

Porte-monnaie Mycelium



Ce document montre comment procéder au transfert de bitcoins depuis un porte-monnaie papier vers une adresse publique bitcoin au moyen du portefeuille [Mycelium](#).

Mycelium est un porte-monnaie électronique qui peut être installé sur un smartphone *Android*, ou *Apple iOS* (iPhone). Comme pratiquement tout les produits de la technologie Bitcoin, son [code source](#) est ouvert et disponible sur [github](#) pour toute personne ayant au moins des connaissances en programmation.

Les explications suivantes se limitent à une manipulation simple de transfert de bitcoins depuis **un portefeuille papier** vers **une adresse publique** bitcoin. Cette dernière peut être celle d'un autre portefeuille papier, d'un autre porte-monnaie "portable" comme Mycelium ou [Copay](#), d'un portefeuille en ligne situé dans une plateforme d'échange de bitcoin ou de gestion de portefeuille.

Lorsque Mycelium n'est utilisé que pour cet usage, il n'est pas besoin de connaître toutes ses fonctionnalités, ni de faire une sauvegarde de son propre portefeuille qui restera vide après l'opération de transfert. En fait il est possible d'installer Mycelium, d'effectuer le transfert et de le désinstaller du smartphone si on ne veut plus l'utiliser.

Mycelium est quand même un portefeuille complet qui permet de recevoir, envoyer, gérer les bitcoins qui y sont contenu. Son utilisation est très simple et sécurisée. L'interface est en français. Il peut gérer plusieurs comptes, stocker un carnet d'adresse, conserver un historique des opérations, sauvegarder / restaurer sa clé secrète pour être ré-installé, etc...

Les explications et les copies d'écran suivantes ont été faites au moyen d'un smartphone Android.

Dernière mise à jour : 13 octobre 2017 - Pour m'envoyer message / commentaire / avis / remarque : [Contact](#)

Lien vers cette page : <http://didier.celse.free.fr/bitcoin/mycelium/index.htm>

[Télécharger cette page en PDF](#) (11 pages - environ 5 Mo)

Ce site ne stocke pas de cookies.

Autres tutoriels : [Bitcoin](#) [Copay](#) [Ripple](#) [Kraken pour Android](#)

> On peut cliquer sur un des liens ci-dessous <

[Moyens et documents nécessaire](#)

[Vérifications préliminaires](#)

[L'opération de transfert](#)

[Vérification de la transaction](#)

Moyens et documents

Il va sans dire que l'utilisateur qui a besoin d'effectuer une transaction de transfert de bitcoin depuis un portefeuille papier sait ce qu'il va faire et a déjà manipulé ce genre de produits que sont les bitcoins et les porte-monnaie. Si cela n'est pas acquis, alors le tutoriel générique pour savoir utiliser les bitcoins et quelques produits associés se trouve [ici](#).

Donc pour éviter d'avoir à chercher au dernier moment, on aura besoin de 6 choses :

1 - Un smartphone dans lequel est installé l'application **Mycelium** ! Il faut que le smartphone soit connecté à internet pendant toute la durée de l'opération.

Pour installer Mycelium il faut se rendre sur le *Play Store* :



Mycelium Bitcoin Wallet

Mycelium Developers

3+

INSTALLER

Plus de 100 000 téléchargement(s)



Mycelium Bitcoin Wallet

Mycelium Developers

3+

Installation...

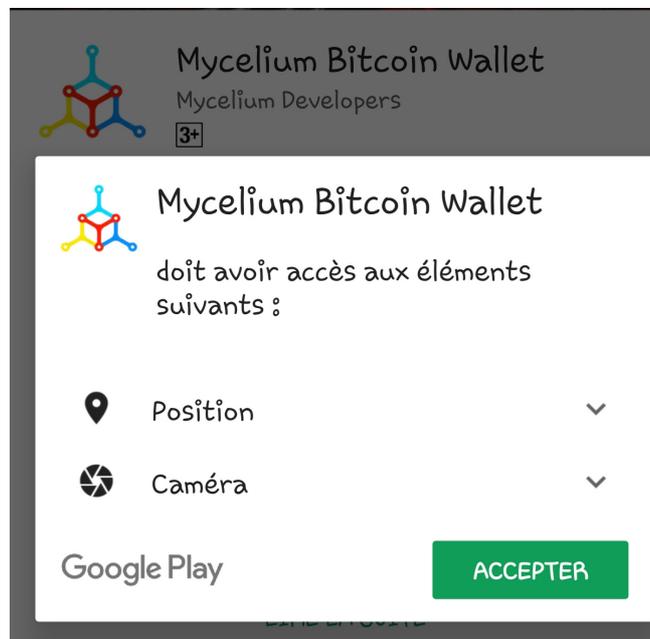
Plus de 100 000 téléchargement(s)

Découvrez également...

PLUS



Il faut *Accepter* dans l'écran suivant l'accès à la localisation du smartphone (*Mycelium propose des servir d'achat/vente de BTC à proximité*) et à l'utilisation de l'appareil photo (*pour scanner les QR-code*).



Dans l'écran de bienvenue il faut sélectionner **Créer** :



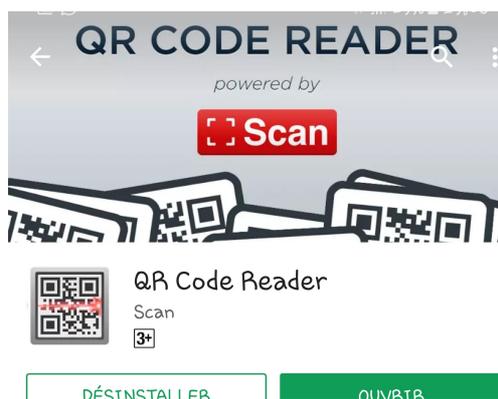
Finalement on arrive à l'écran d'accueil qui montre le solde à zéro du nouveau portefeuille :



Dans le cas de l'opération de transfert que l'on va effectuer, ce nouveau portefeuille Mycelium, dont on voit la clé publique (par exemple `1NXrL...Hfncf` ci-dessus), ne sera pas utilisé et restera vide. Pour la transaction à effectuer, Mycelium va seulement servir de moyen de transfert.

2 - Si possible, ce n'est pas obligatoire, un PC ou une tablette qui va permettre de préparer l'affichage des QR-code des portefeuilles. Et aussi de naviguer sur le web pour vérifier l'état des portefeuilles en question avant et après l'opération. Eventuellement un deuxième smartphone connecté au web peut faire l'affaire.

3 - Une application qui permet de vérifier les QR-code. Ceci n'est pas obligatoire, mais c'est conseillé. Par exemple l'application **QR Code Reader** fait parfaitement l'affaire, il est conseillé de l'installer à partir du *Play Store* :



L'installation est simple et classique.

- 4 - La clé privée** du portefeuille papier, celui d'où vont être *débités* les BTC. En principe celle ci a été précieusement conservée dans un endroit sûr. C'est-à-dire : soit elle est imprimée sur un document que l'on a sortie d'un coffre fort ou d'un lieu secret. Soit elle est stockée dans un fichier informatique qu'on doit extraire du lieu de stockage sécurisé. Il peut s'agir d'un document au format **texte**, **PDF** ou image **JPG**. Cette clé peut être transférée provisoirement dans le smartphone au format texte, le temps d'effectuer l'opération de transfert. Le mieux c'est d'avoir le QR-code de la clé privée, soit imprimé, soit affiché par exemple sur l'écran de l'ordinateur ou de la tablette. Par exemple ceci est le QR-code d'une clé privée au format image JPG :

Clé Privée WIF (51 caractères base58, débute avec un a '5'



5JFBFgC4P5j3pVYdHAjC2a2W7KeFxGiYn9jMiwMzWt6NF6hmssV

(C'est une vraie clé privée qui a déjà été utilisée et qui peut être scannée pour essayer)

Si le QR-code de la clé privée n'est plus disponible, il ne reste que le texte comme *5JFBFg...6hmssV*, alors il est possible de re-crée son QR-code en suivant la procédure qui se trouve [ici](#).

- 5 - La clé publique** du portefeuille papier, donc celui qui va être *débité*, pour vérifier le montant disponible. Cette vérification peut se faire en sur le site <https://blockchain.info/>, selon la méthode expliquée [ici](#).

- 6 - La clé publique** du portefeuille destinataire, donc celui qui va être *crédité*. Comme pour la clé privée, le mieux est d'avoir son QR-code imprimé, ou affiché sur un écran.

Par exemple : le portefeuille de destination est celui d'un compte [Kraken](#) (c'est une plateforme d'achat / vente de bitcoins). Dans la page web du site qui donne [les instructions pour créditer](#) des BTC, il est possible d'afficher de QR-code de réception en cliquant sur le bouton **QR code**. Cela fait afficher un écran similaire à celui ci :

Connect to peers to your market, and funds to earn to your market, or Launch to launch your wallet with the address entered.

- **Six confirmations** are required before the funds are available for trading. With BitGo Instant, funds will be confirmed immediately upon receipt.

Minimum ฿0.00010

Deposit address	Status	
35D5inrAqqGCCfs9f1qgxG4SaJJjxVHwMM	Used address	← Select QR Code ↗ Launch
3HD5snnh4pBbZ1QweREMRKxZrwQYiXqjm9	Used address	← Select QR Code ↗ Launch

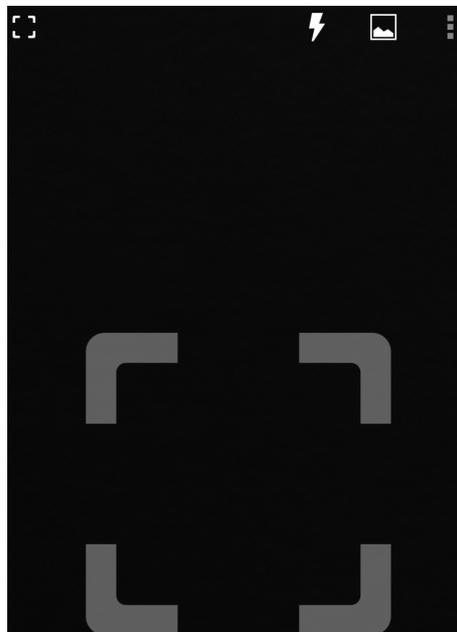
[Generate New Address](#) < >

On laisse donc l'écran du PC tel quel, prêt pour scanner la clé publique destinataire.

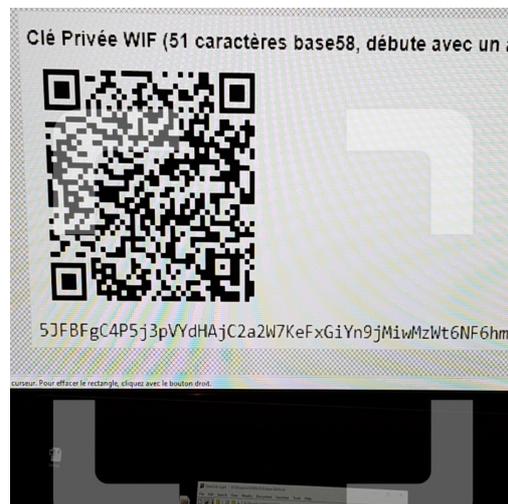
Vérifications préliminaires

Cette étape de vérification n'est pas obligatoire mais conseillée. Il s'agit en fait de vérifier qu'il n'y a aucun problème pour scanner et décoder les QR-code. C'est pour être certain d'une part que le smartphone avec son appareil photo fonctionne correctement. Et d'autre part de voir si l'affichage ou l'impression des deux QR-code nécessaires est convenable : sans erreur, sans problème de contraste, ou autre surprise de dernière minute.

Pour cela on lance l'application **QR Code Reader** qui va afficher un genre de cadre à 4 coins en sur-impression de l'image captée par l'appareil photo :

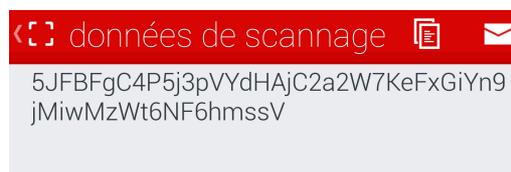


Avec l'appareil photo du smartphone, il faut donc bien viser en encadrant le QR-code de la clé privée préalablement affichée à l'étape précédente :



Si nécessaire bouger l'appareil d'avant en arrière. On peut s'entraîner avec la clé privée affichée à l'étape précédente.

Dès que *QR Code Reader* a réussi à capter ce qu'il attend, il decode l'image et affiche un écran avec le texte qu'il a trouvé :



Là il faut juste vérifier que le texte affiché correspond bien à celui de la clé privée.

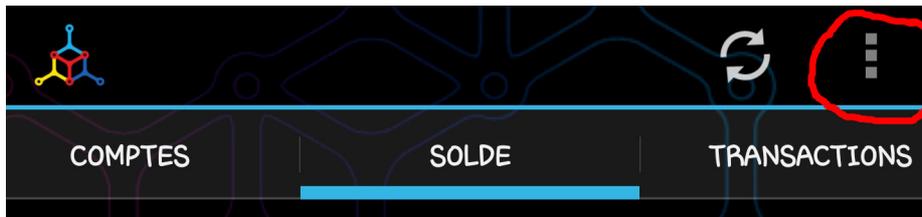
Maintenant, toujours avec *QR Code Reader*, il faut vérifier de la même façon que la clé publique du portefeuille destinataire peut être scannée et décodée sans problème.

Si ces deux vérifications on réussi, tout devrait être OK pour effectuer la transaction..

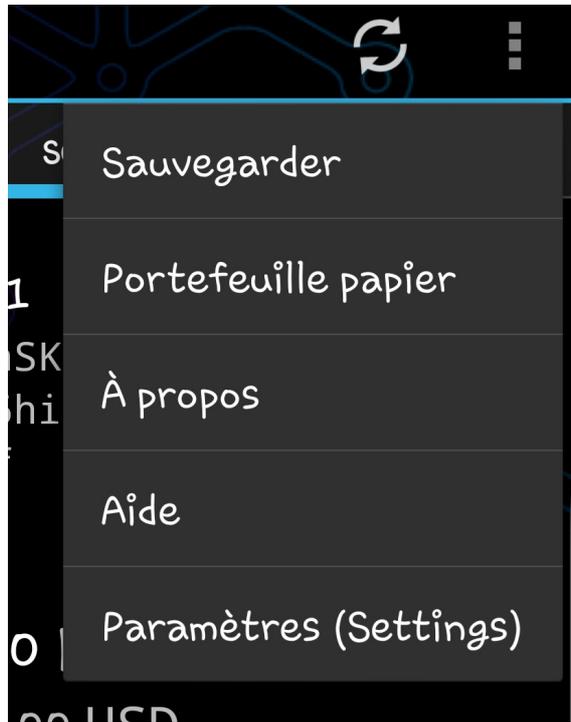
L'opération de transfert

Si le QR-code de la **clé privée** n'est pas disponible, alors il faut que cette clé au format texte soit dans le smartphone. Il faut préalablement l'éditer ou la visualiser, sélectionner le texte en question, puis le copier dans le presse-papier.

Lancer Mycelium qui va afficher l'écran d'accueil affichant le solde :



En haut à droite il y a ces trois points qu'il faut sélectionner pour afficher le menu suivant :



On sélectionne **Portefeuille papier**, cela va afficher l'écran suivant :

Récupération des fonds hors ligne

Vous êtes sur le point de faire une dépense d'une clé privée hors ligne. Cela pourrait être une sauvegarde papier d'une clé privée ou d'un bordereau de clé privée provenant d'un guichet automatique Bitcoin. Les formats suivants sont supportés :
Clé privée, Master Seed, xPriv Key

Une fois que la transaction a été envoyée, toute trace de celle-ci sera effacée de la mémoire interne.

Obtenir la clé privée depuis :

Code QR

Presse-papier

Racine Initiale

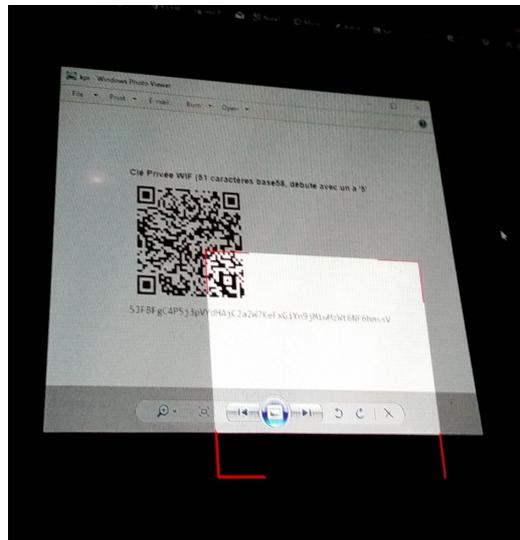
Signer avec :

Trezor

KeepKey

Si le presse-papier n'est pas vide, on suppose qu'il contient la clé privée, et le bouton **Presse-papier** est actif. Il faut le sélectionner.

Sinon sélectionner le bouton **Code QR**. Cela va activer l'appareil photo avec un cadre à 4 coins rouge en sur-impression de l'image :



Il faut bien viser pour amener le cadre pile poil sur le QR-code de la clé privée affiché à l'écran, ou bien imprimé sur un document papier. Lorsque Mycelium a réussi à capter l'image il va afficher ceci :

Récupération des fonds hors ligne

Vous utilisez une clé privée avec
l'adresse Bitcoin suivante :

132kvhUHuRj6
9LZRF91z7m4p
kgEyRDBkAx

1.23980079 BTC

4,967.93 USD

Envoyer

Mycelium s'est servi de la clé privée pour aller consulter sur internet le contenu du portefeuille papier. On voit affiché la clé publique de ce portefeuille et le montant disponible. Là on peut vérifier que clé et montant correspondent bien à ce qui est prévu.

Avant de continuer il faut être certain d'avoir sous la main la **clé publique** du portefeuille destinataire. Donc soit le QR-code affiché ou imprimé. Si le QR-code n'est pas disponible, alors il faut avoir la clé au format texte dans le smartphone. Dans ce cas, il faut préalablement l'éditer ou la visualiser, sélectionner le texte en question, puis le copier dans le presse-papier.

A partir de l'écran ci-dessus il faut sélectionner le bouton **Envoyer**. On affiche alors l'écran suivant :

Entrez l'adresse du destinataire

Numériser le code
QR

Mes adresses

Presse-papier

Saisie manuelle

Entrez le montant

0,00 BTC



Frais de transaction

Économiques ~2 heures	Normaux ~30 minutes	Prioritaires ~10 minutes
0,30007 mBTC ~1,20 USD 132 sat/byte	0,3059 mBTC ~1,22 USD 135 sat/byte	0,3093 mBTC ~1,24 USD 136 sat/byte

Envoyer

Si la clé publique est disponible dans le **Presse papier**, le bouton correspondant est en bleu, on peut le sélectionner. Sinon il faut scanner le QR-code en sélectionnant le bouton **Numériser le QR code**. Comme pour la clé privée, l'appareil photo est activé, il faut bien viser ! Si nécessaire faire avancer / reculer le smartphone pour provoquer la saisie de l'image.

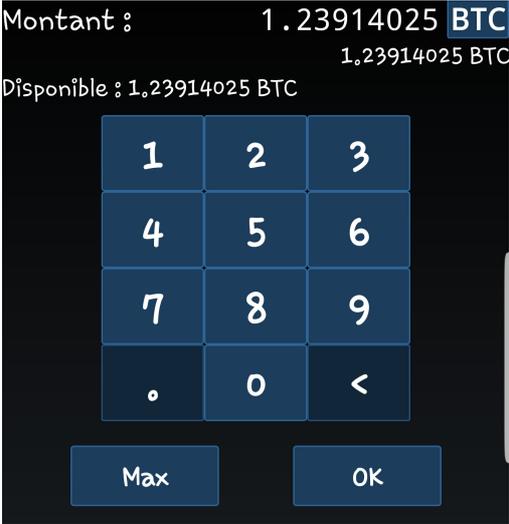
Lorsque la clé publique du destinataire est décodée elle est affichée :

Adresse du destinataire
3HD5snnh4pBb
Z1QweREMRKxZ
rwQYiXqjm9
Étiquette de transaction
Kraken

Il faut alors sélectionner le bouton qui représente un clavier :



On obtient un affichage similaire à celui ci :



C'est là qu'il faut saisir le montant en BTC qui doit être transféré. On peut également sélectionner le bouton **Max** pour vider complètement le portefeuille papier, c'est ce qui a été fait dans l'exemple ci-dessus. Lorsque le montant est saisi, sélectionner le bouton **OK**. On revient à l'écran précédent :



Avant de valider, on peut choisir le montant des frais en millième de BTC (mBTC). Ce montant est converti en \$ en fonction du cours actuel du BTC. Sélectionner ensuite le bouton **Envoyer**. Un écran relativement furtif s'affiche, puis on revient à l'écran d'accueil de Mycelium.

Vérier...

La transaction vient d'être envoyée sur le réseau bitcoin et elle est visible sur le site blockchain.info à l'aide du PC, de la tablette ou du smartphone. Cela se fait selon la méthode expliquée [ici](#).

Sommaire	Transactions
Adresse 3HD5snnh4pBbZ1QweREMRKxZrwQYXqjm9	Nb de transactions 27
Hash 160 aa39aa3e48b739bfa7d8b923f6205e9f7f4f3509	Total reçu 20.39440839 BTC
Outils Tags en relation - Outputs non-dépensés	Solde final 1.23914025 BTC

[Demande de paiement](#) [Bouton de donation](#)



Transactions (Les plus anciennes en premier) Filtre ▾

96a2be078af254388f0bb9f2625817496ed74c2f8330aa553a902f6758a3b78	2017-09-19 16:37:16
132kvhUHuRjG9LZRF91z7m4pkgEyRDBkAx	1.23914025 BTC
➔	
3HD5snnh4pBbZ1QweREMRKxZrwQYXqjm9	1.23914025 BTC
Transaction non confirmée ! 1.23914025 BTC	

Là on peut voir le montant et l'heure de la transaction et reconnaître les adresses publiques d'origine et de destination utilisées dans les exemples. Cette transaction n'est pas encore confirmée.

Voici un autre exemple qui illustre le résultat d'un vidage partiel de porte monnaie. Ceci est un extrait de la page web [18x4bw...FKNZ](#) :

1ae8043b62719ce92c8afcf86c27f796f27f70fa9a8bd78cac47a017c3018cf	2017-06-13 13:06:55
18x4bwvcyup8z54nqcNn9aVcH8DexiFKNZ	0.66969689 BTC
➔	
18x4bwvcyup8z54nqcNn9aVcH8DexiFKNZ	0.4884 BTC
1KKncHb1PxpLqTvK4kTUnmBbPzK2DGn6DW	0.4884 BTC
-0.48936311 BTC	

Le 13 juin 2017 un porte-monnaie papier *18X4bw...FKNZ* a été partiellement vidé selon la méthode expliquée auparavant. Le contenu initial du porte-monnaie papier expéditeur était de **1,15906 BTC**. Ce montant a été réparti comme ceci :

0,4884 BTC pour le porte monnaie destinataire *1KKnc...n6DW*
0,00096311 BTC pour les frais de transaction
0,66969689 BTC retourne dans le porte monnaie expéditeur comme rendu de monnaie

Commentaires concernant la sécurité et les clés

Ne pas oublier : si la clé privée qui a servie à l'opération de transfert se trouve stockée au format texte dans le smartphone, il très fortement conseillé de supprimer le fichier qui la contient.

Au moment de la numérisation du QR-code par *Mycelium*, puis au moment de l'envoi de la transaction sur le réseau, la clé privée secrète ne circule pas sur internet. Elle reste confinée dans le smartphone. Elle sert à crypter les données de la transaction. Ce sont ces données qui sont envoyées vers le réseau Bitcoin. Cette clé n'est pas stockée dans le smartphone non plus, elle est effacée et oubliée lorsque l'application *Mycelium* est fermée.

La clé privée utilisée dans les copies d'écran ci-dessus a réellement servie à effectuer la transaction montrée dans les exemples. Maintenant cette clé est "grillée". Evidement il est totalement déconseillé de s'en servir à nouveau !

