Bitcoin P2P

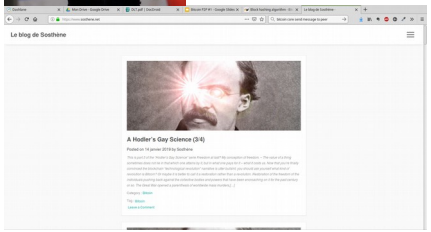
Conservation des clés


Happy Bitcoin Pizza Day!
MAY 22

Conservation des clés

1. Qu’est-ce qu’une clé privée ? Pourquoi est-ce important ?
2. Quelles sont les solutions existantes ?
3. Quelles sont les bonnes pratiques ?

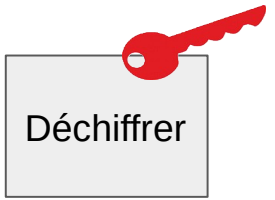
www.sosthene.net
@Sosthene@bitcoinhackers.org



Cryptographie asymétrique

Une seule clé pour toutes les opérations et les participants

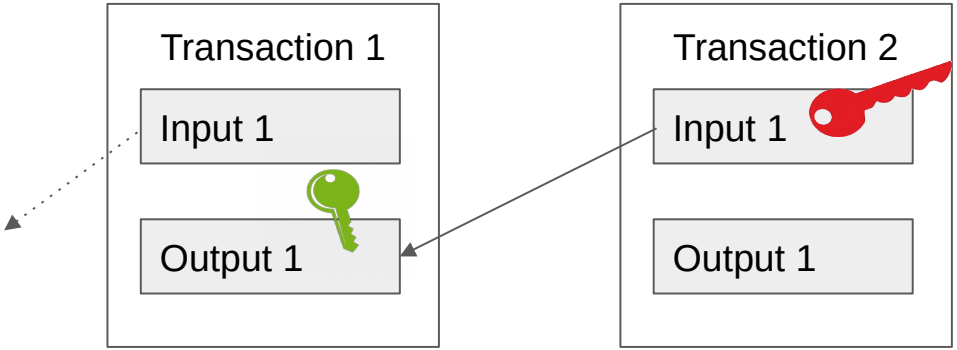
- Une paire de clé publique + privée par participant
- La clé privée permet de déchiffrer un message chiffré avec la clé publique correspondante



Le principe de base de la cryptographie asymétrique :

- tout le monde connaît la clé publique de tout le monde
- si Alice veut écrire un message à Bob, elle va le chiffrer avec la clé publique de Bob, car ainsi seul ce dernier pourra le déchiffrer

Une transaction Bitcoin

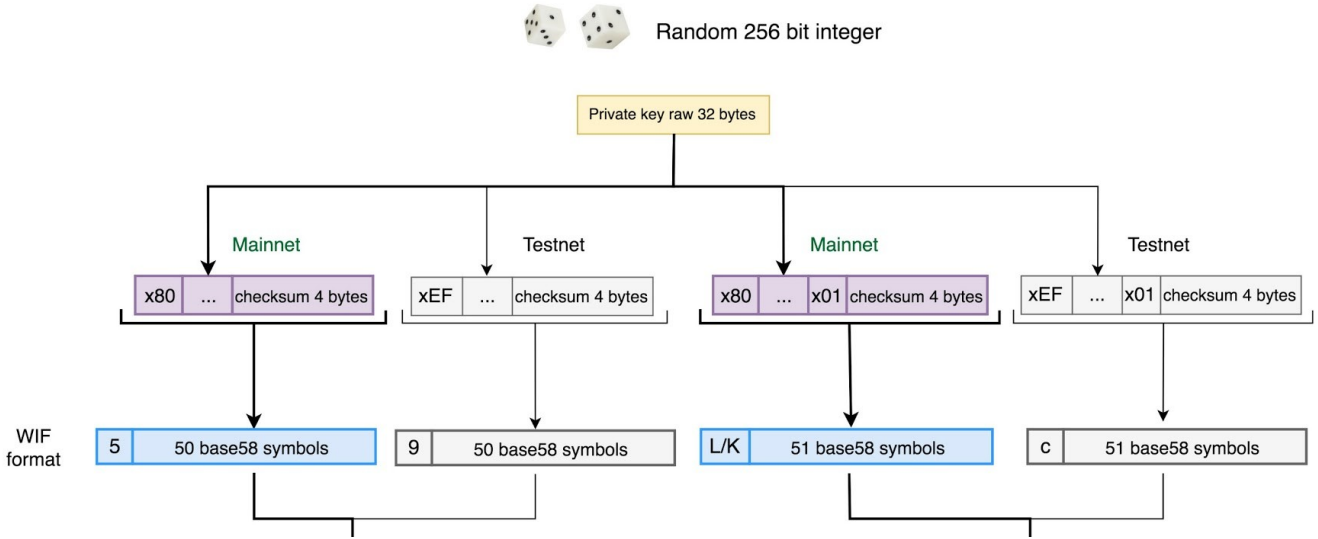


Lors de la transaction 1, Alice a verrouillé l'output 1 avec la clé publique de Bob, ce qui signifie que seul Bob peut utiliser cet output comme input dans la transaction 2 car il possède la clé privée correspondante.

Posséder des bitcoins, cela signifie donc posséder la clé privée qui permet de déverrouiller un UTXO (unspent transaction output)

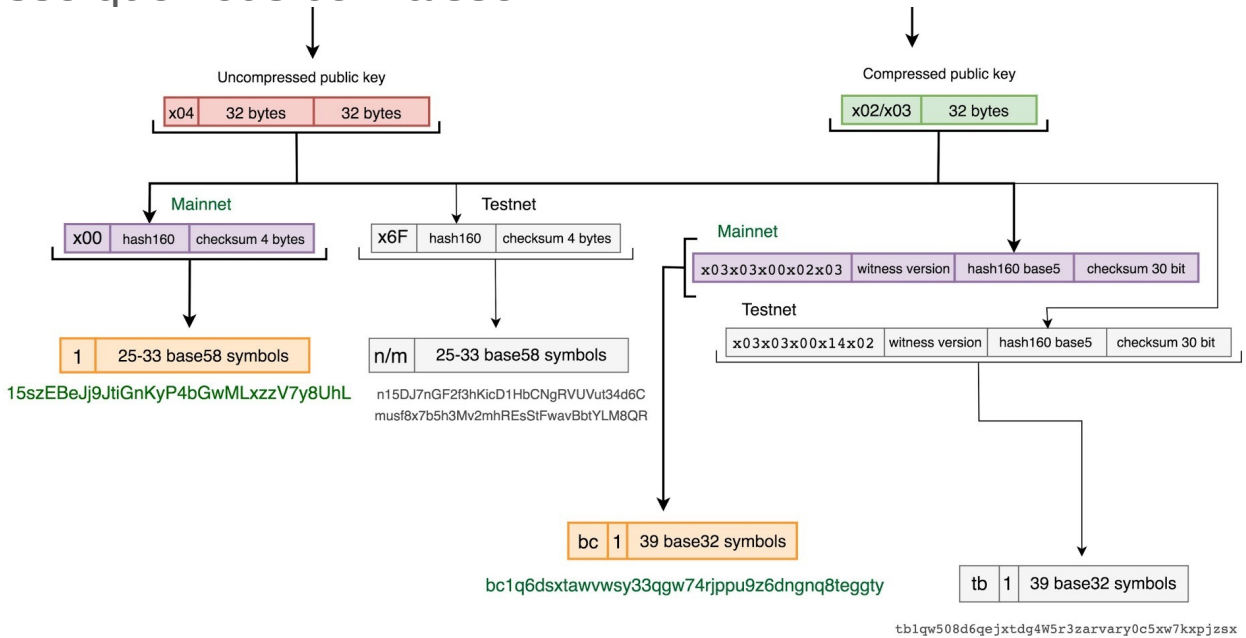
C’est quoi une clé privée ?

C’est un nombre entier de 256 bits (2^256), qui peut être représenté sous différents formats.



C’est quoi une clé privée ?

Il est utilisé pour déduire les clés publiques qui sont ensuite encodées sous une forme d’adresse que vous connaissez



Concrètement...

...vous n’aurez (presque) jamais à manipuler directement vos clés privées, c’est extrêmement dangereux et le plus souvent inutile.

De plus la clé seule ne suffit pas toujours pour retrouver vos bitcoins, car il faut aussi savoir comment sont générées les adresses (ce qu’on appelle le “chemin de dérivation”).

La plupart des wallets vous fournissent une seed, qui est probablement le moyen le plus simple et le plus sûr de conserver sa clé, ou alors un fichier contenant les clés privées et toutes les métadatas (c’est le cas de wallet.dat dans Bitcoin Core)

Typologie des risques

1. Perte accidentelle des clés privées en raison d'une erreur humaine
2. Perte accidentelle due à un facteur extérieur : défaillance matérielle ou logicielle, catastrophe naturelle...
3. Quelqu'un d'autre entre en possession de mes clés sans mon consentement :
    a. Vol avec violence
    b. Chantage, escroquerie
    c. Hacking
    d. Confiscation par une autorité

- Contrainte : les mesures prises pour mitiger ces risques ont un impact sur ma capacité à effectivement utiliser mes UTXO dans une transaction
- Important, mais hors périmètre : le risque d'arnaques sophistiquées si vous ne pouvez pas valider vous-mêmes la blockchain, la confidentialité (son absence fait de vous une cible)

Idéalement, il s'agit de conserver vos clés privées à la fois en **sécurité** et **facilement accessibles** par vous, tout en garantissant **l'authenticité** et la **confidentialité** de vos transactions.

Analyser votre situation

Comme pour la monnaie fiat, des montants différents nécessitent des solutions adaptées, du plus facile à utiliser (mais moins sécurisé) au plus sûr (mais difficile à utiliser) :

1. L’argent de poche (< 1000€) : n’importe quel wallet non custodial
2. Petite épargne (< 10 000€) : un hardware wallet
3. Un gros investissement (< 100 000€) : un cold storage sophistiqué avec multisignature
4. Une fortune (> 100 000€) : demandez conseil à des professionnels

Analyser votre situation

- Quel est mon environnement ? Quels sont les risques inhérents (politique, criminalité…) ?
- Quelle est ma situation personnelle et familiale ?
  - Risque que je sois personnellement en incapacité de dépenser mes bitcoins : profession à risque, exposition politique, maladie invalidante, décès
  - Qui doit être en mesure de reprendre le contrôle si je ne suis plus en capacité de le faire : mes associés ? mon épouse ? mes héritiers ?
  - Jusqu’à quel point suis-je prêt à leur faire confiance ?

Posséder ses bitcoins : quelles solutions ?

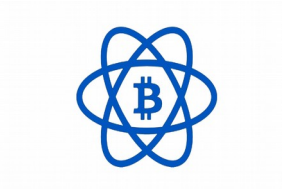
Solution	Erreur humaine	Accident	Vol	Utilisabilité
Custodial Wallet				
Software Wallet				
Hardware Wallet				
Cold storage protocol*				
Multisig	+			-

* Glacier, RustyRussel, SmartCustody etc

Custodial wallet

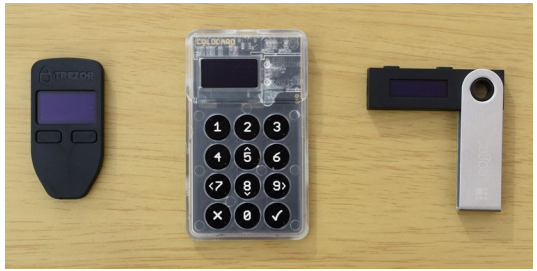
- Vous ne possédez pas de bitcoins, mais un IOU
- Le track record de ce type de stockage est absolument désastreux
- Le seul avantage est qu’en cas de décès ou d’incapacité, les bitcoins ne sont pas perdus puisque vous n’avez pas vos clés (mais de toute façon on vous les volera sûrement avant)
- Au vu de l’offre de software wallets tout aussi facile à utiliser, il n’y a absolument aucune raison d’utiliser un custodial wallet aujourd’hui

Software wallet



- La génération et le stockage de la clé privée et des adresses sont effectués de façon logicielle sur du matériel non-dédié (smartphone, ordinateur…)
- La sécurité dépend à la fois de la fiabilité du logiciel et du matériel utilisé.
- Il s’agit généralement de “client léger” (= qui ne valide pas les transactions avec la blockchain), mais le wallet intégré de Bitcoin Core est aussi un software wallet

Hardware wallet



- Un hardware dédié à la génération et la conservation des clés
- Il est conçu pour être résistant aux malwares, même si des attaquants très sophistiquées avec un accès physique à l’appareil et du matériel spécialisé peuvent réussir à découvrir les clés
- Il implique de faire confiance au fabricant et à la chaîne de fabrication (même si aucune attaque de ce genre n’est répertorié à ce jour)
- Il a un énorme inconvénient : il est très facilement identifiable, ce qui peut être problématique dans certains scénarios

Cold storage

- Il s’agit d’un protocole qui permet de conserver les clés privées hors d’atteinte d’une attaque informatique
- Il en existe plusieurs, plus ou moins facile à mettre en œuvre et sûr :
  - Le paperwallet (un papier avec une clé privée et l’adresse correspondante)
  - La seed (une suite de mots en apparence aléatoire, c’est le mode de back-up le plus courant aujourd’hui)
  - L’ordinateur “air-gapped” (l’utilisation d’un ordinateur mis en quarantaine pour signer les transactions)
  - les protocoles de haute sécurité comme Glacier (génération de clés privées avec deux machines neuves en quarantaines pour détecter des supply chain attack et une entropie générée manuellement par des lancers de dés casino-grade)
  - plein d’autres...

Le multisig

- Il s’agit de créer un wallet dans lequel les transactions doivent être signées par un certain nombre de clés parmi un pool pré-défini pour être valide.
- Le cas d’usage est évidemment le cas où plusieurs personnes doivent avoir le pouvoir sur un wallet, mais on peut tout à fait faire des multisigs seul dans un soucis de redondance !
- Il permet également d’éviter la perte des bitcoins dans le cas de la disparition ou de l’incapacitation d’un des signataires
- Parmi les combinaisons les plus courantes :
  - “2 de 3” : souvent utilisé dans les séquestres
  - “1 de 2” : deux époux qui font un “compte joint”
  - “3 de 5” : préparation de succession avec un ou deux acteurs institutionnels
  - “5 de 7” : conseil d’administration d’une entreprise avec une ou deux clés conservées en sécurité par la banque

Le multisig *as a service*

- Casa propose un service par abonnement qui comprend différents schéma de multisig pour protéger vos bitcoins. L’idée est de privilégier la redondance pour que Casa puisse retrouver vos bitcoins ou que vous puissiez les récupérer même si Casa venait à disparaître
- Ledger propose désormais Vault, un système custodial à destination des entreprises
- Sur téléphone Green propose quelque chose d’assez similaire quoique plus simple avec un multisig 2 de 2

tl;dr

- Éviter les solutions custodiales (*not your keys, not your bitcoins*)
- Vos clés privées ne doivent JAMAIS être échangées ou stockées électroniquement en clair.
- Une seed se note sur papier, ne jamais prendre de photos avec votre téléphone, ne jamais l'enregistrer électroniquement
- Faire des back-up, les chiffrer avec un bon mot de passe ou les protéger physiquement
- Vous n'êtes pas immortels : assurez-vous que quelqu'un dans votre famille sait comment accéder à vos bitcoins, mettez en place un multisig
- Chercher la sécurité maximale augmente aussi le risque de perte accidentelle. La bonne solution est celle que vous comprenez et qui est proportionnée à vos risques

Les étapes critiques

1. Générer les clés privées
2. Créer un wallet
    a. Multisig (redondance et répartition entre plusieurs parties prenantes)
    b. Création des adresses
3. Stocker et gérer des clés
    a. Protection des clés (chiffrage)
    b. Existence de back-up
    c. Vérification des back-up
    d. Protection des back-up
4. Utiliser les clés (signature de transactions)
5. Révoquer les clés (en cas de perte, de vol, de compromission d’un détenteur…)

1. Générer les clés privées

- Comme tout secret cryptographique, la génération de clés privées pour Bitcoin nécessite de générer un secret de façon fiable
- C’est une opération prise en charge par le wallet et il vaut mieux ne pas s’en mêler (Bitcoin Core et Electrum sont *a priori* suffisamment fiable)
- Le protocole Glacier prévoit une procédure semi-manuelle et un double check sur 2 ordinateurs neufs mis en quarantaine :
  - Une partie du secret est générée par 62 lancers de dés “casino-grade”
  - L’autre partie par le système d’exploitation
  - Réaliser l’opération sur 2 machines permet de vérifier que le hardware n’a pas été compromis pour générer des clés plus facile à deviner

2. Créer le wallet

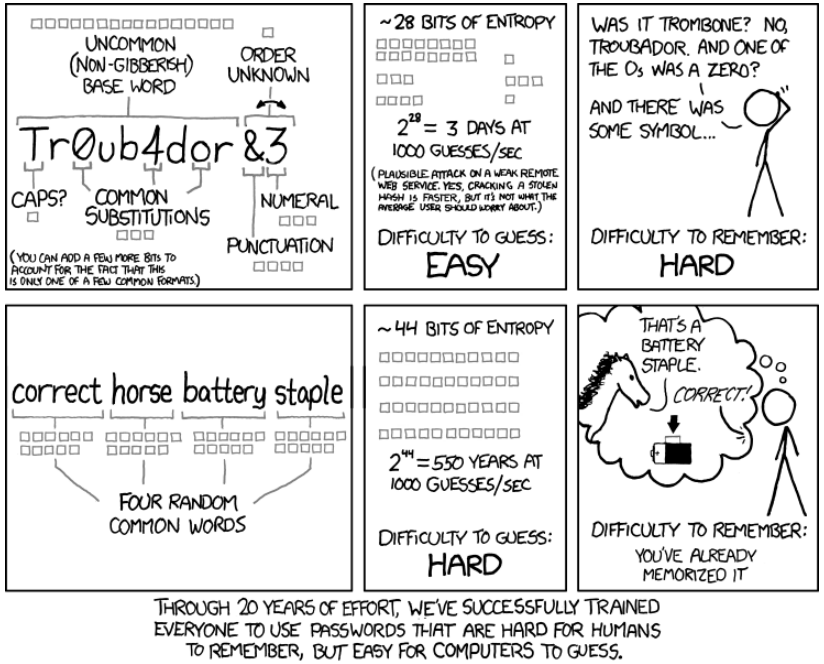
- La génération des adresses est une étape souvent négligée alors qu’elle est critique : si vous ne savez pas comment votre wallet génère ses adresses, il est très probable que même avec la clé privée vous ne puissiez pas retrouver votre argent !
- Aujourd’hui la plupart des wallets sont *Hierarchical determinist*, ce qui signifie qu’ils génèrent toujours les mêmes adresses dans le même ordre (ce n’était pas le cas avant)
- C’est aussi à ce moment que vous pouvez décider si votre wallet sera multisig ou non

3. Stocker et gérer les clés privées

- Les clés sont le plus souvent dans un fichier, il est donc indispensable de protéger ce dernier par un mot de passe
- Pour éviter que la perte de ce fichier vous fasse perdre vos bitcoins, il vaut mieux avoir des back-up :
  - plusieurs exemplaires de la seed
  - Bitcoin Core : faire une copie du fichier wallet.dat, la chiffrer avec VeraCrypt, et la conserver à plusieurs endroits différents
  - un back-up non testé = 0 back-up
- La protection d'un back-up :
  - chiffrage
  - sécurité physique : coffre-fort, banque…
  - protection contre les incendies, les inondations ⇒
  - Shamir's secret

Comment faire un bon mot de passe

- Prendre une liste de mots (par ex : https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt)
- Jeter un dé 5 fois en notant le résultat et noter le mot correspondant dans la liste
- Répéter l'opération jusqu'à avoir une série aléatoire d'une longueur suffisante
- NE JAMAIS RÉUTILISER UN MOT DE PASSE



Source : https://blog.fleetsmith.com/password-security-guide/
https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret

Shamir’s secret

- Permet de chiffrer une information et de la diviser en un nombre arbitraire de parties. Le texte en clair ne peut être retrouver qu’avec un nombre arbitraire de parties du secret (par exemple, 3 sur 5)
- Peut être utile pour protéger une seed, ou dans certains schémas organisationnels complexe ou plusieurs individus doivent se partager une clé d’un multisig

4. utiliser les clés (signature de transaction)

- C’est un moment de vulnérabilité car on est obligé de déchiffrer nos clés pour signer
- Toute la logique d’un “airgap” est de signer les transactions sur une machine hors réseau afin de mitiger au maximum cette vulnérabilité

5. Révoquer les clés

- Que faire si vous perdez vos clés ou que vous supposez que quelqu’un aurait pu entrer en leur possession ?
- Pas de panique si un appareil contenant un wallet est volé (si vous l’avez protégé avec un mot de passe et que vous avez un back-up)
- Si c’est une seed qui a été volé, c’est une course de vitesse pour déplacer les bitcoins avant le voleur
- Dans tous les cas, l’idée est de déplacer les bitcoins vers une autre adresse sous votre contrôle