Description

Titre de l'invention : Méthode de gestion de cagnottes solidaires multi-crypto-actifs créant une plateforme d'échange sans oracle ainsi que des stablecoins sur la blockchain Ethereum

[0001] Cet algorithme consiste en une plateforme d'échange entièrement décentralisée impliquant la gestion de cagnottes de crypto actifs sur Ethereum (ethers et tokens), l'invention a pour objectif d'encourager un mode de consommation social et mutualisé grâce à un réseau doté d'un système innovant de cagnottes et de statistiques. Le dispositif est constitué d'un « Smart Contract » proposant la création de groupes d'adresses pouvant ouvrir et fermer des cagnottes d'ethers et de tokens ERC20 ainsi que la possibilité d'y échanger des actifs directement sans utiliser d'oracle.

[0002] Pour comprendre la finalité de technologie blockchain il est nécessaire d'admettre qu'autant la robotisation a pour objectif de faciliter les taches manuelles et l'intelligence artificielle de faciliter les taches décisionnelles, la blockchain aura pour objectif de faciliter la création de services en les automatisant ainsi qu'en supprimant les intermédiaires de confiance et les infrastructures obsolètes. Les blockchains de première génération comme celle du Bitcoin sont une démonstration d'un système distribué et décentralisé d'échange sécurisé de valeurs de pair à pair.

[0003] Ethereum est une blockchain de seconde génération sa cryptomonnaie de fonctionnement est l'*ether*. Sur cette blockchain il est possible de déployer des programmes appelés *smart contracts* permettant de créer diverses formes de transaction et par exemple ici de créer des cagnottes ou des actifs exotiques appelés *tokens*. Un des principaux standards de token est le standard ERC20 qui est le standard qui nous intéresse par son caractère fongible et son interopérabilité. Grâce à l'essor de l'écosystème nous avons à disposition déjà aujourd'hui de nombreux ERC20 sur la blockchain Ethereum, Ethers et/ou ERC20 peuvent facilement s'échanger sur des plateformes d'échange cependant leurs cours respectifs varient beaucoup par conséquent il est nécessaire de solliciter ce que l'on appelle des *oracles*.

[0004] Les oracles ne sont pas contrôlés par le réseau comme le sont les « smart contrats » ce sont des programmes externes constituant une faille de sécurité en plus de complexifier les transactions les rendant plus longues et chères. En effet ils impliquent le recours à une tierce partie dont le rôle est de rechercher l'information demandée. Plusieurs inconvénients sont à prévoir par exemple si l'oracle n'envoie aucune information dans la blockchain dans ce cas le contrat ne pourra pas s'exécuter ou il envoie par erreur ou de façon volontaire une information inexacte.

[0005] C'est pourquoi dans un souci d'indépendance et de fiabilité notre méthode exclue

l'utilisation d'oracle mais comme nous l'avons vu précédemment le réseau ethereum propose une multitude de crypto-actifs et une accumulation de différents ERC20 dans une cagnotte peut devenir encombrant pour l'utilisateur lors de la fermeture car ce dernier voudra surement en échanger ultérieurement. Pour ne pas nécessiter l'utilisation d'oracle tout en proposant des échanges pratiques et acceptables nous allons en premier temps restreindre les ERC20 acceptés dans les cagnottes à un type bien précis que l'on appelle les *stablecoins*. Un stablecoin est un type de cryptomonnaie dont la valeur est stable car basée sur celle d'un actif sous-jacent. La plupart sont adossés à une monnaie fiduciaire, à des matières premières ou commodités, d'autres sont adossées à d'autres cryptomonnaies. Les stablecoins ont pour objectif de résoudre divers problèmes comme la volatilité, les frais de conversions ou la taxation. On remarque sur ethereum différents stablecoins adossés à la même valeur notamment sur le dollar US.

[0006] Notre objectif est de concevoir dans un réseau social des cagnottes pouvant regrouper une multitude d'actifs différents, le problème pour l'utilisateur est de devoir changer des actifs reçus dans une cagnotte en actif de son choix ce qui est peu pratique et absolument pas avantageux étant donné que l'utilisateur doit payer des frais de transactions aux mineurs du réseau lors de la fermeture d'une cagnotte pour chaque type d'actif ainsi que pour chaque conversion. Le procédé exposé par cette invention garanti la sécurité, la réduction des coûts et actions par une méthode de sélection et de regroupement de tokens ERC20 par catégorie de stablecoin ainsi que de création de stablecoins adossés à ces catégories que nous appelons ERC20 propriétaires. Pour illustrer cette idée nous avons créé un « Smart Contract » organisant nos cagnottes dans un réseau social que nous pouvons résumer comme il suit :

[0007]
- Chaque utilisateur peut ouvrir une cagnotte dans un groupe dont il est membre.
- Tous les membres d'un groupe peuvent alimenter une cagnotte.
- Le créateur d'un groupe en devient administrateur et peut ajouter ou supprimer un membre ou transmettre son pouvoir administratif.
- Chaque membre (adresse) possède un pseudonyme unique dans le réseau.
- Les stablecoins ERC20s sont regroupés par catégorie d'indice de valeur (par exemple une valeur comme le dollar ou l'euro).
- Les cagnottes peuvent être alimentés uniquement par de l'ethers ou des tokens ERC20 de type stablecoin.
- Lors de la fermeture de la cagnotte l'utilisateur peux récupérer uniquement des ethers ou des ERC20s propriétaires.
- Pour chaque unité de stablecoin ERC20 entrant dans une cagnotte il sera distribué (miné) une unité de token ERC20 propriétaire correspondant à la

sortie.

- Les ERC20s propriétaires et stablecoins catégorisés peuvent être échangés directement en un pour un contre n'importe quel ERC20 de même catégorie
- Les ethers représentent une catégorie exceptionnelle sans ERC20 propriétaire correspondant dont il est l'unique membre, ils sont distribués intégralement à la fermeture de la cagnotte et ne peuvent pas être échangés.

[0008] Montrons un cas d'utilisation prenant pour exemple une application exploitant ce « Smart Contract », Considérons deux types de ERC20s propriétaires :

[0009]
- Le « Togethers-USD » pour le groupe de stablecoins stabilisés sur le dollar US, dans lequel sont accéptés le Dai, le Tether et le Gemini, ces derniers sont par conséquent considérés équivalents.
- Le « Togethers-EUR » pour le groupe de stablecoins stabilisés sur l'euro, dans lequel est accepté le Stasis uniquement.

[0010] « Groupe A » est un groupe d'utilisateurs de cette application qui a pour membres Alice, Paul, Bob et Denis.

[0011]
1. Denis a besoin de fonds et décide d'ouvrir sa cagnotte dans Groupe A, elle est initialement vide, ni ethers, ni Togethers-USD ni Togethers-EUR.
2. Alice veut injecter dans la cagnotte de Denis des stablecoins qu'elle possède et acceptés par le « Smart Contract ».
3. Alice décide de mettre 1 Dai dans cette cagnotte.
4. Puis Paul décide d'y mettre 0,1 ether.
5. Ensuite Bob y met 1 Gemini (GUSD).
6. Enfin Alice ajoute encore 1 Tether (USDT).
7. Denis décide de fermer sa cagnotte pour récupérer son contenu, il récupère donc 0,1 ether et 3 Togethers-USD. Les Dai, Gemini et tethers restent dans le « Smart Contract ».
8. Suivant l'utilisation globale de la plateforme une certaine quantité de stablecoins catégorisés et ERC20s propriétaires sont disponibles dans le « Smart Contract », par conséquent Denis peut échanger ses tokens ERC20 avec ceux du « Smart Contract ».
9. Ne désirant que du Dai Denis échange ses 3 Togethers-USD contre 3 Dai.

[0012] Résultats : Ici Denis a pu consommer sa cagnotte et récupérer les crypto-actifs de son choix en seulement 4 transactions :

[0013]
- Lors de la fermeture 1 transaction a été faite pour l'acquisition des ethers et 1 autre pour l'acquisition des Togethers-USD (TGTU).
- Lors de l'échange 2 transactions ont été faites pour le remplacement des Togethers-USD (TGTU) en Dai (1 pour ERC20 entrant et 1 pour ERC20 sortant) sur notre plateforme d'échange.

[0014] Sans ce système Denis aurait effectué 8 transactions :

[0015]
- Lors de la fermeture 1 transaction aurait été faite pour l'acquisition des ethers et 1 autre pour l'acquisition de chaque stablecoins soit 4 au total.
- Lors de l'échange 2 transactions auraient été faites pour le remplacement de chaque stablecoin (USDT et GUSD) en Dai soit 4 au total avec utilisation d'oracle. Nous rappelons qu'ici l'échange s'est fait sur une autre application ou place de marché étant donné que la plateforme d'échange est devenue inexistante dans le « Smart Contract » car plus aucun actif n'y est stocké de manière équivalente.

[0016] Avantages obtenus par Denis : 4 transactions en moins, toutes les opérations effectuées sur la même plateforme, pas d'utilisation d'oracle.

[0017] Les choix de stablecoins de même catégorie lors de l'échange tenant compte de leur nature et de leur valeur précise sont à l'appréciation de l'utilisateur. Aussi les ERC20 propriétaires pourrons éventuellement être échangés sur d'autres plateformes d'échange et étant adossés à des stablecoins équivalents via les cagnottes ils sont par conséquent eux aussi des stablecoins, quand ces derniers sont échangés sur la plateforme interne ils sont aussi stockés et échangeables selon leur catégorie dans le « Smart Contract » pour préserver leur existance et leur valeur. Un utilisateur peut de plus utiliser cette plateforme pour échanger directement des stablecoins de même catégorie sans impliquer de ERC20 propriétaire (ex : Dai <-> Tether).

Revendications

[Revendication 1] 1 : Méthode de gestion de cagnottes telle que le « Smart Contract » fait office de plateforme d'échange direct en quantités égales (en tenant compte des décimales) pour tout ERC20 de même catégorie (stablecoins et propriétaires) entre l'utilisateur d'une part et le « Smart Contract » d'autre part ce dernier étant alimenté en premier lieu suivant les flux entrant dans les cagnottes, les conversions sont opérées sans utilisation d'oracle.

[Revendication 2] 2 : Méthode de gestion de cagnottes selon la revendication 1, caractérisée en ce que chaque unité de stablecoin entrée dans une cagnotte sera stockée dans le « Smart Contract » et il sera miné pour l'utilisateur une quantité équivalente de ERC20 propriétaire échangeable correspondant lors de la fermeture de sa cagnotte.

[Revendication 3] 3 : Méthode de gestion de cagnottes selon la revendication 2, caractérisée en ce que la cagnotte d'un utilisateur peut être soldée uniquement en ether et/ou ERC20 propriétaire(s).

[Revendication 4] 4 : Méthode de gestion de cagnottes selon la revendication 2, caractérisée en ce qu'une cagnotte ouverte peut être alimentée par d'autres utilisateurs uniquement en ether ou en stablecoin ERC20 catégorisé, jamais en ERC20 propriétaire.

[Revendication 5] 5 : Méthode de gestion de cagnottes selon les revendications 2, 3 et 4, caractérisée en ce qu'un ERC20 propriétaire corresponds à une catégorie de valeur de stablecoin ERC20 existant(s) échangeable(s) sur une plateforme d'échange externe.

[Revendication 6] 6 : Méthode de gestion de cagnottes selon la revendication 5, caractérisée en ce qu'un token ERC20 propriétaire est paramétré avec 18 décimales pour assurer des échanges égaux pour des montants minimaux et avec un *totalSupply* initial de 0, il peut être miné uniquement par le « Smart Contract » lors de la fermeture d'une cagnotte (il est produit pour l'utilisateur fermant la cagnotte) et il ne peut pas être brulé.

[Revendication 7] 7 : Méthode de gestion de cagnottes selon la revendication 5, caractérisée en ce que l'association des ERC20 catégorisés et propriétaires est sécurisée et déterminée dynamiquement par l'administrateur du « Smart Contract », un stablecoin ERC20 peut être ajouté ou supprimé dans une catégorie et ne peut pas faire partie de différentes catégories simultanément.

Abrégé

Procédé portant sur une méthode de gestion de cagnottes solidaires multi devises qu'elles soient personnelles, professionnelles ou associatives. Cette méthode s'appuie sur un « Smart Contract » fonctionnant sur la *blockchain Ethereum* de manière à proposer un système pratique et avantageux pour l'utilisateur au sein d'un réseau social. Ces cagnottes mettent à disposition de l'utilisateur une plateforme d'échange performant des conversions rapides sans utiliser d'oracle externe grâce à la conception de stablecoins résultants des cagnottes soldées. Le libellé « Smart Contract » que nous citons est à la fois notre plateforme d'échange ainsi que notre gestionnaire de cagnottes tandis que les ERC20 propriétaires évoqués sont les stablecoins que nous créons dans le cadre de l'invention.