Portefeuille multi-signature (Safe Wallet)

Introduction : Qu’est ce qu’un multi-sig ?

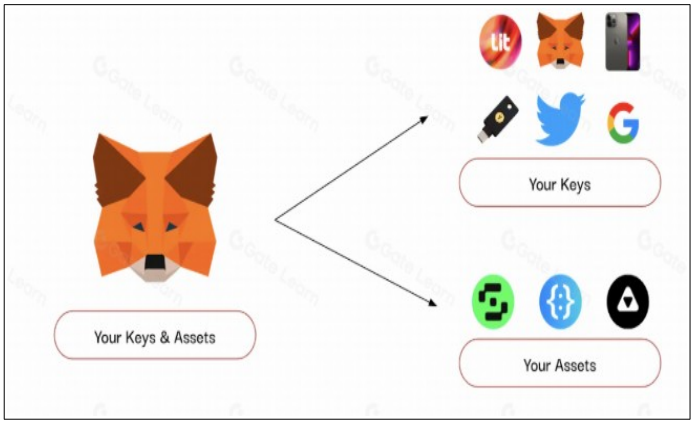
Un portefeuille « classique» (MetaMask, Rabby,.Ledger,..) regroupe deux fonctions :

- le stockage de vos actifs (Stablecoin, RealToken, REG, ..),
- la signature (avec la clé privée associée) de vos transactions (usage de vos actifs).

Avec un wallet multi-sig (ou un Abstract Account) sur des blockchains Ethereum (EVM) compatibles (comme Gnosis), ces deux fonctions sont dissociés :

- le stockage des actifs est dans un smart contract,
- l’usage des actifs dans ce smart contract est autorisé au travers de un ou plusieurs wallets signataires (d’ou la qualification de de multi-signature).

Un tel wallet apporte plus de sécurité, ainsi que des fonctions programmables grace au smart contract.



La sécurité d’un wallet dépend de la gestion de sa clé privée :

- Pour le Hot wallet (MetMask, Rabby,..) la clé privée est stockée dans un logiciel (soit une extension de votre navigateur pour un PC, soit dans une application sur votre smartphone). La sécurité est alors limitée.

- Pour le Cold Wallet (Ledger, Tangem,...), la clé privée est stockée dans un matériel spécifique et n'en sort jamais, d'où une sécurité plus elevé.
- Pour le wallet mult-sig, la sécurité est accrue par le fait qu'il est necessaire d'avoir plusieurs signataires pour valider une transaction. Par exemple 2 sur 3.
  Par ailleurs, si un des wallets d'autorisation est perdu ou hacké, il est possible de le remplacer.
  A la différence d'un wallet « classique » (Hot ou cold wallet) : ou la perte de la clé, induit la perte des actifs associés.

Le wallet multi-sig est très utilisé par les entreprises, les organisations décentralisées (DAO) et les particuliers qui souhaitent protéger leurs fonds contre les risques de défaillance d'un point unique.

Sur les blockchain EVM compatible, il existe de nombreux le wallet multi-sig et le plus populaire est le Safe Wallet (anciennement Gnosis Safe). C'est ce dernier que nous détaillerons dans la suite de ce document.

Création d'un Safe wallet

1. Aller sur le site Safe Wallet : https://app.safe.global/welcome
   (Nota : l'application est aussi disponible sur smartphone)
2. En haut à droite, connectez vous à l'application avec le premier wallet qui sera signataire du Safe,
3. Passer à la première étape de création du Safe « Set up the basics » et renseigner :
   - Le nom que vous souhaitez donner à votre Safe Wallet,
   - Les blockchains, sur lesquels vous souhaitez que votre Safe Wallet soit disponible.
     A la différence d'un wallet « classique » (qui intègre sa clé privé) et qui est utilisable sur de multiples blockchain (compatible EVM), un multi-sig n'est utilisable que sur les blockchains sur lesquelles le smart contrat a été déployé.
     Par defaut la blockchain proposée est celle du wallet avec lequel vous vous êtes connecté à l'application.
     Vous pouvez (/ pourrez) ajouter d'autres Blockchains : votre safe wallet aura la même adresse sur tous ces réseaux.
     Attention à n'utiliser votre adresse Safe que sur les blockchains que vous avez activés ! (sinon, les actifs qui y seraient transférés seraient perdues..). Un chapitre spécifique détail ce point.
4. Dans l'étape suivante, vous devez définir l'ensemble des wallets signataires (qui ont le pouvoir de soumettre et approuver les transactions).
   Le premier est celui avec lequel vous vous êtes connecté et créé le Safe.

Ajoutez les suivants, en leur donnant un nom et leur adresse publique (il pourra s'agir d'un wallet Ledger ou mobile).
Vous pourrez ultérieument modifier la liste des signataires.
Indiquez en suite le seuil (Threshold) : cela correspond au nombre de signature pour valider une transaction.
Assurez vous d'avoir le coin de la blockchain, pour les frais de création du Safe.

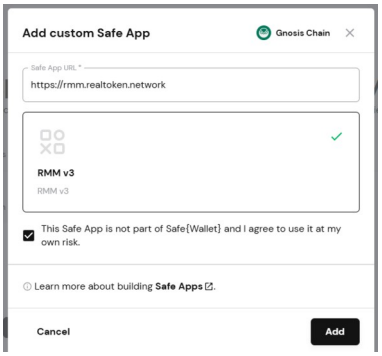
La création prendra entre 20 et 40 secondes et les frais sont offerts pour la blockchain Gnosis.

Utilisation du Safe Wallet

Une fois créé, lorsque vous retournez sur l'application (https://app.safe.global/) et que vous vous connectez avec l'un des wallet signataire, vous voyez apparaître votre compte Safe.

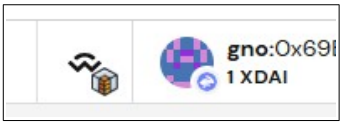
En le selectionnant, apparaissent toutes les fonctions disponibles (menu à gauche) :

- Home : Synthèse de vos actifs, transactions en cours, avec les principales fonctions (envoyer, recevoir, swapper) et Application. L'ensemble étant détaillé dans la suite du menu.
- Asset : Actif présents sur votre Safe (avec possibilité de les envoyer et swapper),
- Transactions : Toutes les transactions de votre Safe (en cours et historique)
- Address Book : addresse que vous avez enregistrées
- Apps : Applications par defaut (> 100) ou personnelles.
  Les applications RealToken (RMM, YAM, Voting,..) ne permettent pas une connection direct avec un Safe wallet.
  Vous devez passer par ce menu :
  - La première fois : Ajouter l'application : selectionner « My custome apps », indiquer l'url de l'application et ajouter.
  - cliquer sur l'icone de l'app, pour y accéder avec votre Safe wallet.



Nota : il est aussi possible de connecter votre Safe à une application, avec la fonction WalletConnect :

- Sur l'application : faire une connection avec WalletConnect, copier (ou scanner) le code,
- Connectez vous à votre Safe, puis (dans le menu du haut) cliquez sur WalletConnect, et coller le code
- Vous êtes connecté à l'application avec votre safe.



Nota bis : Il est aussi possible de connecter votre safe à une application en utilisant Rabby :

- A partir de la liste des adresses (en haut), cliquer sur « Add New Adress », puis selectionner « Connecter des wallet institutionnels », puis chosir Safe, indiquer l'adresse de votre safe, indiquer un nom pour votre Safe. Avec votre wallet Rabby, sur l'adresse de votre Safe, vous pouvez vous connecter directement aux applications.

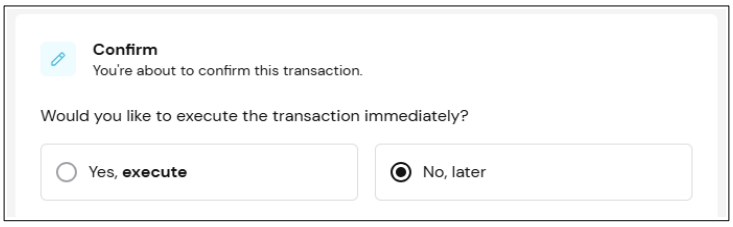
- Settings : Gérer votre Safe (ajout / retrait de signataires, modification du seuil de signature, limites de dépenses, Apparence, Sécurité, Notification,..)
-

Cycle d'une transaction

Une transaction sur le Safe, suit le cycle suivant :

- Création : par un des wallet signataires (ou « Proposer »)
- Confirmations : Signature par les wallet signataires du Safe.
  - La première est celle du wallet signataire qui crée la transaction (sauf dans le cas du Proposer, qui ne fait que créer sans pouvoir signer).
  - Les suivantes, sont faites par les autres wallets signataires jusqu'à atteindre le seuil (nombre) de signature necessaire pour que la transaction Safe soit executée,

- Execution : Elle peut etre lancée par le dernier signataire (qui a permis d'atteindre le seuil du Safe), ou par un autre signataire. Les frais d'execution de la transaction sont à la charge de celui qui lance l'execution.



Gnosis a actuellement un programme de sponsoring, qui prend en charge 5 transactions gratuites par heures.

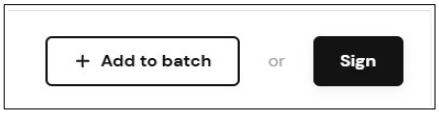
Nota : Une transaction peut aussi être rejeté par un signataire. Le rejet est alors une nouvelle transaction Safe, soumis à la signature des autres signataires.

Dans l'historique des transactions vous pouvez voir les différentes étapes du cycle et les signataires correspondants.

Regroupement de transactions

Avec Safe Wallet, vous pouvez grouper plusieurs transactions, pour toutes les valider simultanément. Cela coutera au final, une seule transaction de frais.

A la fin de chacune des transactions, il vous suffit de l'ajouter au batch (plutôt que de la signer).



Puis de lancer le batch (en haut de la page), avec une seule signature (par signataire).

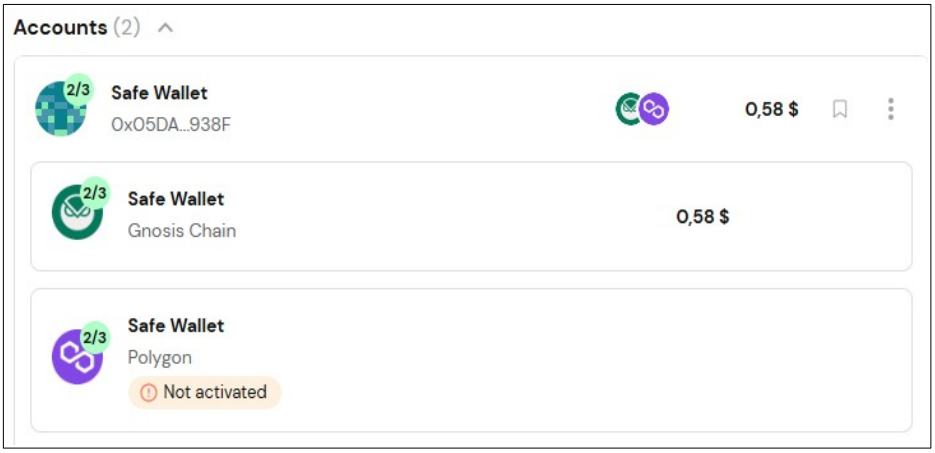
Nota : Vous pourriez créer un Safe wallet avec un seul walet signataire, juste pour bénéficier de cette fonction (indisponible avec un wallet classique).

Activation d'un Safe Wallet sur plusieurs blockchains

Comme évoqué précédement, un Safe wallet ne fonctionne que sur les blockchains sur lesquelles il a été activés.
Les applications de bridge considère généralement que vous avez la même adresse pour passer d'une blockchain à une autre. Dans le cas du Safe, si vous n'avez pas activé le Safe sur la blockchain cibre du bridge, vos fonds risque d'être perdus !

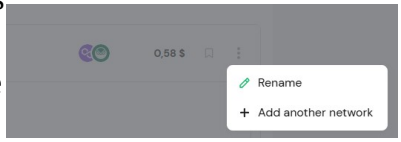
Sur un Safe wallet les blockchains sont d'abord déclarée puis activée.
La déclaration peut se faire soit au moent de la création du Safe Wallet (cf chapitre ci-avant), soit après.

L'activation du Safe sur une blockchain (un réseau) donné, necessite d'avoir des coins de la blockchain correspondante pour payer les frais d'activation (création du smart contrat sur la blockchain). Raison pour laquelle vous pourriez, lors de la création, ne pas activer toutes les blockchains.
Cela apparaitra dans l'application Safe, de la façon suivante : Après etre connecté à l'application Safe avec un wallet signataire, dans la liste de vos comptes Safe vous verrez alors les Blockchains activés et non acivés (cf image ci-après)



Ajout d’une blockchain

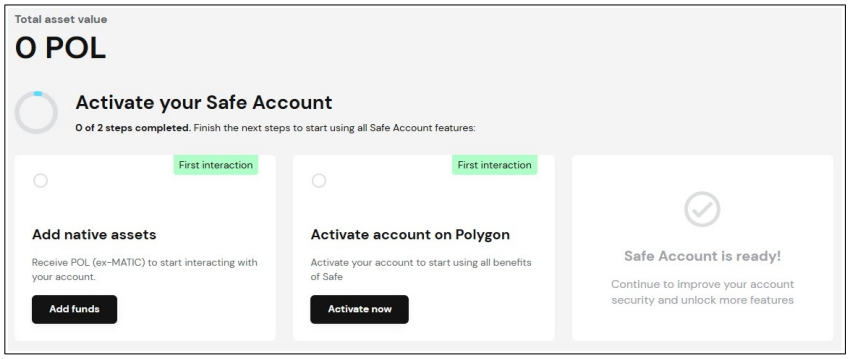
Si la blockchain souhaitée n’apparait pas dans cette liste (initialisée lors de la création du Safe), il est possible d’en ajouter une nouvelle en allant simplement dans les trois petits points au bout de la ligne du Safe et en faisant « Add another network ».

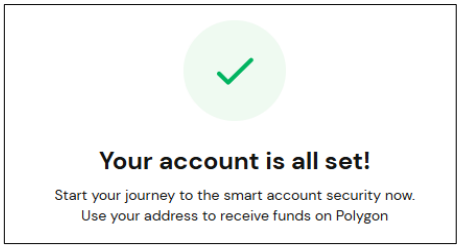


Activation d’une blockchain

L’activation se fait en deux étapes : L’ajout du coin correspondant sur le wallet signataire, puis l’activation du Safe sur la blockchain.

Par exemple dans le cas de ‘limage ci-avant, pour activer le Safe sur le réseau Polygon :





Le Safe Wallet sur mobile

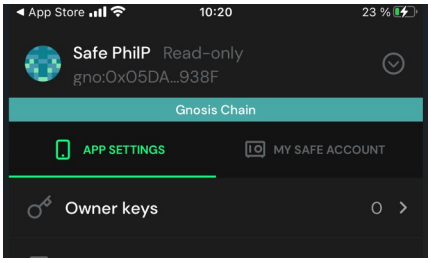
Dont un des intérêts majeur est la « Push notification », hélas disponible que sur IOS !.

Pour installer l’App :

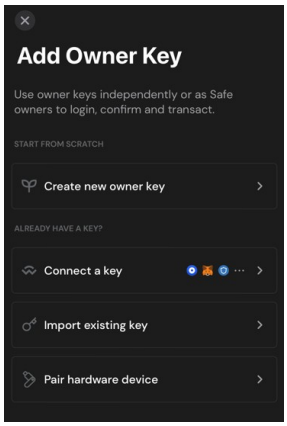
- Sur Android : https://play.google.com/store/apps/details?id=io.gnosis.safe
- Sur IOS : https://apps.apple.com/mu/app/safe-wallet/id1515759131

Vous pouvez : créer ou charger un Safe existant sur IOS, et seulement le charger sur Android.

Une fois le Safe chargé, vous êtes en mode « Read-Only » (indication en haut, après le nom de votre Safe).
Dans ce mode vous pouvez uniquement voir :



- Les actifs sur le Safe (menu inférieur « Asset »),
- Les transactions en cours et passées (menu inférieur « Transactions »),
- Les clés signataires du Safe (menu inférieur « Settings » et onglet « My safe account ») et le seuil de signature.

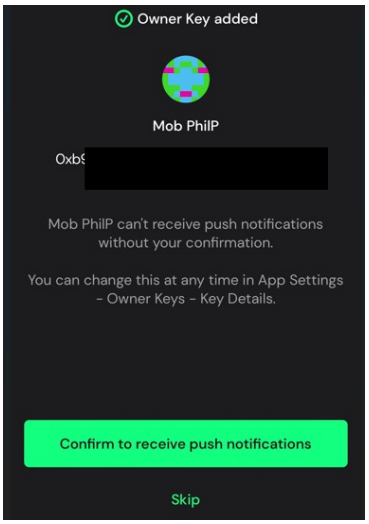


Pour pouvoir executer des transactions sur le Safe, vous devez ajouter ou connecter une clé signataire (alias « Owner ») : Settings > App Settings > Owner keys >…

Une fois la clé signataire ajoutée, la qualification « Read-Only » disparaitra.

Il est aussi possible de créer un nouveau compte « signataire » sur votre mobile. L'opération se fait en deux temps :

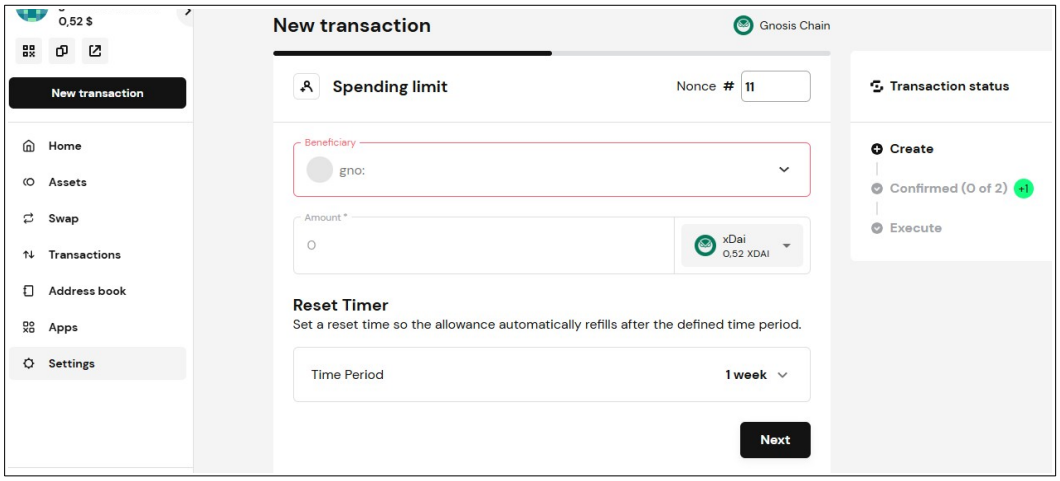
- création d'un nouveau wallet, par l'application sur le smartphone (dont la clé privée sera stockée sur le smartphone:une fonction permet de sauvegarder la seed phrase correspondante).
- ajout par un des comptes signataires existants, de la nouvelle adresse générée par le smartphone, afin de devenir signataire du Safe. Transaction qui devra être validée, suivant le seui du Safe.



Sur IOS, lors de l'ajout d'une clé signataire vous pouvez confirmer votre souhaite de recevoir des notifications lorsqu'il y a des actions sur le Safe.

Autorisation de dépenses limitées

Il est possible d'autoriser n'importe quel portefeuille à dépenser un montant limité d'un actif depuis le Safe, pendant une période spécifique. Cette fonction n'est disponible que sur l'application web : Settings > onglet Setup > Spending limits



Cette autorisation est soumise au seuil d'approbation avec les signataires du Safe.

Le wallet autorisé à dépenser sur le Safe, n'a pas besoin d'être signataire du Safe et n'aura pas besoins d'approbation des signataires (il contournera le dispositif de seuil). Il doit juste se connecter au Safe pour executer le transfert.

Les signataires du Safe, peuvent consulter l'usage la limite de dépense accordée et la modifier.

Dec. 2024 - PhilP