME	WEIGHTED AVG
	€724.969	€730.000	€719.280	2,425.29	€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 ↕
XLN/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 !

afnic

www.afnic.fr
contact@afnic.fr

afnic