

Tuto pour sécuriser de vos RealToken avec le hardware wallet Ledger



Pourquoi ajouter ce niveau de protection :

L'identité des acheteurs de RealToken étant connue de RealT (via les procédures : KYC et Whitelist), vous pensez peut être que vos RealToken ne peuvent être volés ..

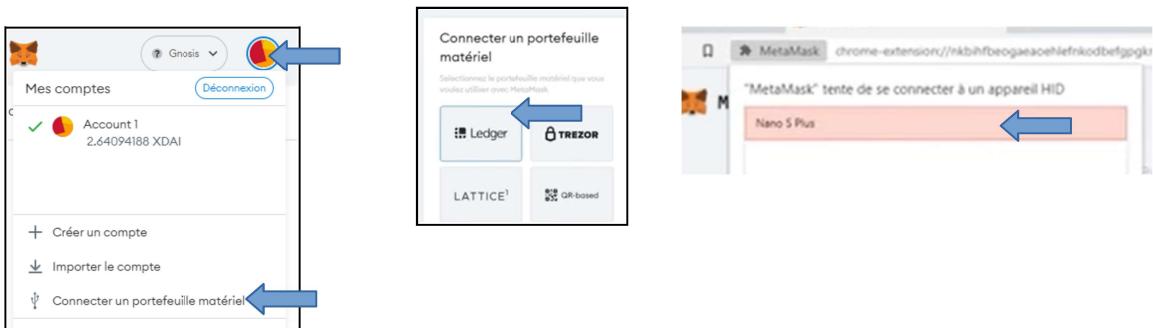
Sauf, si votre *seed phrase* (stockée dans le logiciel MetaMask) tombe entre de mauvaises mains : le hacker, usurpant alors votre identité, vendra vos RealToken (en votre nom) sur un échangeur (Swapcat, 1inch, Levinswap), puis récupérera l'argent correspondant.

Bien que RealT puisse bloquer/détruire/recréer les RealToken (en cas de perte de wallet, par ex.), ils ne pourront rien faire suite à ce vol car les RealToken auront été acquis de bonne foi par de nouveaux acheteurs :-(

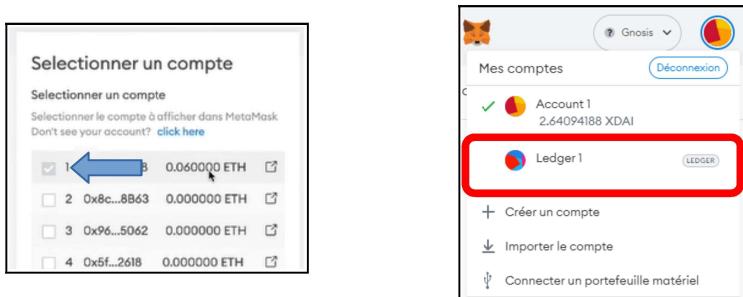
Nota : En complément du transfert de vos RealToken sur un hardware wallet (Ledger, dans ce tuto), à la fin du document une protection supplémentaire est détaillée : afin qu'un mail vous soit adressé à chaque transaction sur votre wallet « coffre fort ».

Etape 1 : Initialisation de la Nano et création du wallet Ledger :

- Initialisation de la Nano S Plus : <https://support.Ledger.com/hc/fr-fr/articles/4416927988625-Configurer-votre-Ledger-Nano-S-Plus?-docs=true>
 - Il faut initialiser la Nano comme un « *New Device* », afin qu'elle crée un nouveau wallet (/compte) dont la clé privée sera sur ce matériel (donc plus sécurisée...),
 - Une nouvelle *Seed Phrase* va être générée, pour ce nouveau compte Ledger (en plus de celle que vous avez déjà pour le compte MetaMask). Bien veiller à sa protection !...
- A partir de l'application *Ledger Live* : installer l'application Ethereum sur la Nano (afin qu'elle puisse gérer cette blockchain et les EVM compatibles comme Gnosis).
L'application Ledger Live ne supportant pas Gnosis, l'accès au compte Ledger sur cette blockchain va se faire via MetaMask.
- Sur la Nano, activer l'option « *Blind signing* » :
<https://support.Ledger.com/hc/fr-fr/articles/4405481324433-Activer-l-option-de-signature-aveugle-dans-l-application-Ethereum-ETH?-docs=true>
- Sur MetaMask, création de l'accès au wallet Ledger :
(la nano étant branchée, le pin code entré et l'application Ethereum lancée)



Sélectionner un des comptes de la Nano (le 1er par ex), qui va maintenant apparaître dans MetaMask

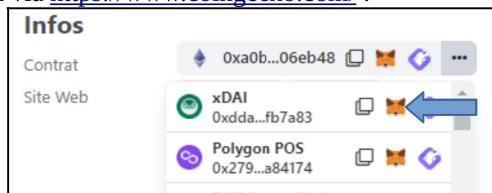


Si Pb : <https://support.ledger.com/hc/fr-fr/articles/360020871157-Résoudre-un-problème-de-connexion-à-MetaMask>

Vous avez donc maintenant deux comptes (donc deux phrases de récupération !...) :

- l'adresse existante sur MetaMask (où sont vos RealToken et autres fonds) et dont la clé privée est stockée dans votre browser (cad moyennement sécurisée...)
- une nouvelle adresse Ledger, dont la clé privée est stockée sur la Nano (donc bien mieux protégée...).

Nota : il sera nécessaire d'ajouter, sur le nouveau compte Ledger dans MetaMask, les jetons dont vous avez besoin sur la blockchain Gnosis (USDC, WXDAI,...), comme vous l'avez fait par le passé sur le compte MetaMask d'origine. Par ex via <https://www.coingecko.com/> :



Vous aurez aussi besoin d'un peu de xDai sur chacun des 2 comptes, pour faire des transferts et transactions sur Gnosis.

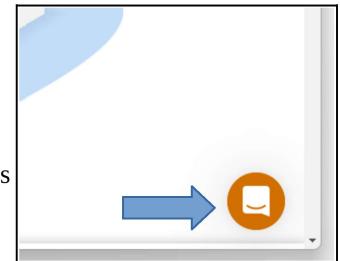
Etape 2 : Demander à RealT de whilister votre nouvelle adresse Ledger

Sur l'application RealT, via la bulle en bas à droite, vous devez demander au support d'autoriser la modification (sur le portfolio) de vos adresses.

Puis, faire les modifications suivantes :

- sur l'adresse « Property Wallet » : indiquer la nouvelle adresse Ledger pour la livraison de vos RealToken,
- voire sur l'adresse « Rent Wallet », indiquer la nouvelle adresse Ledger si vous souhaitez que vos loyers soient versés sur le compte Ledger.

Cette dernière modification est à éviter, si vous souhaitez réinvestir chaque semaine vos loyers et dédier la Nano à une fonction de « coffre fort » (voir le chapitre « changements de vos usages, avec la Nano»)



Nota : votre nouvelle adresse (Ledger) sera aussi whitelistée pour l'ensemble des propriétés pour lesquelles vous auriez déjà fait des demandes avec votre adresse d'origine (MetaMask).

Etape 3 : Transfert de vos RealToken du compte MetaMask au compte Ledger

Préalable RMM :

Si votre RealToken est en collateral sur le RMM (donc pas sur votre wallet), vous devrez au préalable le retirer du RMM ... donc, suivant votre Health Factor, de rembourser l'emprunt correspondant .. donc de disposer des xDai nécessaires !

Une fois le transfert du RealToken vers le compte Ledger réalisé : vous pourrez (à partir du compte Ledger) remettre le RealToken en collateral et réemprunter. (voire, suivant vos disponibilités : de transférer les xDai empruntés du compte Ledger vers le compte MetaMask, pour refaire la même opération pour un autre RealToken sur le RMM)

Pour transférer vos RealToken, ils doivent s'afficher sur votre application wallet. Ce que MetaMask ne fait pas par défaut. Il existe par contre un wallet mobile, qui affiche par défaut tous les RealToken : c'est *RealT Wallet*.

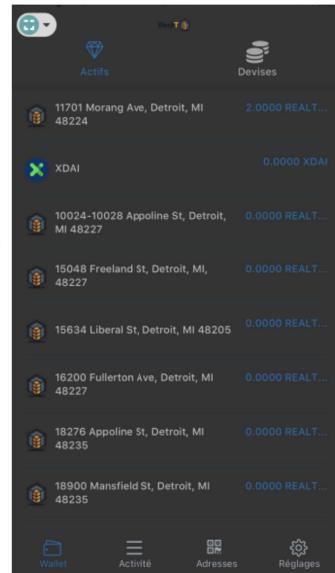
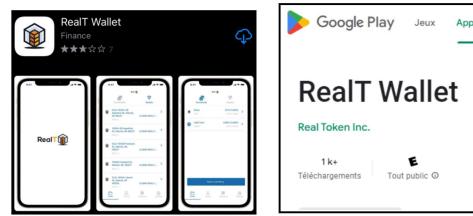
Deux solutions de transfert seront donc présentées ci-après : à partir de *RealT Wallet* et à partir de Metamask.

Transfert à partir de l'application mobile RealT Wallet

Pour ce faire, vous devez installer l'application mobile sur votre smartphone :

Importer votre seed phrase MetaMask dans le RealT Wallet.

Attention de ne surtout pas vous tromper, en utilisant la nouvelle seed phrase du compte Ledger (pour des raisons de sécurité, cette dernière doit être réservée à une restauration sur un hardware wallet et jamais sur un software wallet)



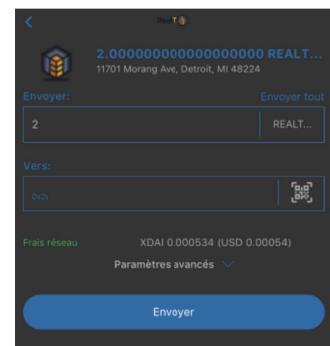
Passer sur la blockchain Gnosis (en haut à gauche) et vous voyez apparaître les RealToken que vous possédez (ici 2 Morang) et ensuite tous les autres (> 250).

Le transfert se fait alors simplement :

En cliquant sur le realtoken possédé et en faisant envoyer



En faisant « envoyer tout » puis en scanant l'adresse du compte Ledger cible (*)



(*) : le Qrcode s'obtient en allant sur Metamask, en étant positionné sur le compte Ledger (et pas sur le compte Metamask , nommé account1 dans les exemples ci-avant), en cliquant sur les trois petits points en haut à droite, en choisissant « détail du compte ».



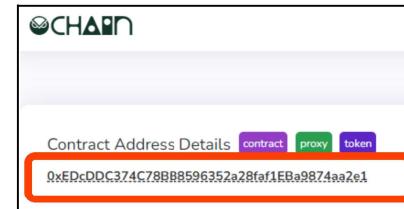
Une fois les transferts réalisés, si vous ne souhaitez plus utiliser l'application mobile RealT Wallet , avant d'effacer l'application de votre smartphone, il est souhaitable : d'aller dans Réglage, puis Connexion et Sécurité et « effacer les données du téléphone ». Ainsi la seed Phrase que vous avez rentrée à l'initialisation de l'application mobile sera effacée du smartphone.

Transfert à partir de MetaMask

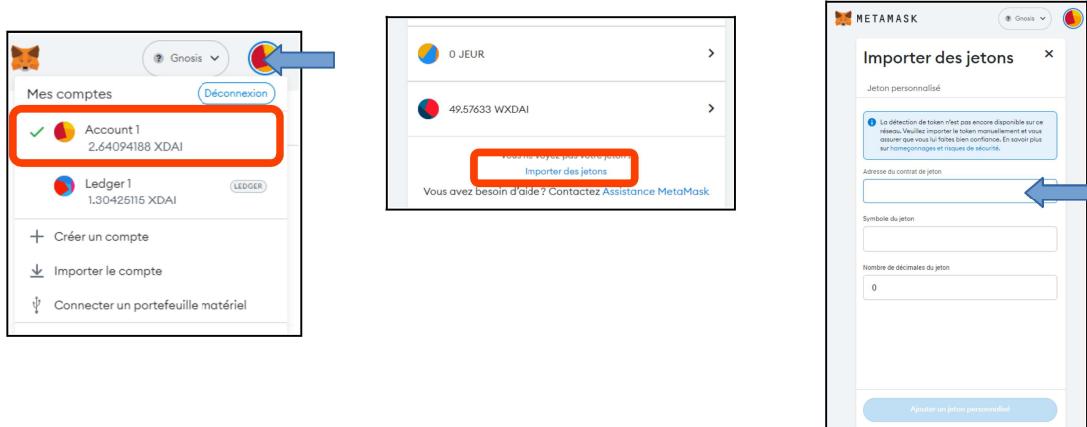
- Dans cette solution, il faut faire afficher (un à un, d'où le coté fastidieux ..) les RealToken sur votre MetaMask:
 - Trouver l'adresse gnosis du RealToken : A partir de votre portfolio, cliquer sur « xDai » en haut à droite de l'onglet de la propriété



- Copier l'adresse qui apparaît dans blockscout :



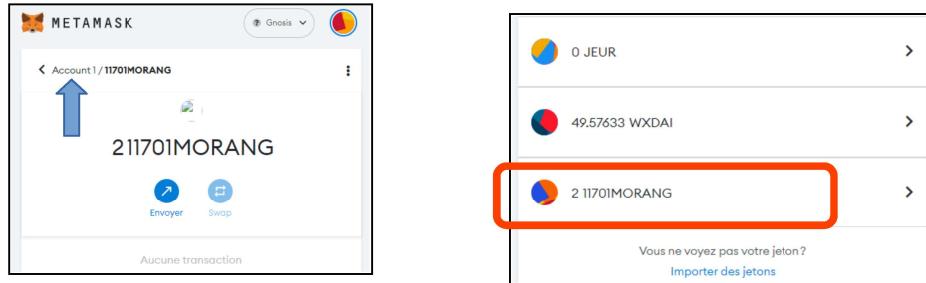
- L'ajouter comme un nouveau Jeton dans le compte MetaMask (ici nommé Account1)



- après avoir collé l'adresse du RealToken dans la partie Adresse : modifier le nom Symbole du token pour le réduire à 11 caractères et importer le jeton :

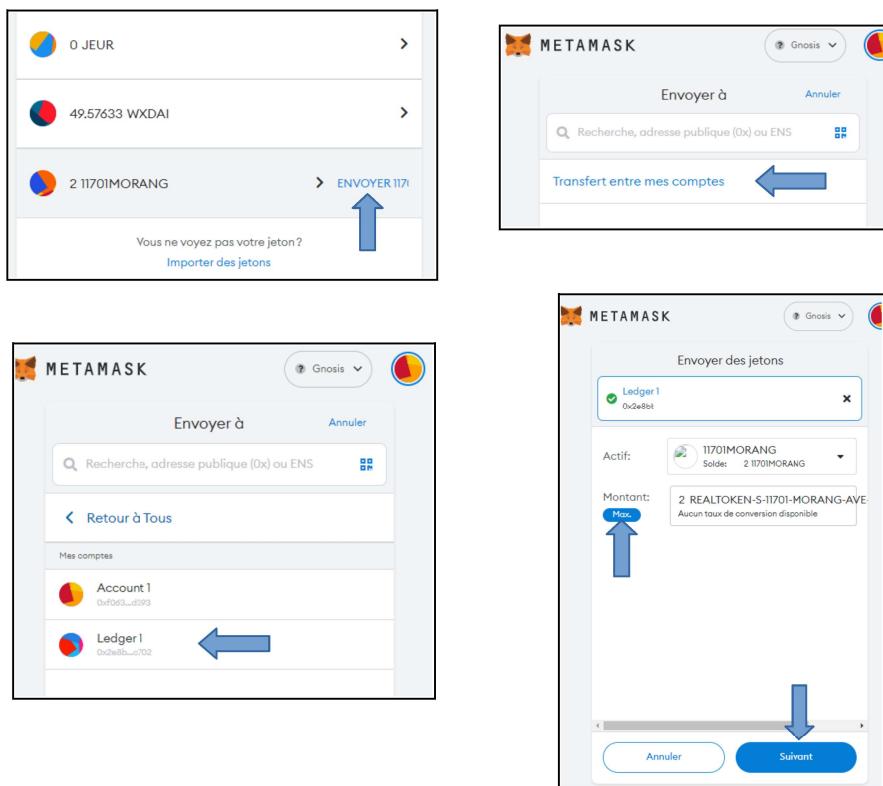


- En cliquant (en haut à gauche) sur « Account1 » on revient à la liste des jetons sur le compte MetaMask et le RealToken est apparu (en fin de liste) ainsi que le nombre de RealToken possédé (le premier chiffre, 2 ici, devant le nom symbole du RealToken)



- Transfert du compte MetaMask vers Ledger

A partir du Compte MetaMask :



Après confirmation, le RealToken est transféré.

Si vous souhaitez afficher le RealToken transféré sur le compte Ledger, il faudra ajouter le jeton de ce RealToken sur le compte Ledger (comme on l'a fait précédemment sur le compte MetaMask).

Changements dans vos usages, avec la Nano:

Pour vos Comptes :

Vous disposez donc maintenant de deux comptes (voir plus ..). Ils sont tout les deux accessibles par MetaMask et vous passez de l'un à l'autre via le rond coloré en haut à droite de MetaMask :



Pour un maximum de sécurité, il est préférable de « spécialiser » les usages des deux comptes :

- Le compte MetaMask (d'origine), pour la fonction de « porte-monnaie » (ou « hot wallet »)
 - Pour vos transactions au quotidien avec la Defi,

- Les approbations sur ce compte sont uniquement sur MetaMask (aucune action sur la Nano),
- Avec des fonds limité sur ce compte, puisque qu'il est moins sécurisé : clé privée sur le browser, nombreuses autorisations / accès données lors des transactions,...
- Le compte Ledger, pour la fonction de « coffre fort » (ou « cold wallet »):
 - Pour sécuriser au maximum vos RealToken et vos fonds plus conséquents,
 - En limitant au maximum les accès / approbations sur la defi avec ce compte (*),
 - Les approbations nécessiteront des étapes supplémentaires : Nano branchée, code pin entré, application Ethereum activée, puis après l'approbation MetaMask : revue des détails de la transaction, et approbation sur la Nano,
 - Le plugin MetaMask assurant juste le lien entre les applications et le compte sur la Ledger (dont le clé privée reste sur ce matériel).

En cas de perte, vol ou destruction de la Nano :

- Elle est protégée par son code PIN,
- La Nano se réinitialise après 3 tentatives de code PIN infructueuses,
- Vous pouvez réinstaller votre compte Ledger sur une nouvelle Nano (ou l'ancienne, par ex pour tester votre procédure de sauvegarde : action souhaitable, lors d'un premier usage..) à partir de la seed Phrase générée en étape 1.
- Voir recréer un nouveau wallet Ledger sur une nouvelle Nano. Après transfert, l'ancienne sera ainsi vidée.

Pour vos transactions de RealToken :

- Achat :
 - Sur le site RealT : Vous pouvez payer, avec le compte MetaMask (via Request Finance) et être livré des RealToken directement sur le compte Ledger. Solution bien utile, quand on souhaite acheter sans avoir sa Nano avec soi...
 - Sur Swapcat : Là, par contre l'adresse de paiement est celle de livraison des RealToken.
- Loyers :
 - Suivant vos choix en étape 2, ils seront versés sur sur l'un ou l'autre des comptes.
 - Si vous avez opté pour une maison de réinvestissement, la quantité de RealToken correspondante sera envoyée directement sur le compte Ledger.
 - L'état hebdomadaire, envoyé par RealT, fait la séparation des montants pour chacun des deux comptes.
- RMM :
 - Pour mettre en collateral les RealToken de votre compte Ledger, il faudra alors connecter le compte Ledger au RMM et confirmer les ajouts/retraits via la Nano. Les preuves de dépôt et les xDai empruntés seront sur le compte Ledger.
 - Pour le RMM, les deux comptes sont séparés, il n'y pas de consolidation (notamment au niveau du Health Factor) entre les deux comptes.

(*) Exemple d'arnaques, malgré l'usage de Ledger : <https://www.Ledger.com/academy/smart-contract-functions-essential-red-flags-to-know-about>

Pour vos *Seed Phrase* :

- Celle d'origine du compte Metamask :
 - C'est la moins sécurisée, car stockée dans un logiciel (le plugin de votre browser). Vous pouvez d'ailleurs retrouver la clé privée associée dans MetaMask via : les trois petits points > Détail du compte > Exporter la clé privée,
 - Elle ne sert que pour importer ou réinstaller ce compte sur un Software Wallet (PC ou mobile),
 - Elle ne doit jamais être utilisée pour créer un compte Ledger (elle pourrait avoir été corrompue...).
- Celle du nouveau compte Ledger :
 - C'est la plus sécurisé, car nouvellement générée et stockée uniquement dans le matériel Ledger. Vous ne pouvez d'ailleurs pas retrouver la clé privée associée dans MetaMask ...,
 - Elle ne sert que pour réinstaller ce compte sur un Hardware Wallet (comme le matériel Ledger),
 - Elle ne doit jamais être utilisée pour importer ou réinstaller le compte Ledger sur un Software Wallet (PC ou mobile),
 - Si vous avez besoin de lier ce compte, dans Bridge Wallet par ex : il faut utiliser la clé publique.
- Et qu'en est il des comptes supplémentaires, que l'on peut créer dans MetaMask ...
 - Ils sont rattachés à la *Seed Phrase* MetaMask,

- Si vous supprimez le plugin MetaMask de votre browser, vous pourrez retrouver ces comptes supplémentaires après avoir réinstallé MetaMask (avec sa *Seed Phrase*), en faisant à nouveau « *créer un compte* ». Ils réapparaîtront avec la même clé publique que précédemment (et donc avec les jetons associés).

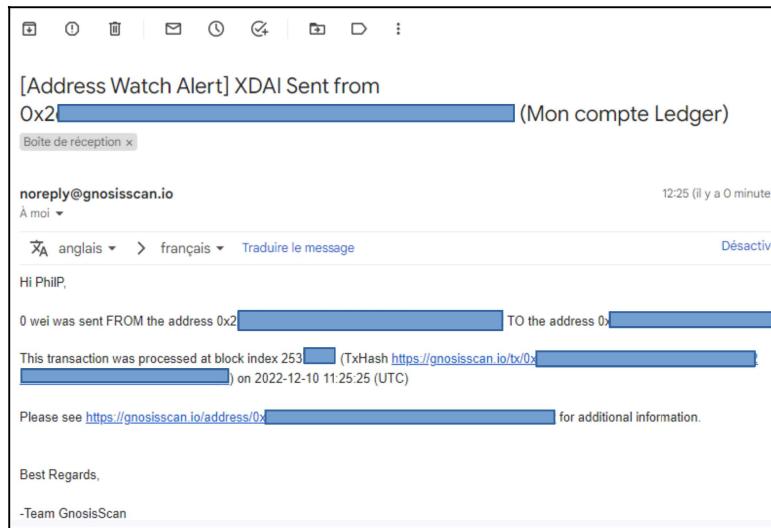
Alerte par email des mouvements sur votre wallet

Les mouvements surveillés sont sur la blockchain Gnosis. Pour ce faire :

- ouvrir un compte : <https://gnosisscan.io/register> :

- ajouter l'adresse de votre wallet à surveiller :

Et voilà le genre de mail que vous recevrez, lors d'un mouvement :



Fin 😊

(PhilP – V3 Dec - 2022)