

> wallet de conservation · 2 parts sur 3 · aucun serveur

[SEEDLESS WALLET]

Un portefeuille crypto de conservation, sans phrase secrète à recopier.

Mode d'emploi pour grand débutant.

Ce guide suppose que tu n'as jamais utilisé de portefeuille crypto. Chaque mot technique est expliqué la première fois qu'il apparaît, et un lexique complet se trouve page 4.

Version : prototype sur le réseau de test Sepolia (faux ETH, aucune valeur réelle).

Matériel de référence : clé de sécurité YubiKey 5C NFC. Le wallet fonctionne avec toute clé de sécurité FIDO2 compatible, et avec une passkey Apple, Android ou Windows.

[1. Avant de commencer]

Ce wallet sert à **une seule chose** : garder des cryptomonnaies en sécurité et les envoyer à quelqu'un quand tu le décides. C'est un coffre, pas un couteau suisse.

> Ce qu'il fait

- > Créer un portefeuille (une adresse) sans jamais te montrer de phrase secrète à recopier.
- > Afficher ton solde.
- > Envoyer des ETH à une adresse que tu tapes toi-même.
- > Te permettre de le récupérer sur n'importe quel appareil, sans fichier, avec 2 de tes 3 « clés ».

> Ce qu'il ne fait pas, volontairement

- > Il ne se connecte à aucun site web ni application tierce (pas de DeFi, pas de NFT, pas de « Connect wallet »).
- > Il ne signe rien d'autre que des envois d'ETH que tu as toi-même remplis.
- > Il ne crée aucun fichier de sauvegarde à télécharger : c'est voulu, pour qu'aucun mauvais clic ne puisse faire fuiter quoi que ce soit.
- > Il te retient tant que la sauvegarde n'est pas publiée sur la blockchain : tu peux déposer de quoi payer les frais, mais pas plus. Le vrai dépôt attend la sauvegarde complète.

> Version de test

Pour le moment, le wallet tourne sur **Sepolia**, un réseau d'entraînement d'Ethereum. Les ETH qu'on y manipule sont des faux, sans aucune valeur. C'est fait exprès : on apprend, on casse, on recommence, sans risque. N'envoie jamais de vrais ETH à une adresse de ce prototype.

[2. L'idée, en deux minutes]

Un portefeuille crypto, c'est en réalité un **nombre secret** (la « clé privée »). Qui connaît ce nombre peut dépenser l'argent. D'habitude, on te demande de le recopier sous forme de 12 ou 24 mots (la « seed phrase ») et de les cacher. Si quelqu'un trouve le papier, il a tout. Si tu perds le papier, tu as tout perdu.

Seedless Wallet fait autrement. Le nombre secret est **découpé en 3 morceaux**, et il faut **2 morceaux sur 3** pour le reconstituer :

MOT	CE QUE ÇA VEUT DIRE, SIMPLEMENT
Morceau A	Protégé par une clé de sécurité physique (YubiKey ou autre clé FIDO2). Tu peux en enrôler plusieurs : n'importe laquelle suffit.
Morceau B	Protégé par la passkey de ton téléphone ou ordinateur (Face ID, Touch ID, empreinte Android, Windows Hello).

MOT	CE QUE ÇA VEUT DIRE, SIMPLEMENT
Morceau C	Protégé par une passphrase : une longue phrase de passe que tu es le seul à connaître.

Un seul morceau ne sert à rien, même entre les mains d'un expert : c'est mathématique, pas une question de puissance de calcul. Et comme il n'en faut que deux, tu peux perdre n'importe lequel des trois sans perdre ton argent.

> Le point à retenir

Tu n'as rien à recopier. Ton coffre s'ouvre avec 2 choses parmi : ta clé physique, ton visage ou ton doigt sur ton appareil, ta phrase de passe.

Les 3 morceaux chiffrés sont publiés sur la blockchain, dans un petit registre public. Ça ne révèle rien (ils sont illisibles sans tes clés), mais ça permet de retrouver ton wallet depuis n'importe quel navigateur, en touchant simplement ta clé. Pas de fichier, pas de papier, pas de serveur.

[3. Le lexique]

Tout le jargon du guide, dans l'ordre où tu le rencontreras.

MOT	CE QUE ÇA VEUT DIRE, SIMPLEMENT
Wallet (portefeuille)	Le logiciel qui garde ton nombre secret et te permet d'envoyer des cryptos. Ici, c'est une simple page web qui tourne dans ton navigateur.
Adresse	Ton « numéro de compte » public, qui commence par 0x suivi de 40 caractères. Tu peux la donner à n'importe qui pour recevoir des ETH.
Clé privée	Le nombre secret qui contrôle l'adresse. Ici, il n'est jamais affiché, jamais écrit : il n'existe que quelques millisecondes en mémoire quand tu envoies de l'argent.
Seed phrase	Les 12 ou 24 mots des wallets classiques. Seedless Wallet n'en a pas, c'est tout son intérêt.
secp256k1	Le nom de la formule mathématique qu'Ethereum utilise pour relier une clé privée à une adresse. Tu n'as rien à en faire, c'est juste pour savoir ce que c'est si tu le croises.
Shamir (partage de secret)	La méthode qui découpe la clé privée en 3 morceaux dont 2 suffisent. Inventée en 1979, utilisée partout en sécurité.
Clé de sécurité / FIDO2	Une petite clé USB (ou NFC) qui prouve que c'est bien toi. YubiKey est la marque la plus connue ; FIDO2 est le standard, donc d'autres marques fonctionnent (SoloKeys, Nitrokey, Token2, Feitian, Google Titan récentes...).
PIN FIDO2	Le code que tu dois taper pour utiliser ta clé de sécurité. Il se définit une fois, avec l'application du fabricant (Yubico Authenticator pour une YubiKey). Après 8 erreurs, la clé se verrouille.

MOT	CE QUE ÇA VEUT DIRE, SIMPLEMENT
Passkey	Une « clé » rangée dans ton téléphone ou ordinateur, déverrouillée par ton visage, ton doigt ou ton code. Chez Apple elle se synchronise par iCloud, chez Google par ton compte Google, chez Microsoft par Windows Hello.
PRF	Une capacité des clés de sécurité et des passkeys récentes : produire un code secret stable que personne ne peut extraire. C'est ce code qui verrouille ton morceau A ou B.
Passphrase	Une phrase de passe longue (12 caractères minimum, 4 ou 5 mots conseillés). Contrairement à une seed phrase, elle ne donne pas accès à l'argent toute seule.
Touche / cérémonie	Quand le navigateur te demande de toucher ta clé ou de valider par Face ID. L'enrôlement d'une clé demande 2 ou 3 touches de suite, c'est normal.
Facteur	Dans l'app : un moyen d'ouvrir un morceau. Une clé de sécurité, une passkey ou la passphrase. Pour signer, on choisit 2 facteurs de morceaux différents.
Blockchain / on-chain	Le registre public et partagé où vivent les transactions. « On-chain » veut dire « écrit sur la blockchain ».
Ethereum / ETH	La blockchain utilisée ici, et sa monnaie.
Sepolia	La copie d'entraînement d'Ethereum. Mêmes règles, mais les ETH y sont gratuits et sans valeur. On y apprend sans risque.
Faucet	Un site qui distribue gratuitement des ETH de test Sepolia. Il suffit de lui donner ton adresse.
RPC	Le « nœud » : le serveur par lequel ton navigateur lit la blockchain et envoie tes transactions. Il ne voit jamais ta clé, seulement des transactions déjà signées. L'app en propose un par défaut, tu peux en mettre un autre.
Gas / frais	Le petit coût de chaque transaction, payé en ETH. Sur Sepolia, c'est gratuit en pratique.
Transaction / tx	Une opération écrite sur la blockchain : un envoi, un dépôt de sauvegarde, etc. Chaque transaction a un identifiant unique (son « hash »).
Etherscan	Un site qui permet de voir n'importe quelle adresse ou transaction sur la blockchain. L'app y renvoie par des liens.
Registre	Le petit programme (contrat) sur la blockchain où l'app dépose tes 3 morceaux chiffrés. Il est déjà configuré, tu n'as rien à faire.
Publier la sauvegarde	L'action de déposer tes morceaux chiffrés dans le registre. Indispensable : sans ça, ton wallet n'existe que dans le navigateur où tu l'as créé.
Token / ERC-20 / NFT	Un token est une monnaie ou un objet qui vit sur Ethereum en plus de l'ETH. ERC-20 est le format des tokens « monnaie », les NFT sont les objets uniques (ERC-721 / 1155).
Autorisation (allowance)	Permission donnée à un contrat de dépenser un de tes tokens à ta place. Utile pour la DeFi, inutile pour un wallet de conservation : à révoquer si tu en trouves.

[4. Ce qu'il te faut]

MOT	CE QUE ÇA VEUT DIRE, SIMPLEMENT
Une clé de sécurité	YubiKey 5 (firmware 5.2.3 ou plus récent) ou toute clé FIDO2 qui gère les « credentials résidents » et l'extension PRF (hmac-secret). Sur iPad et iPhone, il faut une clé USB-C ou Lightning : l'iPad ne lit pas les clés en NFC. Idéalement 2 ou 3 clés, pour en avoir une de secours.
Un appareil avec passkey	iPhone, iPad ou Mac (Face ID / Touch ID), téléphone Android, ou PC Windows avec Windows Hello. C'est lui qui portera le morceau B.
Un navigateur récent	Safari 18 ou plus (iOS 18, macOS Sequoia), Chrome 116 ou plus, Brave, Edge. Firefox ne gère pas encore la PRF.
Une passphrase	À choisir maintenant : 4 ou 5 mots au hasard, faciles à retenir pour toi, impossibles à deviner. Exemple de forme : « tortue cuivre lanterne fjord 2026 ». N'utilise pas celle-ci.
5 minutes de calme	L'enrôlement demande plusieurs touches de clé à la suite. Pas de stress, chaque étape explique ce qu'elle attend.

> Préparer ta clé de sécurité (une seule fois)

Ta clé doit avoir un **PIN FIDO2**. Sans lui, le navigateur l'ignore et tu verras une erreur sans que la clé ne clignote.

01	Installe l'application du fabricant Pour une YubiKey : Yubico Authenticator (gratuite, sur iPhone, iPad, Mac, Windows, Android). Pour une autre marque : son outil équivalent, ou les réglages de sécurité de Windows / Chrome.
02	Branche la clé et ouvre l'onglet Passkeys (ou FIDO) Tu y verras « Définir le PIN » si aucun PIN n'existe.
03	Choisis un PIN de 6 chiffres ou plus Note-le quelque part de sûr. Ce n'est pas le PIN de ta carte bancaire ni celui de ton téléphone : il est propre à la clé. Après 8 erreurs d'affilée, la clé se bloque définitivement.

> Pourquoi un PIN sur la clé ?

Pour que la clé, volée ou perdue, ne serve à rien à celui qui la ramasse. Trois barrières : il faut **avoir** la clé, **savoir** son PIN, et il manquerait encore un deuxième morceau.

[5. Créer ton wallet]

Ouvre le site du wallet dans ton navigateur et clique sur **Commencer**. Les boutons se débloquent dans l'ordre : tant qu'une étape n'est pas finie, la suivante reste grisée. Tu ne peux pas te tromper d'ordre.

01	Générer la clé et la découper Un clic. Le navigateur tire un nombre secret au hasard et le découpe en 3 morceaux. Ton adresse (0x...) apparaît. Rien n'est encore enregistré nulle part.
02	Enrôler ta clé de sécurité (morceau A) Donne d'abord un nom à ta clé dans le champ au-dessus du bouton (facultatif mais conseillé : « YubiKey bleue », « clé du bureau »). C'est ce nom que tu verras partout, y compris dans Yubico Authenticator. Puis clique sur « Enrôler la clé de sécurité 1 ». Le navigateur te demande de brancher la clé, taper son PIN et la toucher. Ensuite le bouton change de nom (« touche 2/3 : lecture... ») : reclique, retape le PIN, retouche. Puis une dernière fois pour le contrôle. Sur Chrome c'est 2 touches, sur Safari 3. La carte « Part A » passe en vert.
03	Ajouter une autre clé (facultatif, conseillé) « + Ajouter une autre clé de sécurité » et recommence avec ta deuxième clé. Chaque clé reçoit le même morceau A : n'importe laquelle suffira plus tard. Tu pourras aussi en ajouter après coup.
04	Enrôler ta passkey (morceau B) Clique sur « Enrôler la passkey ». Ton appareil te propose Face ID, Touch ID, ton empreinte ou ton code. Valide, puis reclique pour la touche de contrôle. La carte « Part B » passe en vert.
05	Chiffrer le morceau C avec ta passphrase Tape ta passphrase deux fois, puis « Chiffrer la part C ». L'app vérifie aussitôt qu'elle sait la rouvrir. Carte « Part C » en vert.
06	Terminer Le nombre secret et les morceaux sont effacés de la mémoire. Tu arrives sur l'écran principal, avec un bandeau rouge et l'adresse masquée : à partir de là, trois règles jusqu'à la publication (chapitre 6) : ne mets aucun fonds dessus, ne ferme pas la page, publie d'abord. Le navigateur te retient d'ailleurs si tu tentes de fermer l'onglet.

> Les fenêtres qui reviennent, c'est normal

Chaque « touche » est une fenêtre du navigateur. Si une fenêtre réapparaît juste après que tu as touché la clé, ce n'est pas un bug ni un retour en arrière : c'est l'étape suivante. Ne la ferme pas. Si tu la fermes par réflexe, l'app affiche « cérémonie annulée » : reclique sur le bouton, ça reprend à la même touche.

> Dans ton appareil, comment ça s'appelle

Dans Yubico Authenticator (onglet Passkeys) ou dans Réglages > Mots de passe (Apple), tes enrôlements apparaissent sous le nom « Seedless A1 · 0x1234...abcd » : la lettre du morceau, le numéro de la clé, et le début de ton adresse. Pratique pour t'y retrouver si tu crées plusieurs wallets.

[6. Publier ta sauvegarde (avant toute chose)]

Pour l'instant, ton wallet n'existe que dans ce navigateur. Si tu vides son historique ou changes d'appareil, il est perdu. La sauvegarde consiste à déposer tes 3 morceaux **chiffrés** sur la blockchain, dans le registre. Personne ne peut les lire, mais toi tu pourras les retrouver partout.

> Tant que ce n'est pas fait, l'app te bloque

Adresse masquée, pas de bouton Copier, pas d'envoi. C'est volontaire : on ne met **jamais** de fonds sur un wallet non sauvegardé. Une seule exception, expliquée ci-dessous : le strict minimum pour payer les frais de la publication.

01 Récupère juste de quoi payer les frais

Publier est une transaction, donc elle coûte quelques frais (gratuits sur Sepolia, quelques centimes d'ETH sur un vrai réseau). Clique « Afficher l'adresse pour payer les frais de publication », copie l'adresse, et demande une petite somme à un faucet Sepolia (cherche « Sepolia faucet » : Google Cloud, Alchemy, Infura, ou un faucet « PoW »). Clique « Rafraîchir » : le solde apparaît au bout d'une à quelques minutes.

02 Choisis 2 facteurs

Dans « Facteurs de signature », clique sur 2 pastilles de morceaux différents, par exemple « A · Clé 1 » et « C · Passphrase », et tape ta passphrase. (Deux clés de sécurité ensemble ne marchent pas : elles portent le même morceau.)

03 Clique « Publier la sauvegarde on-chain »

L'app te demande une touche pour **chaque** clé de sécurité et passkey enrôlée (pour calculer les index de recherche), puis une dernière validation pour signer la transaction.

04 Attends « sauvegarde publiée »

Quelques secondes. Le bandeau passe en vert, le bouton devient grisé « Sauvegarde on-chain à jour », l'adresse complète et la section « Envoyer » apparaissent. C'est fait, pour toujours.

> Quand republier ?

Seulement si tu ajoutes ou retires une clé. L'app le signale avec un bandeau jaune et réactive le bouton. Le reste du temps, il n'y a rien à faire.

> Ce qui est visible publiquement

Ton adresse, le nombre et le type de facteurs, et des blocs chiffrés illisibles. Jamais ta clé privée, jamais ta passphrase, jamais rien qui permette de dépenser.

[7. Mettre des ETH de test dessus]

Maintenant que la sauvegarde est publiée, l'adresse est affichée en entier et le bouton « Copier l'adresse » est disponible. Donne-la à un faucet Sepolia, ou à un ami qui veut t'envoyer des ETH de test, et clique « Rafraîchir » pour voir le solde.

Le bouton « Etherscan » ouvre la page publique de ton adresse. Tu y verras arriver les ETH de test, et plus tard toutes tes transactions.

> Pas de panique si le solde tarde

Un faucet peut mettre une à quelques minutes. Si « Rafraîchir » affiche un point d'interrogation, c'est le nœud RPC qui ne répond pas : attends un peu ou change de RPC (section « Sauvegarde et maintenance »).

[8. Envoyer des ETH]

01 Choisir 2 facteurs

Deux pastilles de morceaux différents. Si tu prends la passphrase, tape-la dans le champ qui apparaît.

02 Tape l'adresse du destinataire

Les 42 caractères, en commençant par 0x. Vérifie les 4 premiers et les 4 derniers avec la personne : une adresse fausse, c'est de l'argent perdu, personne ne peut l'annuler.

03 Tape le montant

En ETH, avec un point pour les décimales (0.001). Les frais s'ajoutent automatiquement ; l'app refuse si le solde ne suffit pas.

04 Clique « Signer et envoyer »

Touche ta clé ou valide par Face ID, selon les facteurs choisis. Le journal affiche « signée, clé effacée de la mémoire », puis le lien Etherscan, puis « confirmée au bloc ... ».

> Ce que l'app vérifie à ta place

Qu'elle parle bien à Sepolia (elle refuse de signer sur un autre réseau), que le solde couvre montant + frais, et que l'identifiant de la transaction renvoyé par le nœud correspond au sien. Mais elle ne peut pas vérifier que l'adresse tapée est la bonne personne : ça, c'est toi.

Après chaque signature, la passphrase est effacée du champ : il faut la retaper pour l'opération suivante. C'est voulu.

[9. Récupérer ton wallet sur un autre appareil]

Le wallet ne reste **jamais** dans le navigateur une fois la page fermée : fermer l'onglet, c'est se déconnecter, et le bouton « Se déconnecter » fait la même chose tout de suite. À chaque retour, tu passes par cette récupération (une touche + un deuxième facteur). C'est voulu : rien ne traîne sur l'appareil. Aucun fichier à transférer, et ça marche aussi sur un autre téléphone ou ordinateur.

- | | |
|----|--|
| 01 | Ouvre le site et clique « Récupérer un wallet (on-chain) »
Le registre est déjà rempli. Ne touche à rien. |
| 02 | Clique « Toucher une clé de sécurité ou utiliser la passkey »
Branche ta clé et touche-la (PIN demandé), ou choisis ta passkey si cet appareil est sur le même compte Apple / Google. L'app retrouve ta sauvegarde en quelques secondes et affiche ton adresse. |
| 03 | Valide avec un deuxième facteur
Une page de vérification te demande 2 facteurs (par exemple la clé que tu viens d'utiliser et ta passphrase). Tant que ce n'est pas fait, rien n'est enregistré. Si c'est bon : « Wallet enregistré », et tu retrouves ton écran principal, solde compris. |

> Pourquoi deux facteurs pour récupérer ?

Une seule touche suffit à retrouver tes blocs chiffrés, mais pas à les ouvrir. La vérification prouve que tu possèdes bien 2 morceaux sur 3, donc que le wallet est réellement utilisable sur cet appareil.

[10. Gérer tes clés et tes appareils]

> Ajouter une clé de sécurité

Section « Facteurs », bouton « + Ajouter une clé de sécurité ». Étape 1 : touche une clé déjà enrôlée (pour relire le morceau A). Étape 2 : enrôle la nouvelle, en 2 ou 3 touches. Puis republie la sauvegarde (bouton réactivé).

> Nommer et renommer une clé

Chaque clé porte un nom, choisi à l'enrôlement. Pour en changer : « Renommer » dans la liste des facteurs, tape le nouveau nom, puis **touche la clé concernée**. L'app vérifie que c'est bien elle qui rouvre son morceau ; sans la bonne clé, le renommage est refusé. Résultat : le nom affiché correspond toujours à la clé physique, et tu ne retireras jamais la mauvaise par erreur.

> Retirer une clé

« Retirer » apparaît sur chaque clé de sécurité tant qu'il en reste une autre (1 minimum, 3 maximum). La passkey et la passphrase ne se retirent pas. Republie ensuite. Attention : retirer une clé est une mesure d'hygiène, pas une révocation. Une clé perdue ou volée peut toujours rouvrir son morceau déjà publié ; elle ne suffit jamais seule, mais si un facteur est réellement compromis, transfère les fonds vers un nouveau wallet.

> Faire le ménage dans tes clés

Chaque enrôlement occupe une place dans ta clé de sécurité (25 places sur une YubiKey 5 ancienne, 100 depuis le firmware 5.7) et crée une passkey dans ton compte Apple ou Google. L'app ne peut pas les effacer : c'est une protection du standard FIDO.

- > Clé de sécurité : Yubico Authenticator > Passkeys (ou l'outil de ta marque), tu vois la liste par site, avec le nom « Seedless A1 · 0x... », et tu supprimes.
- > Apple : Réglages > Mots de passe (iPhone, iPad) ou l'app Mots de passe (Mac), rubrique Passkeys.
- > Android : Gestionnaire de mots de passe Google > Passkeys.

> Ne supprime jamais l'enrôlement d'un wallet actif

Supprimer un enrôlement rend son morceau définitivement inutilisable. Fais le ménage seulement pour les wallets de test que tu as abandonnés, et vérifie le nom (début d'adresse) avant de supprimer.

> Vérifier les autorisations (allowances)

Sur Ethereum, un token peut porter une « autorisation » : l'ordre donné à un contrat de dépenser ce token à ta place (on dit « approve »). Ce wallet n'en crée jamais, mais un token reçu (airdrop, cadeau, test) peut en avoir une, parfois illimitée. Section « Autorisations », bouton « Scanner » : l'app liste les autorisations encore actives et propose « Révoquer » sur chacune. La révocation est une transaction signée avec 2 facteurs, comme un envoi. Fais ce scan de temps en temps, et après chaque token reçu.

Pour trouver les tokens qui ont transité par ton adresse, l'app a besoin d'une **clé API Etherscan**, gratuite et personnelle. Les nœuds publics gratuits (dRPC, publicnode) ne permettent pas de chercher dans toute la blockchain sans ça. La clé reste dans ton navigateur, elle ne donne aucun accès à ton wallet, et chaque utilisateur crée la sienne.

01 Créer un compte Etherscan

Va sur etherscan.io, « Sign In » puis « Click to sign up ». Un e-mail et un mot de passe suffisent, c'est gratuit. Confirme l'e-mail reçu.

02 Créer une clé API

Une fois connecté : menu de ton profil (en haut à droite) > « API Keys » > bouton « + Add ». Donne-lui un nom (par exemple « seedless ») et valide. Une suite de 34 caractères apparaît : c'est ta clé. Copie-la. Une seule clé sert pour tous les réseaux, Sepolia compris.

03 Colle-la dans le wallet

Section « Autorisations » > champ « Clé API Etherscan » > colle > « Enregistrer la clé ». À refaire une fois par navigateur ou appareil où tu utilises le wallet.

04 Scanne

« Scanner les autorisations ». Le journal affiche les tokens trouvés (ERC-20, NFT), puis le résultat : vert « Aucune autorisation active », ou la liste à révoquer.

> Et le nœud RPC ?

Par défaut, le wallet utilise un nœud public dRPC, sans clé, suffisant pour tester. Si tu veux ta propre clé dRPC (plus de marge), crée un compte sur drpc.org, choisis le réseau Sepolia, copie l'URL HTTP et colle-la dans « Changer de RPC ». Même logique : personnelle, stockée dans ton navigateur, aucun accès au wallet.

> Changer d'appareil Apple ou Google

Ta passkey (morceau B) suit ton compte : un nouvel iPhone connecté au même compte iCloud l'a automatiquement. Si tu changes d'écosystème (Apple vers Android), enrôle une passkey sur le nouvel appareil comme une clé supplémentaire avant de quitter l'ancien, et republie.

[11. Les bons réflexes]

- > **Garde toujours 2 facteurs accessibles.** Le wallet survit à la perte d'un seul. Deux clés de sécurité + la passkey + la passphrase, c'est confortable.
- > **Publie la sauvegarde avant de déposer quoi que ce soit**, et après chaque ajout ou retrait de clé. L'app masque d'ailleurs l'adresse et refuse d'oublier un wallet non publié.
- > **Une passphrase longue.** C'est le seul facteur qu'on pourrait tenter de deviner. 4 ou 5 mots au hasard, et ne la réutilise nulle part.
- > **Un seul site, une seule adresse web.** Tes clés sont liées au nom du site. Si l'adresse du site change, elles ne répondent plus. Mets-le en favori.
- > **Un navigateur propre.** Sans extension inconnue. Sur iPhone et iPad, Safari est parfait.
- > **Vérifie l'adresse de destination** avec la personne, pas depuis un message qui pourrait être trafiqué.
- > **Sepolia, c'est pour apprendre.** Fais au moins une fois chaque scénario : envoyer, récupérer sur un autre appareil, ajouter une clé, en retirer une. Quand tout te semble évident, tu es prêt pour plus tard.

[12. Problèmes fréquents]

MOT	CE QUE ÇA VEUT DIRE, SIMPLEMENT
« Cérémonie annulée ou refusée » (NotAllowedError)	Tu as fermé une fenêtre trop tôt, ou le délai est passé, ou la clé n'a pas de PIN FIDO2. Reclique sur le bouton : ça reprend à la même touche. Si ça persiste, vérifie le PIN avec Yubico Authenticator.
La clé ne clignote pas	Branche-la seulement quand le navigateur te le demande, pas avant. Sur iPad, utilise le port USB-C directement, sans hub. Vérifie aussi que la clé a un PIN.
« Ne supporte pas l'extension PRF »	La clé est trop ancienne (YubiKey 4, NEO, ou firmware inférieur à 5.2.3) ou le navigateur ne gère pas la PRF (Firefox). Change de clé ou de navigateur.
« 0 publication trouvée » à la récupération	Soit la sauvegarde n'a jamais été publiée (vérifie sur le wallet d'origine), soit tu as choisi, dans la liste proposée par le navigateur, un enrôlement d'un autre wallet. Regarde le nom (début d'adresse).
Le solde reste à « ? »	Le nœud RPC ne répond pas. Attends, ou change de RPC dans « Sauvegarde et maintenance ».
J'ai oublié ma passphrase	Pas grave tant que tu as ta clé de sécurité et ta passkey : signe avec A + B. Et profite-en pour ajouter une seconde clé de sécurité.
J'ai perdu ma clé de sécurité	Signe avec B + C (passkey + passphrase). Puis ajoute une nouvelle clé (il faut une clé déjà enrôlée pour ça : d'où l'intérêt d'en avoir toujours deux). Si c'était ta seule clé, le wallet reste utilisable avec B + C, mais tu ne pourras plus ajouter de clé : crée un nouveau wallet et transfère.
J'ai perdu 2 facteurs	Le wallet est perdu, définitivement. Personne ne peut le récupérer, pas même l'auteur de l'app. C'est le prix de « personne d'autre que toi ».
Le renommage d'une clé est refusé	Tu as touché une autre clé que celle que tu renomes, ou fermé la fenêtre. C'est la protection voulue : seule la clé concernée peut changer son nom. Recommence avec la bonne clé.
Le site a changé d'adresse	Les enrôlements ne répondront plus sur la nouvelle adresse. Crée un wallet sur la nouvelle adresse et transfère tes fonds depuis l'ancienne (qui reste accessible à l'ancienne adresse).

[13. Pour les curieux : ce qui se passe sous le capot]

Tout tourne dans ton navigateur, sans serveur. Le nombre secret est tiré par le générateur aléatoire de ton appareil, découpé par la méthode de Shamir (2 sur 3), et chaque morceau est chiffré en AES-256 avec une clé dérivée de ta clé de sécurité (PRF), de ta passkey (PRF) ou de ta passphrase (PBKDF2, 600 000 itérations). Les morceaux chiffrés sont déposés dans un contrat de 25 octets sur Sepolia, indexés par un hash de la PRF de chaque clé. Le code est lisible de bout en bout, sans dépendance externe, sans télémétrie.

Un wallet de conservation, c'est volontairement ennuyeux. C'est le but.