MoulinEth

FAQ

Comment participer à un round ?

- Vérifiez qu'un round est actif. Dans le cas contraire, cliquez sur **Init Round**.
- Utilisez votre adresse Ethereum de dépôt pour déposer les Ethers que vous souhaitez mixer: indiquez le montant en wei que vous souhaitez mixer, puis cliquez sur **Deposit**.
- Notez bien l'ID du round auquel vous avez participé, et prenez connaissance de la date et de l'heure à laquelle se termine le round.
- Avant la fin du round, utiliser votre adresse Ethereum de retrait pour faire une demande de retrait en versant une caution égale (ou inférieure) au montant déposé à l'étape précédente: indiquez le montant en wei de votre caution, puis cliquez sur **Request**.
- Pour augmenter l'efficacité du mixage, vous pouvez faire plusieurs dépôts dans le même round (avec différentes adresses de dépôts) et / ou plusieurs demandes de retraits (avec différentes adresses de retraits) toujours dans le même round.

  Par exemple (une même personne contrôle les 5 adresses ci dessous):

  - Adresse de dépôt 1 dépose 0,4 Ether
  - Adresse de dépôt 2 dépose 0,2 Ether
  - Adresse de retrait 1 réclame 0,25 Ether en versant une caution de 0,25 Ether
  - Adresse de retrait 2 réclame 0,3 Ether en versant une caution de 0,3 Ether
  - Adresse de retrait 3 réclame 0,05 Ether en versant une caution de 0,05 Ether
- ⚠️ Vous ne pouvez pas utiliser une même adresse pour un dépôt et une demande de retrait dans le même round.
- ⚠️ La somme des cautions de retraits doit être égale (ou inférieure) à la somme des dépôts, sinon le round risque d'être renversé.
- Vous pouvez faire votre ou vos demandes de retraits avant de faire votre ou vos dépôts à condition de faire les dépôts et les demandes de retraits dans le même round et avant la fin du round.
- À la fin du round et après sa vérification, si le total des cautions de retraits est égal au total des dépôts vous pourrez récupérer votre dépôt et votre caution de retrait en utilisant votre (ou vos) **adresse de retrait**. Recherchez le round auquel vous avez participé dans la liste des rounds fermés, et cliquez sur **Withdraw**.
- À la fin du round et après sa vérification, si le total des cautions de retraits est inférieur au total des dépôts, le montant non réclamé sera partagé (bonus) entre les participants; vous pourrez récupérer votre dépôt, votre caution de retrait et votre bonus en utilisant votre (ou vos) **adresse de retrait**. Recherchez le round auquel vous avez participé dans la liste des rounds fermés, et cliquez sur **Withdraw**.
- À la fin du round et après sa vérification si le total des cautions de retraits est supérieur au total des dépôts, le round est renversé , un ou plusieurs participants ont essayé de récupérer des Ethers qu'ils n'avaient pas déposés, ils perdent leurs cautions qui seront partagées (bonus) entre les autres participants. Vous pourrez récupérer votre dépôt , votre caution de retrait et votre bonus en utilisant votre (ou vos) **adresse de dépôts**. Recherchez le round auquel vous avez participé dans la liste des rounds fermés, et cliquez sur **Backdraw**. Vos Ethers n'ont pas été mixés, mais le bonus vous dédommage en partie !

Comment mon adresse de retrait peut-elle être "anonyme", si je dois déjà posséder des Ethers dessus afin de verser la caution ?

- Créez une nouvelle adresse Ethereum.
- Utilisez un faucet ou achetez une petite quantité de wei de manière anonyme.
- Faites des rounds avec des montants de plus en plus importants pour disposer de suffisamment d'Ethers "anonymes"... ce qui vous permettra de mixer de plus en plus d'Ethers.
- Faites attention à ce que votre adresse de retrait n'ait aucun lien (transaction directe ou indirecte) avec votre adresse de dépôt.

Quel est l'intérêt de faire une demande de retrait avec une caution inférieure au dépôt ?

Vous pouvez faire une demande de retrait avec une caution légèrement inférieure (ou davantage si vous êtes généreux !) à votre dépôt. Cela augment l'efficacité du mixage et la probabilité que le round soit validé.

Si le round est validé:

- La différence entre votre dépôt et votre caution constitue un bonus qui sera partagé entre tous les participants (y compris vous)
- Vous récupérerez à l'issue du round votre caution multiplié par 2, plus le bonus.
- Vous perdez donc un peu d'Ethers , sauf si de nombreux utilisateurs font de même en versant eux aussi une caution inférieure à leur dépôt.

Si le round est malgré tout renversé:

- Vous récupérerez à l'issue du round votre dépôt multiplié par 2, plus le bonus.
- Vous gagnez donc un peu d'Ethers.

Pourquoi et comment vérifier un round ?

Lors de la vérification du round, le smart contract Ethereum compare le total des dépôts au total des cautions de retraits afin de décider si le round est validé (somme des dépôts >= somme des cautions) ou renversé (somme des dépôts < somme des cautions).

Si les deux montants ne sont pas égaux, le smart contract calcule le bonus qui sera partagé entre les participants.

Pour vérifier un round inactif (si il n'a pas déjà été vérifié), cliquez sur **Check Round**.

Peut-on faire une demande de retrait (en versant une caution) sans avoir fait de dépôt ?

Oui ! Mais vous perdrez votre caution de retrait , sauf si:

- Vous parvenez à faire votre dépôt avant la fin du round.
- Un ou plusieurs participants oublient de faire leurs demandes de retraits (ou font des demandes de retraits avec des cautions inférieures à leurs dépôts) et que le montant des dépôts non réclamés est supérieur ou égal au montant de votre caution, auquel cas vous gagnerez le double de votre caution de retrait.

Je ne parviens pas à faire ma demande de retrait !

Vérifiez que:

- Le round est encore actif.
- L'adresse utilisée pour votre demande de retrait est différente de celle utilisée pour votre dépôt.
- L'adresse utilisée pour votre demande de retrait n'a pas déjà été utilisée dans le même round pour faire une autre demande de retrait.

Je ne parviens pas à retirer mes Ethers !

Vérifiez que:

- Le round est terminé et vérifié.
- L'ID du round correspond bien au round auquel vous avez participé.
- Vous utilisez la bonne adresse: adresse de retrait en cas de Withdraw (round validé), adresse de dépôt en cas de Backdraw (round renversé).

Je n'ai pas fait de demande de retrait dans la limite de temps du round !

C'est vraiment dommage pour vous, mais votre dépôt est définitivement perdu, sauf si le round est renversé, auquel cas vous gagnerez le double de votre dépôt.

A quoi servent les bonus et le bouton «Send Fee» ?

Les bonus correspondent aux dépôts non réclamés (dans le cas d'un round validé) ou aux cautions de retraits excédentaires (dans le cas d'un round renversé) ; ils sont partagés entre les participants du round lors du Withdraw ou du Backdraw. Leurs montants (total des montants avant partage) ne sont connus qu'après la vérification du round.

Les bonus fee que n'importe qui peut verser en cliquant sur **Send Fee** sont des incitations à participer au round. Ces bonus fee seront partagés entre les participants du round lors du Withdraw ou du Backdraw. En incitant à participer au round , il y'aura davantage de participants ce qui augmentera l'efficacité mixage. Les bonus fee (total des bonus fee avant partage) sont connus et affichés au cours du round actif au fur et à mesure de leurs versements.

J'ai reçu davantage d'Ethers que ce que j'ai versé ! Est-ce normal ?

Oui, cela peut arriver. Ce sont des bonus qui correspondent soit à des dépôts non retirés, soit à des cautions de retraits versées sans avoir fait de dépôts , soit à des incitations à participer au round (bonus fee).

Comment accéder à cette dapp ?

Via un navigateur web compatible web3 (Metamask):

- dapp (version de test sur ropsten): https://ipfs.io/ipns/QmQLV56ihsFxyyvp1HyXbamCNcwUDiBnPnbhuvUb83EF7H/
- dapp (mainnet): *Cette dapp n'est pas encore déployée sur le mainnet.*

Via un noeud ipfs:

- ipns hash (version de test sur ropsten): QmQLV56ihsFxyyvp1HyXbamCNcwUDiBnPnbhuvUb83EF7H
- ipns hash (mainnet): *Cette dapp n'est pas encore déployée sur le mainnet.*

Adresse du smart contract Ethereum (Version de test sur Ropsten):

- 0xE2F2EF747d41204b3492AB342A48307857C07e77

Adresse du smart contract Ethereum (Mainnet):

- *Ce smart contract n'est pas encore déployé sur le mainnet.*

100% Free ! Ca signifie quoi ?

Le smart contract Ethereum, et la dapp sont sous licence AGPL V3, il s'agit d'une licence libre ("open source"), dont vous pouvez consulter les termes : https://www.gnu.org/licenses/agpl-3.0.html

Les sources du smart contract et de la dapp sont disponibles sur github: https://github.com/YannBouyeron/MoulinEth.git

100% Décentralisé ! Ca signifie quoi ?

- Ce mixer fonctionne grâce à un smart contract hébergé sur la Blockchain Ethereum.
- Ce smart contract ne contient aucune fonction permettant de l'arrêter !
- L'application web est hébergée sur IPFS. L'IPFS ou InterPlanetary File System est un protocole pair à pair (p2p) de distribution de contenu adressable par hypermédia. Il permet de "stocker" des fichiers ou des arborescences de fichiers de manière décentralisée et permanente, et d'y accéder via un noeud ipfs ou via un navigateur web.
- **Cette dapp est donc totalement "unstoppable" !**