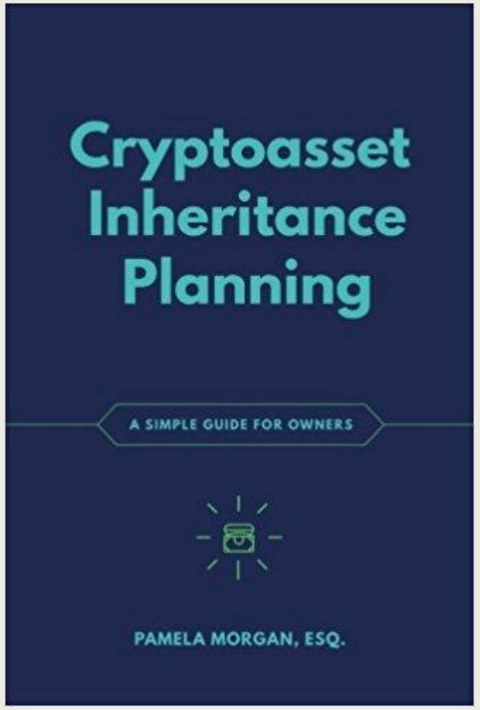
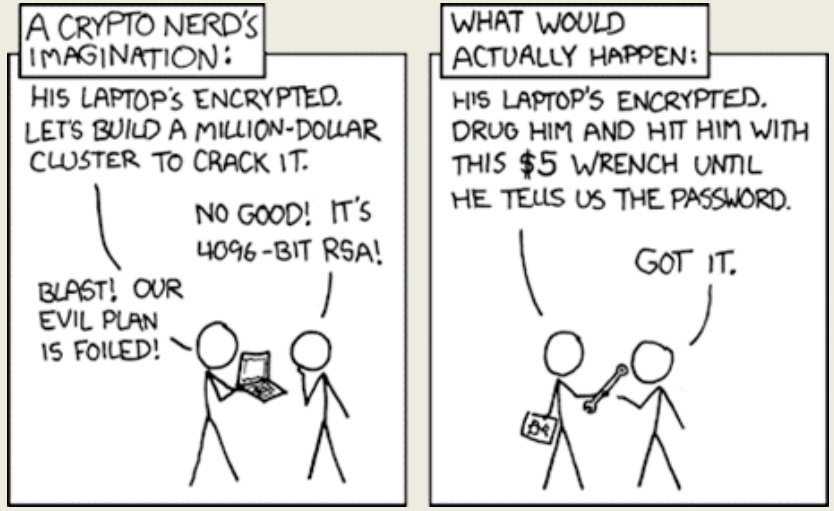
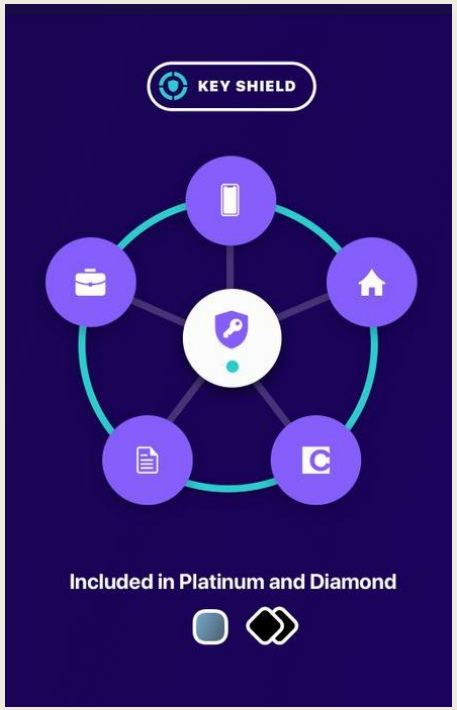
Le Terrier du Bitcoin
Découvre Bitcoin

Quel niveau de sécurité vous faut-il ?

LVL 3.2 BRH – Par Rogzy





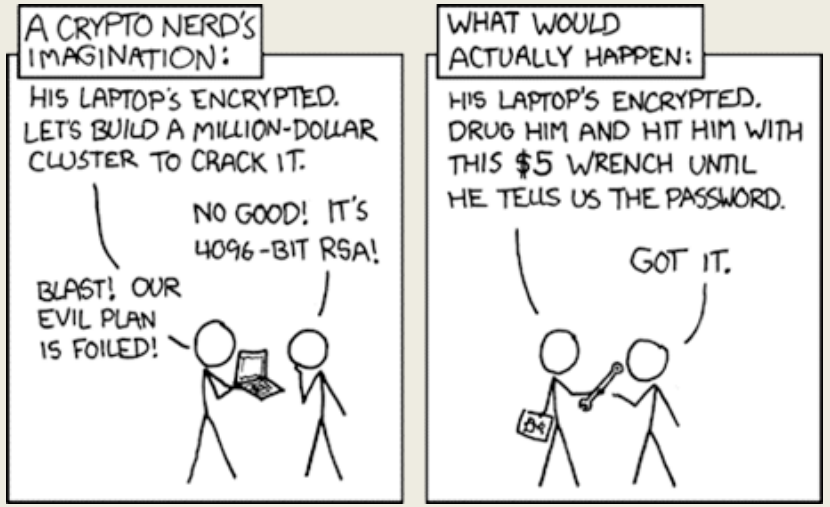


(Spoiler) Vous devrez décider vous-même!

Chaque personne est différente, vous devez donc choisir la solution la mieux adaptée à votre situation. Il y a principalement 3 facteurs à prendre en considération :

- La menace potentielle à laquelle vous êtes confronté.
- Votre mode de vie et vos connaissances en matière de sécurité
- La quantité de bitcoins que vous possédez.

Une fois que c'est fait, nous pouvons décider quelle solution de sécurité est la meilleure pour nous.



Possible attaque

- Hack
- Attaque physique
- Vol
- Catastrophe
- Confiscation gouvernemental
- Amnésie

La mauvaise gestion de la clé privé reste la 1er cause de perte….

+

Mode de vie

- Heure
- Connaissances
- Famille
- Niveau de paranoïa
- Equilibre de vie
- Fréquence d'utilisation
- Utilisation du portefeuille

+

Utilisation des Bitcoins

- Café
- Salaire
- Epargne
- Investissement
- Retraite
- Tout l'ensemble

=

Solution de stockage

- Dépôt
- Portefeuille électronique
- Portefeuille papier
- Brain wallet
- Portefeuille physique (HW)
- HW + passphrase
- Multi-signatures 2/3
- Portefeuille sans clé privé
- Portefeuille de sa propre fabrication

Où vous ne devez PAS stocker vos bitcoins :

- Services de dépôt : ❌

Vous n'êtes PAS responsable de votre clé privée. Par conséquent, vous ne possédez PAS vos bitcoins ; c'est la banque qui en est propriétaire. C'est très risqué (piratage, gel du gouvernement, escroquerie à la sortie) et doit être évité. Si vous achetez vos bitcoin depuis une plateforme d'échange, vous devez bouger les fonds dès que possible.

- Portefeuille électronique : ❌

Bien que très pratique pour les dépenses quotidiennes, ce n'est pas une solution pour le stockage à long terme.

En général, il s'agit d'un portefeuille chaud, ce qui signifie qu'il est connecté à l'internet et qu'il peut donc être piraté. Egalement, comme votre téléphone est généralement mal sécurisé et physiquement avec vous, il peut être assez facile de vous attaquer directement pour obtenir le code PIN.

N'oubliez pas qu'une batte de baseball ne coûte que 10 €...

Samourai Wallet

Evite les choses suivante:

- Portefeuille en papier via air gap
- Mémoriser une clé privée
- « Je peux coder mon propre portefeuille »
- Mes amis me les gardent
- Couper la clé privé en deux

Je m'oppose fermement à ces solutions. Suivez les meilleures méthodes et ne compliquez pas trop les choses.
Nous ne somme pas expert et n'avons pas les compétence pour réussir ce genre de solution sans risque.

Solution de stockage à long terme :

Si vous prévoyez de détenir des bitcoins à long terme, ceci est votre point de départ.
Du simple portefeuille physique, nous passerons à des solution de stockage plus complexe.

Trezor model one

Ledger Nano S.

- Portefeuille physique

Des petits appareil, comme un Trezor ou un Ledger, sont des porte-feuilles physiques, auxquels vous pouvez accéder en les branchant sur votre ordinateur. Considérez-les comme des clés USB pour Bitcoin.

- Il s'agit d'une solution de stockage au froid, ce qui signifie que le portefeuille n'est jamais connecté à l'internet
- La clé privée (ce qui est important) est créée directement sur l'appareil et ne le quitte jamais.
- L'appareil est portable et compatible avec n'importe quel PC.
- Il coûte environ 50 à 100 euros, pas si cher que ça vu les services et la nécessité.
- Vous pouvez stocker n'importe quel montant de bitcoins sur un seul appareil.
- Vous pouvez créer autant de portefeuilles/comptes que vous le souhaitez à partir d'une seule clé.

2 . Portefeuille physique+ Passphrase

Ledger & Trezor ont tous deux une option appelée "Passphrase" sur leur appareil.

Cela vous permet d'ajouter un mot de passe supplémentaire en plus de la clé privée de 24 mots. Cela crée un nouveau compte caché en plus de l'ancien, qui ne peut être accessible que si vous connaissez la passphrase & la clé privée.

Clé privée

\+ « Omeletteufromage71» =

Passphrase (nouveauté)

Compte n°2 :

- Ouverture au moyen d'un code PIN secret
- Récupéré en utilisant :
  - La clé privé
  - La passphrase

Pourquoi l'utiliseriez-vous ?

- **C'est un deuxième niveau de sécurité pour votre portefeuille BTC.**

Un voleur devra maintenant voler votre clé privé et la passphrase

Comme vous allez les stocker dans deux lieux géographiques différents, il est désormais très difficile de le faire.

De plus, l'attaque physique peut être atténuée en donnant le compte N°1 dans lequel vous ne détenez qu'une petite quantité de BTC.

- **Créer un portefeuille illimité en plus d'une clé privée.**

Vous pouvez stocker une clé privée familiale et créer un nouveau portefeuille pour chaque enfant.

- **Si vous pouvez vous souvenir de la passphrase,**

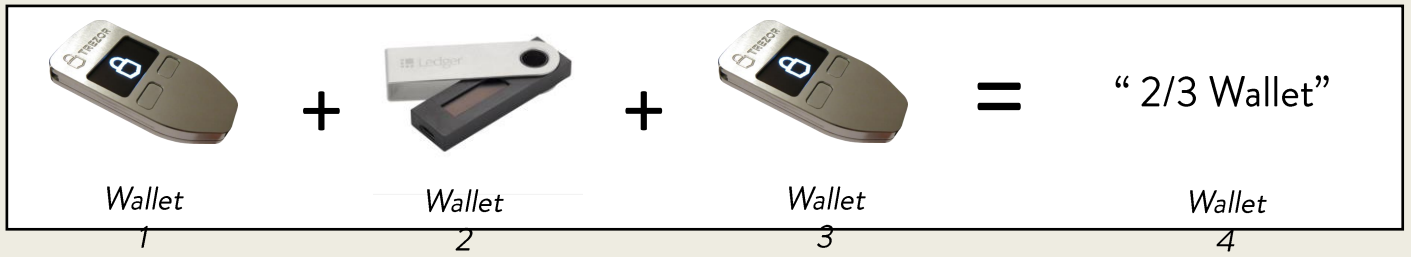
Ce qui permet de ce déplacer plus facilement avec de large somme

3. Portefeuille Multi-Signatures

L'idée c'est de combiner plusieurs portefeuilles (clé privée) en un nouveau portefeuille.

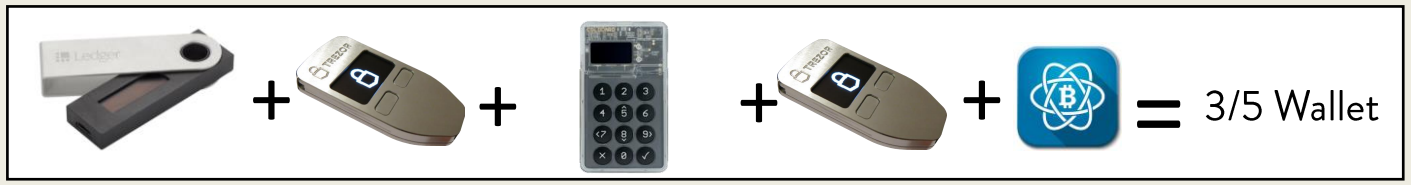
Une fois le nouveau portefeuille (N°4) créé, il fonctionne comme un portefeuille ordinaire pour recevoir des fonds. Cependant, pour envoyer des BTC, vous devrez signer la transaction non pas avec une clé privée mais avec 2 des clés sur 3 . Peu importe laquelle, mais il en faut 2.

- Donc maintenant, si vous venez à perdre un dispositifs, vos fonds seront toujours disponibles en utilisant les deux autres.
- En outre, si un voleur a accès à un des dispositifs, il ne pourra avoir accès à aucun fond. Il lui faudra en voler un deuxième.



Le même principe peut être appliqué à toute forme de portefeuille.

- Nombre de clés nécessaires pour signer.
- Nombre de participants.



Quand l'utiliser ?

C'est très utile si vous avez besoin de séparer la détention du fonds entre les personnes. (Famille, entreprise, organisation)

Si vous possédez une grande quantité de BTC, celle-ci devient obligatoire pour des raisons de sécurité.

L'astuce consiste ici à utiliser différents logiciels / portefeuilles pour créer des clés privées différentes.

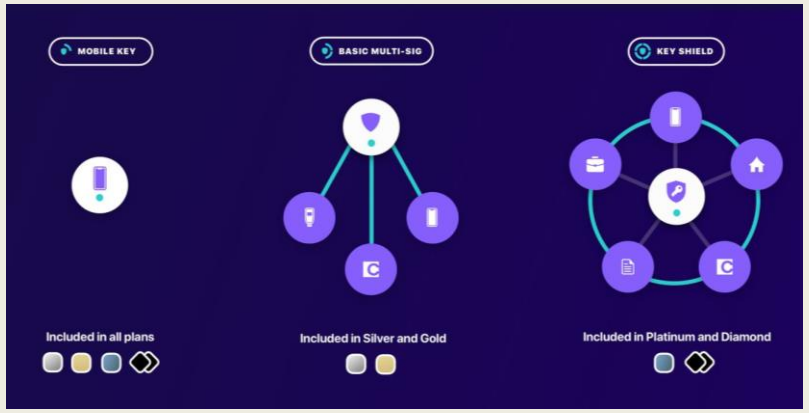
Veillez à stocker votre clé privée/portefeuille dans un endroit séparé afin d'avoir la meilleure sécurité possible.

Electrum est le bon endroit pour commencer à expérimenter.

La sécurité est une cible mouvante.

Vous ne pouvez jamais être sûr à 100 %, mais vous pouvez atténuer vos risques :

- Suivez les conseils des expert en sécurité et les meilleures pratiques du secteur.
- Le portefeuille physique est le minimum requis.
- Renseignez-vous sur la passephrase
- La multi-sign est optimale elle est obligatoire si vous disposez de beaucoup d'avoirs.
- Faites un inventaire clair et simple.
- Revoyez votre sécurité au minimum une fois par an !



Services de stockage Casa (multi-sign avec garde partielle des clés)

- 0- 300 $: Portefeuille Mobile
- 300 - 2500 $: Porte-feuille physique
- 2 500 – 10 000 $: HW + Passephrase
- 10 000 - 50 000 $: • Multi sig 2/3 • Casa ' Gold
- 50 000 – 1M : • Multi sig 3/5 • Casa ' Plat
- Plein : Consultez un expert lol

Conseils :

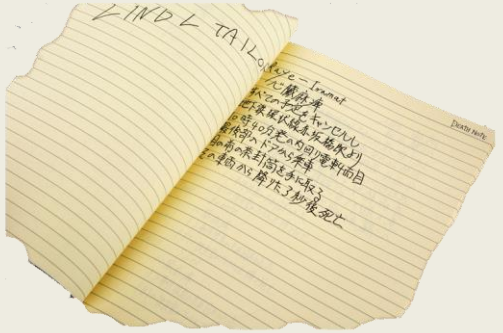
La vie privée, c'est la sécurité ! Gardez un profil bas sur vos bitcoins.
Entraînez-vous, entraînez-vous et entraînez-vous ! Mieux vaut avancer lentement que rapidement.

Important:

Ce sont mes règle personnelles.
Je ne suis PAS un expert en sécurité.
Faites vos propres recherches !

Pas de retour en arrière si vous perdez une clé privée ou si vous l'envoyez à une mauvaise adresse

« Si vous mourez demain, qu'adviendra-t-il de votre bitcoin? »



Si vous ne pouvez pas garantir que votre bien-aimé aura un accès complet à vos bitcoins :

- Physiquement (détention de la clé privée).
- Légalement (approuvé par un notaire).

Alors vous devez sérieusement arrêter tout ce que vous faites dès que possible et commencer à faire ce qui suit :

Option 1: Acheter " Cryptoasset Inheritance Planning " par Pamela Morgan

" Cryptoasset Inheritance Planning " par Pamela Morgan

Option 2: Allez au niveau 6 de mon contenu où j'approfondis ce sujet.

A Crypto Exchange CEO Dies—With the Only Key to $137 Million

Customers of QuadrigaCX are out as much as $190 million after CEO Gerry Cotten died; Cotten reportedly was the only one with the key to retrieve the money.

wired.com

Recap:

Comment choisir un bon portefeuille :

- Open source (obligatoire)
- Portefeuille froid (obligatoire)
- Caractère privé (obligatoire)
- Option de création de transactions (Avancé)
- Support multi-sign et passephrase (Meilleur)
- Bien préparer ses arrières.(Mieux)
- Mettre en place de nouvelles fonctionnalités (Segwit, LN, co-joint, Ricochet etc) (Mieux)

Je vais probablement éviter tout portefeuille qui ne comporte pas 5/7 de ça.

Security type	Wallet type	Security	Ease of set up	Convenience	Best use case	3rd party risk	Amount hold
Cold Storage	Portefeuille physique	Haut	Facile	Faible	Long terme	Non	X > 1000 $
Cold Storage	Portefeuille papier	Haut	Difficil	Tres faible	Tres long terme	Non	Seulement si vous savez ce que vous faites
Hot wallet	Portefeuille mobile	Normal	Tres simple	Haut	Cash	Non	0 - 1000 $
Hot wallet	Desktop wallet	Normal	Facile	Haut	Cash	Non	0 – 500 $
Hot wallet	Exchange wallet	Faible	Facile	Normal	Trading	Oui	Ce que vous êtes prêt à perdre
Dépôt	Intermédiaires titulaires	Faible	Normal	Faible	Perte d'argent	Oui	0 $

Une recommandation personnelle amicale:

Samourai Wallet

1. Commencez par Samourai sur Android

2. Passez à Trezor lorsque vous atteignez 500 - 1 000 $

3. Passez à Multi-sig 2/3 quand vous serez prêts

Pour allez plus loin :

Sur le même sujet:

Animé du jour:

Plongez dans le terrier du lapin Bitcoin:

Dans le Terrier du Bitcoin, nous croyons que l'éducation doit être gratuite et accessible à tous. Alors s'il vous plait, profitez de notre contenu éducatif sur Bitcoin sans rien payer!

www.DecouvreBitcoin.fr

Follow us on

Extra ressources

Portefeuille Bitcoin:

- https://samouraiwallet.com/
- https://trezor.io/
- https://www.ledger.com/
- https://electrum.org/#home
- https://keys.casa/
- https://www.wasabiwallet.io/
- https://coldcardwallet.com/

Andres Antonopoulos video :

- https://www.youtube.com/watch?v=W3XADagE6P8
- https://www.youtube.com/watch?v=bc3HQqCSl7A
- https://www.youtube.com/watch?v=vt-zXEsJ61U
- https://www.youtube.com/watch?v=3zNVDIz6Snw

Gestion de clé

- https://blog.keys.casa/the-dos-and-donts-of-bitcoin-key-management/?mc_cid=f1629f4069&mc_eid=e245cfa3e2
- https://blog.trezor.io/passphrase-the-ultimate-protection-for-your-accounts-3a311990925b

Plan pour héritage

- https://empoweredlaw.com/articles/articles-2/
- https://www.amazon.com/Cryptoasset-Inheritance-Planning-Simple-Owners/dp/1947910116
- https://www.youtube.com/watch?v=6eVTbvQJyfU&feature=emb_logo
- https://www.youtube.com/watch?v=W3XADagE6P8&feature=emb_logo

Allons un peu dans le technique:

- Https://medium.com/mycrypto/the-journey-from-mnemonic-phrase-to-address-6c5e86e11e14
- https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- https://en.bitcoin.it/wiki/Address
- https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt
- https://www.betterbuys.com/estimating-password-cracking-times/
- https://en.bitcoin.it/wiki/Seed_phrase
- https://github.com/bellaj/Blockchain/blob/6bffb47afae6a2a70903a26d215484cf8ff03859/ecdsa_bitcoin.pdf
- https://gist.github.com/bartekn/c877987b722ec792912d720921a7418c
- https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/

Merci d'avoir suivi la classe :)

Si vous désirez nous contacter: contact@decouvrebitcoin.com

Pour nous aider, faites des remarques, corrigez des erreurs et proposez plus de liens & ressources pertinentes. Merci d'utiliser ce lien; **https://bit.ly/3kUPJnA**

Notre contenue est gratuite et il n'y a pas eu de sponsors. Faites attention à vous et gardez vos clefs proches de vous. Notre travail est licensé sous CC BY-SA

V1.2 14/08/2020 Rogzy

Avertissement

Les cryptomonnaies sont des produits risqués

Tout notre contenu est à but purement pédagogique et informatif. Le bitcoin est un actif hautement spéculatif et nous conseillons de discuter avec votre conseiller financier avant de prendre une décision importante. Prenez garde aux arnaques et prenez en compte le risque.

N'investissez que ce que vous pouvez vous permettre de perdre. Les performances financières passées ne sont pas représentatives des performances à venir.

L'industrie des cryptomonnaies est pleine d'arnaques. Ne faites pas confiance aux inconnus (même pas à nous) et ne divulguez pas votre clé privée. Les informations fournies sur ce site ne doivent pas être votre seule référence. Vérifiez et croisez vos sources.

Nous ne sommes pas intéressés dans des partenariats avec des altcoins.

Notre travail est licensé sous CC BY-SA. Nous sommes un fournisseur de contenu indépendant qui n'est pas engagé auprès d'une ICO ou autre cryptomonnaie centralisée.

Nous ne demanderons jamais vos informations personnelles (SEED & clé, nom, adresse, KYC, etc...). Par souci de transparence, nous détenons bien des bitcoins.

Le projet Le Terrier du bitcoin est une activité de la société CEVEX sas. Nous ne sommes pas responsables des pertes liées aux arnaques, aux clés perdues et aux mauvais investissements.

Pour plus d'informations, visitez notre site ou contactez-nous directement.

www.DecouvreBitcoin.com

Decouvrebitcoin@protonmail.com