Vie privée

Telle est ma devise

Qui suis-je ?

Pierre-Yves Lapersonne
développeur logiciel

pylapersonne.info

LIBRE EN FÊTE

Code d'Armor

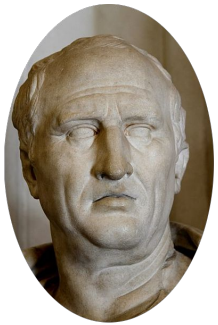
Au cas où...


LIBRE EN FÊTE
Si j'avais un bitcoin...
Cryptomonnaies, mode d'emploi en 20'


Code d'Armor
la révolution des blockchains
"La 2ème révolution numérique"


Code d'Armor
Đapps
on Ethereum with Solidity

“L’argent, c’est le nerf de la guerre :)



Cicéron, gagnant au loto

“T’as raison, mais avec des données personnelles, c’est vachement mieux (>_<)”

Ma banque, gagnant un client

Si quelqu’un regarde vos transactions bancaires via vos relevés, que sait-il de vous ?

Prenons Alice

Une personne standard, vivant une vie standard, utilisant une carte bleue standard, provenant d'une **banque** standard.

Une journée d'Alice...

- **7h30**
  Achat du p'tit déj via CB sans contact
- **8h00**
  Plein de carburant de la voiture via CB
- **12h30**
  Recharge de la carte pour la cantine via CB
- **18h00**
  Faire les courses de la semaine avec sa CB
- **19h00**
  Séance SPA entre copines par CB
- **20h30**
  Restau Thaï et cinéma par CB

… ses habitudes et fins de mois.

- Paiement du loyer par virement
- Prélèvements pour les charges
- Remboursements de frais médicaux par virements
- Don à *Sea Shepherd* via *Paypal*
- Cotisation au *Parti Pirate* via *Paypal*
- Cagnotte *Leetchi* pour le pôt de départ de François (un beau costume) par CB

Que sait-on d’Alice finalement ?

Corrélations transactions → vie privée

- Rythme de vie
(routine, horaires, déplacements ...)

- **Habitudes** de consommation
(boulangerie X, restaurant Y, ...)

- Bassin de vie
(travail, habitation, loisirs, ...)

Corrélations transactions → vie privée

- Pouvoir d'achat
  (revenus, charges, équipement, actes d'achat…)
- Santé financière
- **Données sensibles** au sens de la CNIL
  (santé, politique, militantisme, religion, …)
- Et d'autres **choses personnelles voire privées** !

Peut-on réaliser des transactions sans informer de ses actions d’illustres inconnus ?

Prenons Ada

Une personne bizarre qui utilise des **cryptomonnaies**, pour faire des transactions, utilisant :

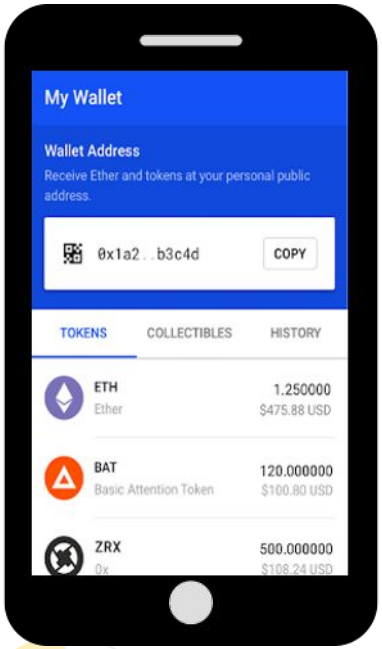
- un porte-monnaie électronique
- une plateforme d'échange
- un smartphone, ordinateur, ...

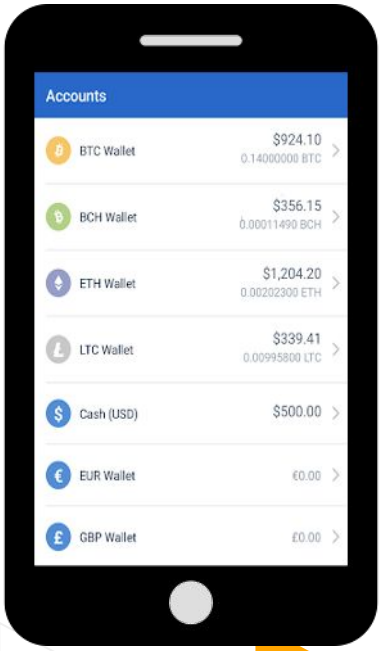
Une cryptomonnaie est une monnaie alternative dont les unités sont généralement libérées via des transactions enregistrées dans un registre après l'obtention d'un consensus.

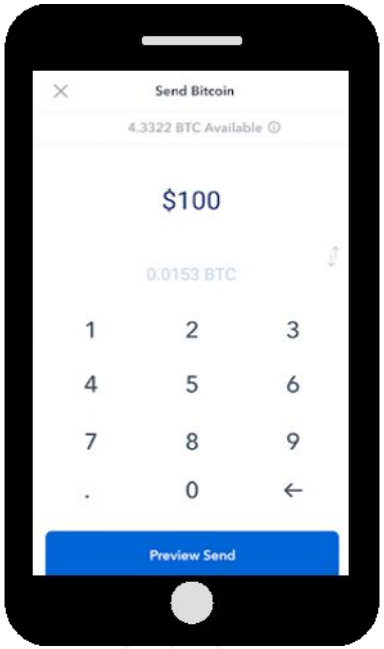
Ce registre est le plus souvent décentralisé, libre, non régulé et infalsifiable.

Il peut s'agir entre autres d'une blockchain.

Un porte-monnaie électronique ?

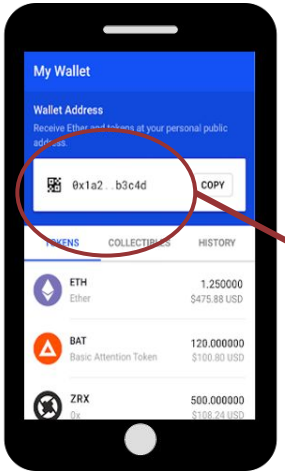






Pour être débité et crédité en (crypto)monnaie !

0,015 BTC



1ABMsSSBvn
BHUXfPLzh6
6hao9HUGaf
woAL

3QQp6i6PwY
7gRv4Q2K3f
8dLvbjwSS6
CREk

100 $ = 0,015 BTC
+TxFees

1 USD = 0,00015 BTC au 14/10/2018

En faisant des transactions.

Destinataire

1ABMsSSBvn
BHUXfPLzh6
6hao9HUGaf
woAL

Adresse

Somme envoyée : 0,015 BTC
Frais de transactions : x BTC
...

Contenu utile

Emetteur

3QQp6i6PwY
7gRv4Q2K3f
8dLvbjwSS6
CREk

Adresse

Zcash

Adoubée par Edward Snowden

ZCash

- Lancée le 28 octobre 2016
- Créée par Zooko Wilcox-O'Hearn

"Zcash's privacy tech makes it the most interesting Bitcoin alternative. Bitcoin is great, but '*if it's not private, it's not safe*.'"

Tweet de Edward Snowden

Quelques chiffres

- Quantité limitée à 21 millions d'unités
- 5 010 363 ZEC sortis
- **1 ZEC = 110,43 USD = 95,40 EUR**
- 133 transactions par heure (moyenne)
- 0,000018 USD de frais de transaction (moyenne)
- Récompense de 12,50 ZEC pour 1 bloc miné

D'après BitInfoCharts le 14/10/2018

Quelques détails techniques

- **Blockchain publique**
- Blockchain pesant 19,71 Go
- 2’29’’ pour miner un bloc
- 1,887 GHash par seconde
- Consensus par *Proof Of Work* avec *Equihash*

D’après BitInfoCharts le 14/10/2018

Quelques outils

- La page BitInfoCarts
- Un explorateur de blockchain
- Le site web
- Le code source

Quels avantages ?

- Adresses transparentes (*t-addr*), et protégées où les détails des transactions sont masqués (***z-addr***)

- Utilisation de ***zk-SNARK*** comme *(Non Interactive) Zero Knowledge Proof* pour blinder les *z-addr*

- *t-addr* et *z-addr* compatibles entre elles

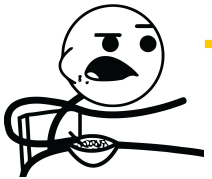
Quels inconvénients ?

- Pour un anonymat total, les deux parties doivent utiliser des *z-addr*, ce qui est encore assez rare
- Les *z-addr* sont **assez peu utilisées** et prises en charge dans les porte-monnaie électroniques
- L'utilisation de ZK-SNARK est coûteuse en ressources (mais mise en place de *Sapling*)

ZcashSapling

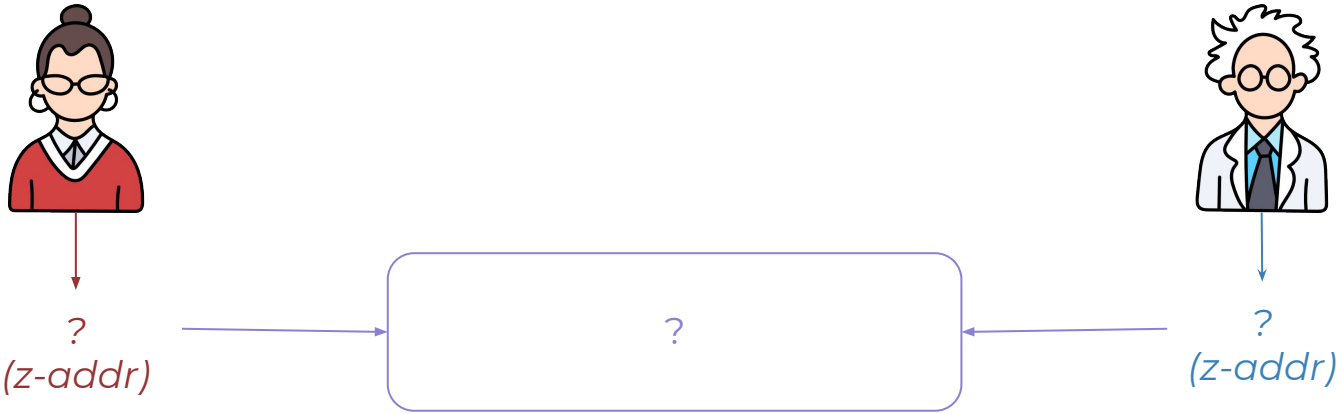
Quels inconvénients ?

- Projet géré par une entreprise (Zerocoin Electric Coin Company)
- 10% des 21 millions unités de ZEC sont donnés aux fondateurs et développeurs du projet



→ **Y a -t-il un risque** de porte dérobée ou de gestion opaque de la cryptomonnaie ?

Exemple idéal de transaction ZCash : rien n'est visible



Monero

La p’tite devise qui monte

Monero

- Lancée le 18 avril 2014
- Créée par Nicolas van Saberhagen
- Anonymat de **bout en bout** !
- Connue dans les médias à cause de Coinhive et WannaCry entre autres

Quelques chiffres

- Quantité illimitée d'unités
- 16 489 965 XMR sortis
- **1 XMR = 107,08 USD = 92,08 EUR**
- 146 transactions par heure (moyenne)
- 0,5 USD de frais de transaction (moyenne)
- Récompense de 3,73 XMR pour 1 bloc miné

D'après BitInfoCharts le 15/10/2018

Quelques détails techniques

- **Blockchain publique**
- Blockchain pesant 62,52 Go
- 2’7’’ pour miner un bloc
- 594 MHash par seconde
- Consensus par *Proof Of Work* avec *CryptoNight*

D’après BitInfoCharts le 14/10/2018

Quelques outils

- La page BitInfoCarts
- Un explorateur de blockchain
- Un autre explorateur
- Le site web
- Le code source

Quels avantages ?

- L'adresse de l'émetteur est **masquée** (Ring Signatures)
- L'adresse du receveur est **masquée** (Stealth Addresses)
- Le montant de la transaction est **masqué** (Ring Confidential Transactions)

Quels avantages ?

- La diffusion de la transaction est **protégée** (Kovri)

- Les balances de Monero ne sont pas associées aux adresses publiques (contrairement à ZCash, Bitcoin, Ethereum, ...)

Quels avantages ?

- Monero est maintenue par une **communauté** de développeurs bénévoles

- Communauté plus active et plus grande que celle de ZCash

Quels inconvénients ?

- Pas encore assez adopté
- Une grosse partie des transactions sont centralisées dans quelques *pools* de minage
- Maintenu par des développeurs **financés uniquement par des dons**, Monero peut sombrer…

Exemple de transaction Monero : on voit rien non plus

(Ring Confidential Transaction)

?

?

?

(Stealth address)

(Ring signatures)

(+ notification de la transaction à la blockchain via Kovri)

Et donc… ?

Un potentiel de dingue !

Emmanuel M.

La route est longue...

- Les cryptomonnaies permettent les **micro-paiements** avec une précision très fine !
- Certaines devises protègent les transactions et la **vie privée** de ceux qui les réalisent, grâce à des **concepts cryptographiques complexes**.
- Pas (encore) de solution parfaite, mais **Monero se démarque de ZCash**.

… et la voie est semée d'embûches.

- Les états **bannissent** les cryptomonnaies ou imposent des cadres juridiques **contraignants**.

- Les usages du **dark net**, la **spéculation** et l'**appât du gain** occultent les réels avantages de ce type de monnaie alternative.

Merci !

Références

- Anatomy of a Zcash Transaction, z.cash
- CryptoCompare, cryptocompare.com
- CryptoNight vs. EquiHash, minergate.com
- CryptoNote, cryptonote.org
- Kovri, getkovri.org
- Monero - An Anonymous CryptoCurrency, Medium
- Monero vs. Zcash and the Race to Anonymity, Medium
- On the linkability of Zcash transactions, jeffq.com
- Payment Contexts & Reusing Shielded Addresses, z.cash
- Ring Confidential Transactions, lab.getmonero.org
- Ring Signatures And Anomysation, Medium
- Sapling, z.cash
- When I say mine you say Conhive, Medium
- You can link Monero Transactions [...], coindesk.com
- Zcash Protocol Specification, Github
- Zk-SNARKs: Under the Hood, Medium

Sites visités le 14/10/2018

Crédits

- Debit card free icon par **monkik** sous *Flaticon Basic License*
- Qr Code free icon par **Vaadin** sous *Creative Commons With Attribution 3.0*
- Question Mark Button free icon par **Bogdan Rosu** sous *Creative Commons with Attribution 3.0*
- Scientist free icon par **Freepik** sous *Flaticon Basic License*
- Singapura free icon par **Freepik** sous *Flaticon Basic License*
- Troll Face Png Available In Different Size, freeiconspng.com
- Icon Download Troll Face, freeiconspng.com
- Woman free icon par **Freepik** sous *Flaticon Basic License*
- Photo de **An Min** sous *Creative Commons Zero*
- Photo sous *Creative Commons Zero*
- Photo du buste de Cicéron de **José Luiz Bernardes Ribeiro** sous *Creative Commons With Attribution with Share Alike 4.0*
- Logo de Monero dans le domaine public
- Logo de WannaCry, Bob McKay
- Logo de ZCash dans le domaine public
- Caneva de présentation par **Jayden Smith** sous *Creative Commons with Attribution*
- Captures d'écran éhontément prises des pages *Google Play* de Coinbase Wallet et Coinbase