

Acteurs

Agriculteur (livraison de la récolte)

Entrepôt (gestionnaire de trésorerie)

Auditeur / Administrateur de coopérative

(signataire(s))

Service blockchain (client utilisé pour créer/signer les transactions)

Conditions préalables

Jeton créé avec :

- trésorerie = compte d'entrepôt
- supplyKey = configuré soit comme KeyList (seuil), soit comme clé unique que l'entrepôt signera via HSM ou Schedule workflow.
- maxSupply défini (fini).

Les auditeurs et l'administrateur de la coopérative disposent de clés et d'un processus convenu pour signer les transactions planifiées.

Étape 0 — L'agriculteur livre sa récolte

1. L'agriculteur apporte sa récolte à l'entrepôt.
2. L'entrepôt pèse et crée un **reçu physique** (reçu d'entrepôt) avec :
 - a. Identifiant du producteur, identifiant du lot, poids brut/net, date, lieu de stockage, rapport d'inspection, preuve photographique.
3. L'entrepôt enregistre la réception dans une base de données hors chaîne et crée une entrée dans le journal d'audit.

Étape 1 — Vérification/approbation

1. Le responsable qualité de l'entrepôt et un auditeur externe (ou l'administrateur de la coopérative) **vérifient** la quantité pesée et la qualité.
2. Tous deux signent (hors chaîne) le récépissé d'entrepôt et enregistrent leurs signatures dans le registre d'audit (hachage du récépissé stocké sur la chaîne ou dans un magasin hors chaîne inviolable).

Étape 2 — Préparation de la frappe en tant que transaction programmée

1. L'entrepôt prépare une **transaction TokenMintTransaction** avec le montant = quantité mesurée en jetons (par exemple, 10 000 jetons pour 10 000 kg).
2. Au lieu de la soumettre directement, l'entrepôt crée une **ScheduleCreateTransaction** qui contient la transaction de frappe et une note de planification qui fait référence à l'ID du reçu et aux hachages de l'auditeur/du reçu.
3. Le calendrier nécessite les signatures de l'**auditeur** et de l'**entrepôt** (ou un seuil).
4. Soumettez **ScheduleCreateTransaction** à Hedera. Le calendrier existe mais n'est pas exécuté tant que les signatures requises ne sont pas jointes.

Étape 3 — Signer le calendrier (par l'auditeur / l'administrateur de la coopérative)

- L'auditeur utilise **ScheduleSignTransaction** pour ajouter sa signature à `scheduleId`.
- Lorsque le calendrier atteint le nombre de signatures requis, Hedera exécute automatiquement la **transaction TokenMintTransaction** et dépose les jetons frappés dans le **compte du trésor (entrepôt)**.

Étape 4 — Rapprochement et distribution post-frappe

1. Le calendrier s'exécute → les jetons sont frappés dans le compte du Trésor (compte d'entrepôt).
2. Le service blockchain lit le reçu de frappe et stocke le `tokenId`, le montant, le `scheduleId` et le `transactionId` dans le registre hors chaîne lié au reçu d'entrepôt.
3. L'entrepôt met à jour son inventaire : les jetons numériques garantissent désormais les biens physiques.
4. L'entrepôt distribue les jetons aux agriculteurs/investisseurs selon la répartition convenue :
 - a. Transférer les jetons du trésor vers le compte de l'agriculteur ou les comptes des investisseurs à l'aide de **TransferTransaction**.
5. Toutes les actions sont consignées à des fins d'audit.

Étape 5 — Rachat

- L'acheteur transfère/brûle les jetons ou les renvoie à la trésorerie (selon votre modèle de rachat), l'entrepôt livre les marchandises physiques et brûle les jetons ou les marque comme réglés.

Plus de détails

Lors de la tokenisation des récoltes sur Hedera, chaque token est défini comme une unité fongible qui représente directement un kilogramme d'un produit agricole tel que le maïs ou le riz. Par exemple, si un agriculteur livre mille kilogrammes de riz, l'entrepôt peut émettre mille tokens. Le token a un approvisionnement limité mais pouvant être frappé. Cela signifie que lorsque le token est créé, une limite maximale est fixée, par exemple un milliard d'unités, et Hedera veille à ce que ce plafond ne soit jamais dépassé. Cependant, au lieu de frapper tous les jetons à l'avance, le système les frappe progressivement à mesure que les récoltes sont physiquement mesurées et vérifiées. Si la récolte prévue est d'un million de kilogrammes, mais que la récolte réelle vérifiée est de sept cent vingt mille kilogrammes, seuls sept cent vingt mille jetons sont frappés. Si trente mille kilogrammes supplémentaires sont confirmés par la suite, trente mille jetons supplémentaires peuvent être frappés. Ce modèle garantit que l'offre de jetons reflète toujours la récolte réelle tout en évitant le risque d'une inflation incontrôlée.

Le compte du Trésor est le portefeuille central qui détient initialement tous les jetons émis, et ce compte est géré par l'entrepôt ou la coopérative. Cela est logique, car l'entrepôt est le dépositaire de la récolte physique et est donc naturellement responsable des jetons numériques. Le solde du compte du Trésor doit toujours correspondre exactement au stock physique stocké dans l'entrepôt. Si l'entrepôt détient physiquement cent tonnes de riz, le Trésor doit détenir cent mille jetons de riz.

Pour sécuriser le processus de frappe, le modèle choisi s'appuie sur les transactions programmées Hedera. Cette méthode empêche l'entrepôt de créer unilatéralement de nouveaux jetons. Au lieu de cela, lorsque l'entrepôt a besoin de frapper des jetons, il prépare une transaction de frappe, mais la soumet en tant que transaction programmée. Cette transaction ne s'exécute pas immédiatement ; elle reste en attente jusqu'à ce qu'une partie externe, telle qu'un auditeur ou un administrateur coopératif, ajoute sa signature. Ce n'est que lorsque l'entrepôt et l'auditeur ont tous deux signé que Hedera exécute la frappe, déposant automatiquement les nouveaux jetons sur le compte du Trésor. Cela garantit que l'émission de jetons passe toujours par une double validation, combinant le rôle de conservation de l'entrepôt et une surveillance indépendante.

Le cycle de vie complet commence lorsque l'agriculteur livre sa récolte à l'entrepôt. À ce stade, l'entrepôt pèse les produits, effectue des contrôles de qualité et délivre un récépissé d'entrepôt. Ce récépissé enregistre des informations telles que l'identité de l'agriculteur, le numéro de lot, le poids brut et net, le contenu, le rapport d'inspection, le lieu de stockage et des preuves à l'appui, telles que des photographies. Le récépissé est stocké dans une base de données hors chaîne et son hachage numérique peut être enregistré sur la chaîne à des fins d'audit. Une fois le récépissé établi, le responsable de la qualité de l'entrepôt et l'auditeur externe ou l'administrateur de la coopérative vérifient les informations. Ils approuvent le récépissé et leurs signatures sont stockées dans un registre d'audit inviolable.

Après vérification, l'entrepôt prépare une transaction de frappe représentant le poids vérifié en jetons. Plutôt que de l'exécuter directement, il intègre la transaction dans une transaction programmée, en y incorporant des métadonnées telles que l'identifiant du reçu et le hachage du fichier du reçu. À ce stade, la transaction existe sur Hedera mais reste en sommeil. L'auditeur ou l'administrateur de la coopérative examine ensuite le reçu et le calendrier, et si tout est valide, il signe le calendrier. Une fois les signatures requises obtenues, Hedera exécute automatiquement la création et les jetons apparaissent dans le compte de trésorerie contrôlé par l'entrepôt.

Après la création, le service blockchain enregistre les détails de la transaction et les relie au récépissé d'entrepôt correspondant dans la base de données hors chaîne. L'entrepôt procède ensuite au rapprochement de ses stocks, confirmant que la récolte physique stockée correspond aux jetons créés. Les jetons peuvent alors être distribués. Les agriculteurs reçoivent les jetons correspondant à leur contribution à la récolte, tandis que les investisseurs peuvent également recevoir des allocations. La distribution s'effectue par le biais de transactions de transfert de jetons, et chaque étape est enregistrée à des fins d'audit.

Plus tard, lorsque les jetons sont rachetés, l'acheteur ou l'agriculteur les renvoie au trésor ou les fait brûler, selon le mode de rachat. En échange, l'entrepôt livre la quantité équivalente de produits physiques. Cela clôt le cycle de vie, garantissant que chaque jeton correspond toujours à un actif physique, et une fois racheté, le jeton est soit retiré de la circulation, soit marqué comme réglé.

Grâce à ce modèle, les jetons restent entièrement liés à la production agricole réelle, leur émission est strictement contrôlée grâce à une double validation avec des transactions programmées, et la responsabilité est maintenue car l'entrepôt gère la trésorerie tandis que l'auditeur garantit la confiance. Le service blockchain fournit le pont numérique, reliant les reçus physiques aux transactions sur la chaîne et maintenant l'intégrité de la piste d'audit.

Nb : Un registre d'audit inviolable est un système conçu pour fournir un enregistrement sécurisé, immuable et vérifiable des modifications apportées aux données, garantissant ainsi que toute tentative de modification des données soit détectable. Ceci est rendu possible grâce à des techniques cryptographiques qui créent une chaîne de preuves, où chaque entrée est liée à la précédente via un hachage cryptographique unique. Une fois les données enregistrées dans un tel registre, elles ne peuvent être modifiées ou supprimées sans rompre la chaîne de hachages, ce qui signale immédiatement toute tentative de falsification.

PROCESSUS DE TOKENISATION HARVEST



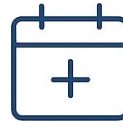
Livraison

Le fermier livre
récolte à l'entrepôt



Vérification

Entrepôt et
auditeur/coopérative
admin vérifier et sip



Frappe

Préparation de l'entrepôt
frappe programmée avec
signature de l'auditeur



Distribution

Entrepôt
transfert des jetons
au fermier et
aux investisseurs

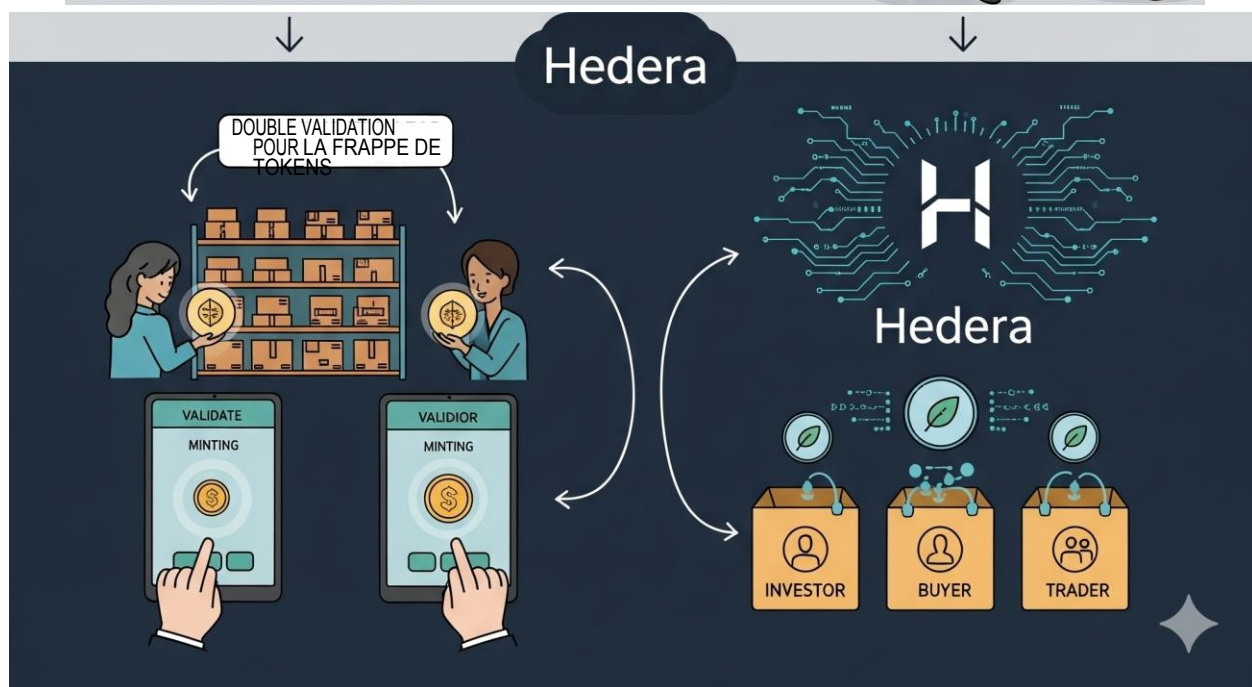
Un jeton fongible représente 1 kilogramme de récolte. Les jetons sont plafonnés à un approvisionnement maximal et minés progressivement à mesure que les quantités récoltées sont confirmées.

Les jetons sont frappés dans un compte de trésorerie géré par l'entrepôt, qui détient les marchandises physiques. L'entrepôt crée une transaction programmée pour la frappe, qui nécessite la signature d'un auditeur ou d'un administrateur de la coopérative pour être exécutée.



Rachat

L'acheteur rachète les jetons
ou les retourne à l'entrepôt



Système de tokenisation agricole basé sur la blockchain

