# Livre Blanc du projet Humble Luck Ball


Protocole de Proof of Entry (PoE)

Tony VERSCHUEREN et Julian CAILLE
Président et Directeur Général de Humble Luck Ball
Le 6 Novembre 2020
Actualisé au 20 Février 2022
V.2.0.0

# Table des Matières

# Lexique Blockchain

| | |
|---|---|
| Application décentralisée | Application qui fonctionne sur un réseau décentralisé, par opposition aux applications classiques qui dépendent de serveurs centralisés. Elle a comme support un ou plusieurs smart contracts déployés sur une blockchain. La partie front-end (interface utilisateur), elle, peut être développée comme sur les applications classiques. Dans l'écosystème de la blockchain ethereum, les applications décentralisées sont appelées dapps. |
| Avalanche | Plateforme décentralisée sous le consensus de Preuve d'Enjeu (Proof of Stake) et du protocole "Snow". Elle se positionne comme blockchain la plus rapide d'exécution par rapport au temps nécessaire à réaliser une opération. |
| Bitcoin | Système de transfert et de vérification de propriété reposant sur un réseau de pair à pair sans aucune autorité centrale, conçu en 2009 par un développeur utilisant le pseudonyme Satoshi Nakamoto. Son unité de compte est la monnaie électronique bitcoin. |
| Blockchain | Technologies permettant de stocker et d'échanger de la valeur sur internet sans intermédiaire centralisé (définition de Blockchain France). Elles sont le moteur technologique des cryptomonnaies, du Web Décentralisé et de son corollaire, la finance décentralisée. Par extension, une blockchain (littéralement une "chaîne de blocs") désigne une base de données sécurisée et décentralisée, répliquée sur un très grand nombre de serveurs, et contenant un ensemble de transactions dont chacun peut vérifier la validité. Une blockchain peut donc être assimilée à un grand livre comptable transparent, pseudonyme et infalsifiable. |
| Consensus | Toute cryptomonnaie fonctionne grâce à un protocole, c'est-à-dire un ensemble de règles de communication permettant d'arriver à un accord de manière décentralisé. Les règles composant ce protocole sont appelées règles de consensus. Dans le cas d'une chaîne de blocs, elles servent à définir la validité des transactions et des blocs. |
| Cryptomonnaie | Monnaie électronique, échangeable en pair-à-pair (c'est-à-dire sans intermédiaire), se basant sur des principes cryptographiques et des mécanismes d'incitation économique pour la validation des transactions et la génération de la monnaie elle-même. |
| Ethereum | Plateforme décentralisée, fondée sur la blockchain éponyme, qui vise l'avènement d'un web décentralisé. La blockchain d'ethereum fonctionne avec la cryptomonnaie ether. Contrairement à la blockchain du bitcoin, focalisée sur l'aspect monétaire, la blockchain d'ethereum a vocation à accueillir des programmes très divers, appelées dapps, qui fonctionnent avec des smart contracts. On parle d'écosystème ethereum pour désigner l'ensemble des acteurs qui travaillent sur cette plateforme. |
| Gossip Algorithm | Un protocole ou algorithme de bavardage (Gossip Algorithm) désigne un algorithme distribué dans un réseau informatique pair à pair pour propager l'information à tous les agents du réseau. |
| ICO (Initial Coin Offering) | Méthode de levée de fonds fonctionnant via l'émission d'actifs numériques, appelés tokens, échangeables contre des cryptomonnaies durant la phase de démarrage d'un projet. |
| Ledger | Un registre distribué (aussi appelé registre partagé ; en anglais, distributed ledger ou shared ledger) est un registre simultanément enregistré et synchronisé sur un réseau d'ordinateurs, qui évolue par l'addition de nouvelles informations préalablement validées par l'entièreté du réseau et destinées à ne jamais être modifiées ou supprimées. |

| | |
|---|---|
| Minage | Utilisation de la puissance de calcul informatique afin de traiter des transactions, sécuriser le réseau et permettre à tous les utilisateurs du système de rester synchronisés. |
| Mineur | Personnes (particuliers ou sociétés) qui connectent sur le réseau une ou plusieurs machines équipées pour effectuer du minage. Chaque mineur est rémunéré au prorata de la puissance de calcul qu'il apporte au réseau. |
| Noeud | Ordinateur relié au réseau blockchain et utilisant un programme relayant les transactions. Les nœuds conservent une copie du registre blockchain et sont répartis partout dans le monde. |
| Proof of Stake (PoS) | Méthode pour atteindre le consensus distribué dans un réseau blockchain. A l'inverse du proof of work, le proof of stake ne demande pas aux utilisateurs d'utiliser leur puissance de calcul, mais de prouver la propriété d'un certain montant de cryptomonnaie. Ethereum vise le passage au proof of stake à moyen terme. |
| Proof of Work (PoW) | "Preuve de travail" ou "preuve de calcul". Méthode utilisée pour atteindre le consensus distribué dans un grand nombre de blockchains publiques, bitcoin en tête. Concrètement, il s'agit du traitement cryptographique permettant la validation des blocs de transactions. Effectuer ce traitement requiert du temps de calcul : en général, un seul ordinateur du réseau y parvient en environ dix minutes. La difficulté est régulièrement adaptée pour maintenir cet intervalle. |
| Répartition équidistributive pRNG | Un générateur de nombres pseudo-aléatoires, pseudorandom number generator (PRNG) en anglais, est un algorithme qui génère une séquence de nombres présentant certaines propriétés du hasard. Par exemple, les nombres sont supposés être suffisamment indépendants les uns des autres, et il est potentiellement difficile de repérer des groupes de nombres qui suivent une certaine règle (comportements de groupe). |
| Scalabilité | Passage à l'échelle. C'est le plus grand défi aujourd'hui des blockchains. L'une des questions majeures est : comment augmenter le nombre de transactions réalisées par seconde, sans compromettre la décentralisation et la sécurité ? Des solutions techniques sont en cours de conception ou d'implémentation sur les grands protocoles : la solution de state channels off-chain (Lightning Network sur Bitcoin, Raiden Network sur Ethereum), le sharding, Plasma pour les smart contracts sur Ethereum, etc. |
| Smart Contract | Programme autonome qui, une fois démarré, exécute automatiquement des conditions inscrites en amont dans la blockchain, sans nécessiter d'intervention humaine. Il fonctionne comme toute instruction conditionnelle de type "if – then" (si telle condition est vérifiée, alors telle conséquence s'exécute). Pour déclencher son exécution, un smart contract se connecte à une base de données jugée fiable, via l'intermédiaire d'un oracle (un service qui fait le lien entre le smart contract et le monde réel). |
| Soft Fork | Un soft fork ("embranchement doux") est une modification rétrocompatible des règles de consensus, qui ne cause pas de séparation si elle est appliquée par une majorité de la puissance de validation. Le soft fork est essentiellement restrictif (ajout de nouvelles règles). |
| Hard Fork | Un hard fork ("embranchement dur") est un embranchement de la chaîne de blocs causé par une modification des règles de consensus. Par extension, le terme sert également à désigner tout changement non rétrocompatible du protocole susceptible de causer une duplication permanente de la chaîne. |
| Token | Actif numérique personnalisé par son auteur, émis et échangeable sur une blockchain, et possédant les caractéristiques d'une cryptomonnaie : infalsifiabilité, unicité, enregistrement des échanges dans un registre immuable, sécurité des échanges, etc. En particulier, un token est transférable (et non duplicable) entre deux parties sur internet, sans nécessiter l'accord d'un tiers. |

## Equipe

Tony VERSCHUEREN
Président & CEO, CFO

Julian CAILLE
Directeur Général & CTO

Camille SERGENT
Marketing et Communication

## Historique

| **2018, 2019** |
|---|
| Emergence de l'idée |
| Recherche et développement des premiers prototypes |
| **2020** |
| Création de la société Humble Luck Ball |
| Site internet Humble Luck Ball disponible |
| Présentation du Livre Blanc V1.0.0 |
| **2021** |
| ICO du 27 Février au 27 Juin |
| Finaliste AIBC Summit à Dubaï en Mai |
| Articles CoinTribune, et Journal Du Coin |
| Migration blockchain Ethereum →Avalanche |
| **2022** |
| Présentation du Livre Blanc V2.0.0 |
| *Déploiement du DEX Humble Market* |
| *Protocole de Preuve d'Entrée, Mainnet 1.0* |

# 1 Résumé

## 1.1 Qu'est-ce que le projet Humble Luck Ball ?

Le projet Humble Luck Ball développe un nouveau consensus de blockchain appelé Preuve d'Entrée (Proof of Entry), dans le but de créer une blockchain facile et accessible à tous sans minage ou séquestration d'actif. Ce consensus est 100% communautaire et le processus de récompense de bloc est non-discriminatoire.

Le constat actuel démontre que des consensus de Preuve de Travail (Proof of Work) et Preuve d'Enjeu (Proof of Stake) contraignent et/ou empêchent les acteurs du réseau d'obtenir les récompenses de blocs facilement, principal responsable de l'inflation des systèmes économiques des blockchains. En effet, il est nécessaire d'acquérir un équipement de minage conséquent, ou de séquestrer énormément d'actif afin d'avoir un poids suffisant sur le réseau et obtenir un rendement.

La solution que propose Humble Luck Ball avec son consensus de Preuve d'Entrée (Proof of Entry) est une solution de validation par entrée, effectué dans le cadre d'un sacrifice d'actif au profit de la communauté. Ce sacrifice octroie à l'utilisateur un poids dans le système d'élection non-discriminatoire du protocole, grâce auquel il peut obtenir une récompense adaptée à sa participation au réseau.

## 1.2 Quelle est la roadmap ?

Le développement du consensus de Preuve d'Entrée (Proof of Entry) suit une méthodologie de Recherche et Développement. Plusieurs verrous techniques existent, et les étapes suivantes permettront de valider les solutions définies :

- Q2 2022 →Le déploiement du Mainnet 1.0, **protocole** de Preuve d'Entrée, simulé sur la blockchain Avalanche.
- Q1 2023 →Le déploiement du Mainnet 1.5, solution de **sous-réseau du consensus** de Preuve d'Entrée, soutenue par Avalanche.
- Q1 2024 →Le déploiement du Mainnet 2.0, **blockchain de service native** sur consensus de Preuve d'Entrée, indépendante.

## 1.3 Utilité du Luck Ball Coin (LBC)

Le LBC est l'actif numérique du projet Humble Luck Ball. D'abord jeton ERC-20, il deviendra le coin natif de la blockchain basée sous Preuve d'Entrée (Proof of Entry). Voici ses caractéristiques :

- Max Supply : **300.000.000** LBCs.
- Déploiement initial : **2.028.237** LBCs.
- Tokenomic : **100% communautaire**.

Le LBC est utilisé sur le protocole de Preuve d'Entrée afin d'en garantir son bon fonctionnement, à travers la validation intrinsèque des blocs et de la genèse de nouveaux LBCs pour la communauté d'utilisateurs.

Dès le 6 Mars, le jeton LBC peut être récupéré contre de l'AVAX sur la Humble Decentralized Offering, disponible au lien suivant : https://ido.humbleluckball.com. Les caractéristiques de cette HDO sont présentés page 21.

# 2 Le projet Humble Luck Ball (HLB)

## 2.1 Description générale

Jeune start-up créée en Septembre 2020, Humble Luck Ball a été désignée finaliste du Sommet AIBC[1] en 2021 grâce à son nouveau protocole de blockchain. La **PoE** "Proof of Entry" doit permettre de pallier les principales lacunes des cryptomonnaies. Le système économique des tokens **LBC** (pour Luck Ball Coin) est une exception dans le domaine des actifs numériques. L'objectif des fondateurs est de créer une cryptomonnaie 100% indépendante, transparente et communautaire à travers l'écosystème **Humble Luck Ball** (HLB).

Actuellement, les cryptomonnaies reposent en majorité sur des consensus de Proof of Work ou Proof of Stake qui récompensent les utilisateurs avec des actifs de la blockchain sollicitée.

Le premier consensus **Proof of Work** est connu pour **consommer énormément d'énergie**, et trouve avec le second (**Proof of Stake**) ses limites **d'équité** envers ses mineurs/validateurs. Sans équipement conséquent ou énormément de jetons à investir, il est presque impossible pour de nouveaux arrivants de participer à l'évolution d'une blockchain. **C'est pour ces raisons qu'Humble Luck Ball cherche à développer une nouvelle technologie basée sur un nouveau consensus de blockchain employant un protocole totalement innovant : "Proof of Entry"**. Il doit permettre de pallier les défauts cités ci-dessus, tout en proposant un système accessible au grand public.

Pour résumer, le consensus de Preuve d'Entrée doit permettre à tout utilisateur de facilement devenir un nœud participant et éligible aux récompenses de bloc du système, indépendamment de leur poids sur le réseau décentralisé. Les utilisateurs devraient ainsi pouvoir participer à un réseau 100% communautaire et scalable.

Nous allons lever de nombreux **verrous scientifiques et techniques** afin **d'aboutir à une technologie et solution implémentable. La conception de cette technologie nécessite de nombreuses études, essais, tests et développements.** Ainsi, l'opération de recherche & développement représente actuellement l'ensemble des activités de la société.

*[1] L'AIBC est l'un des principaux événements mondiaux pour les technologies émergentes visant à rassembler une sélection d'élite de délégués, de politiciens et de leaders d'opinion du monde entier. Ce soutien et cet intérêt internationaux ont contribué à propulser le Sommet de l'AIBC à devenir l'un des favoris du circuit mondial des conférences et expositions sur les technologies émergentes.*

## 2.2 Objectif du projet HLB

La blockchain est une technologie qui permet de stocker et transmettre des informations de manière totalement transparente et sécurisée. On parle souvent de blockchain avec les cryptomonnaies telles que le Bitcoin (avec la Proof of Work) ou l'Ethereum (future Proof of Stake).

| Proof of Work (PoW) | Proof of Stake (PoS) |
|---|---|
| Les noeuds participants sont des mineurs | Les noeuds participants sont des validateurs |
| La capacité minière dépend de la puissance de calcul | La validation de la capacité dépend de l'enjeu du réseau |
| L'exploitation minière produit de nouvelles pièces | Aucune nouvelle pièce n'est formée |
| Les mineurs reçoivent des récompenses de bloc | Les validateurs reçoivent des frais de transaction |
| Consommation d'énergie massive | Consommation d'énergie faible à modérée |
| Significativement sujet à l'attaque des 51% | L'attaque des 51% est pratiquement impossible |

- Le consensus de Proof of Work (PoW) a comme principaux inconvénients d'être extrêmement coûteux en computation informatique et d'être réservé à des individus ayant la capacité de s'équiper d'un outil de calcul puissant et onéreux.
- Le consensus de Proof of Stake (PoS) a comme principaux inconvénients de restreindre son économie sur des actifs déjà en circulation, tout en demandant aux validateurs de séquestrer leurs actifs au titre d'un pouvoir de validation, et ce pour une durée déterminée.

Ici, le projet Humble Luck Ball a pour ambition de proposer un autre protocole de blockchain sur lequel un nouveau consensus (cf. lexique) sera développé : la **Proof of Entry (PoE)**.

| Proof of Entry (PoE) |
|---|
| Les noeuds participants sont des utilisateurs |
| La validation de la capacité dépend du nombre d'utilisateurs |
| L'utilisation du contrat émet de nouvelles pièces |
| Les utilisateurs reçoivent des récompenses de cycle |
| Consommation d'énergie faible à modérée |
| L'attaque des 51% est pratiquement impossible |

La volonté des fondateurs est de concevoir un système :

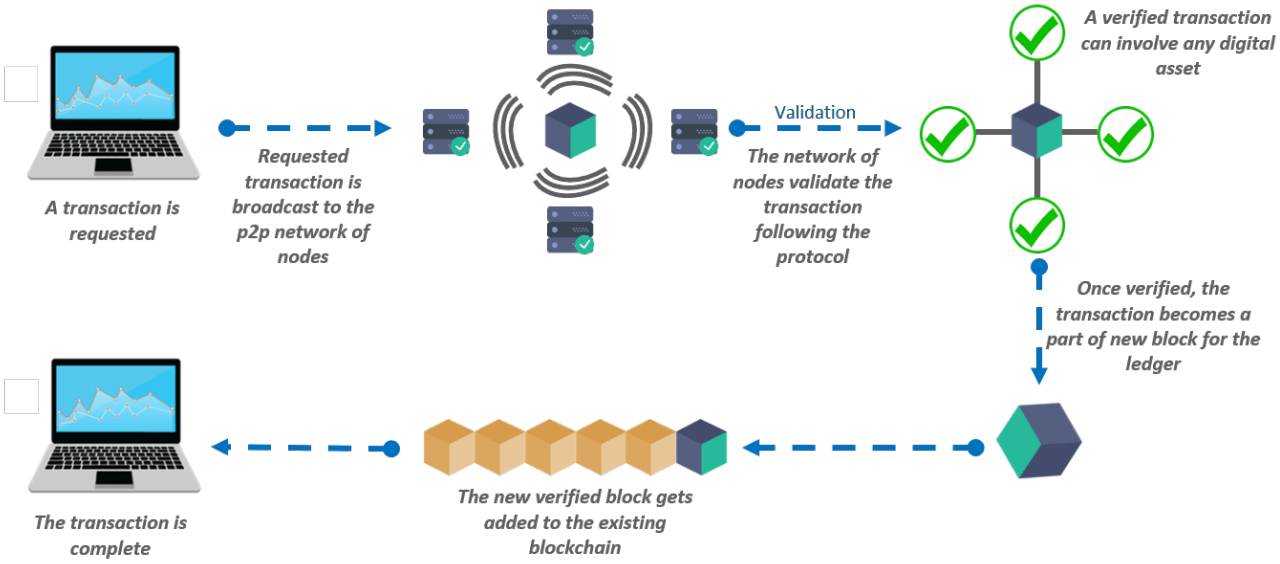
- simple à comprendre et à utiliser.
- basé sur la participation communautaire.
- décentralisé de tout intervenant secondaire.
- équitable entre tous ses utilisateurs.
- sécurisé pour tous ses utilisateurs.

L'intérêt de ce nouveau consensus est de permettre à tout utilisateur de facilement participer en tant que nœud validateur, en ayant un impact sur l'émission de nouvelles pièces tout en obtenant une récompense égale à la contribution communautaire dont la distribution est aléatoire et exclusivement déterminée par la communauté d'utilisateurs.

De plus, le consensus de Proof of Entry permettrait d'utiliser 100% de l'effort validateur au titre de la blockchain et de ne causer aucune perte. Pour y parvenir, le principe est de générer des récompenses en fonction des entrées effectuées sur le réseau et de la stimulation de la blockchain, en fonction du nombre d'actif envoyé sur les cycles d'élection. Cela signifie que plus les utilisateurs interagissent avec la blockchain au cours d'un cycle, plus il y a de tokens LBC générés. Tout cela sera régi par un mécanisme de halving pour éviter une pénurie d'approvisionnement ou des inflations trop importantes. À la fin d'un cycle, le système choisira le nœud recevant une récompense en calculant les entrées de participation générées par les utilisateurs participants, et déclencher un **algorithme de répartition équidistributive pRNG déterministe** pour sélectionner les adresses récompensées.

## 2.3 Etat de l'Art

Une blockchain est un système totalement décentralisé et basé sur un réseau pair à pair (peer-to-peer). Chaque objet du réseau conserve une copie du ledger (cf. lexique) afin d'éviter d'avoir un point unique de défaillance. Toutes les copies sont mises à jour et validées simultanément. Bien que l'objectif initial de la création de la blockchain fût la résolution du problème de la dépense multiple en crypto-monnaie (monnaie virtuelle), cette technologie peut être explorée dans de nombreux cas d'utilisation et utilisée comme un moyen sécurisé de gestion et protection de toute sorte de données (monétaire ou pas). [AYADI 2019]




Etapes de fonctionnement d'une blockchain

*source : Medium*

La blockchain en est encore aux premiers stades de son développement. La première phase est la Blockchain 1.0 [SWAN 2015, GATTESCHI 2018], dont la crypto-monnaie la plus représentative est le Bitcoin [NAKAMOTO 2008]. L'apparition de contrats intelligents a ensuite initié la deuxième phase, la Blockchain 2.0 [CHRISTIDIS 2016].

La prochaine génération de blockchain sera l'ère de la société programmable avec blockchain des choses. Les aspects liés à la blockchain pourraient affecter à la fois l'idéologie humaine et la forme sociale [LU 2018]. C'est sur cet axe du développement des interactions équitables des hommes qu'Humble Luck Ball cherche à développer un nouveau consensus, un protocole innovant et une cryptomonnaie l'employant.

Développer une blockchain nécessite de construire 6 couches successives (cf. schéma ci-dessous).

| **Couches** | **Principales technologies ou composants** |
|---|---|
| **Couche de données** | Bloc de données, structure de chaîne, horodatage, arbre de Merkle, cryptographie |
| **Couche réseau** | Réseau P2P, mécanisme de vérification, protocole de diffusion |
| **Couche de consensus** | PoW, PoS, DPoS, PBFT, ... |
| **Couche de contrat** | Contrat intelligent, codage de script, mécanisme d'incitation |
| **Couche de service** | Ethereum, hyperledger, IBM Azure BaaS, ... |
| **Couche d'application** | Crypto-monnaie, santé, service cloud, ... |

La construction de ces différentes couches nécessite de créer de nouvelles structures, de nouvelles façons d'enregistrer, de stocker, d'exprimer les données, et surtout de les valider. **Le mécanisme de consensus est le point central qui définit une blockchain**. Le principe de consensus choisi définit les règles de fonctionnement de la blockchain en question. La conception de ce mécanisme définit les interactions entre les groupes de nœuds. Sa fonctionnalité en

système distribué et son intégrité représentent un réel enjeu technique [LU 2019].

Par exemple, pour le bitcoin, le protocole engendre une grande quantité de ressources et de puissance de calcul, qui conduisent à un faible débit système et à une latence système longue [SANKAR 2017]. La confidentialité et l'évolutivité sont également critiquées car il n'y a pas d'utilisateurs privilégiés, mais plutôt un participant peut rejoindre le réseau, avoir accès aux informations disponibles sur blockchain, et également valider de nouvelles transactions. Tout comme sont critiquées les limites d'évolutivité en référence à la taille des données et le taux de traitement de la transaction [YLI HUUMO 2016]. Les problèmes de confidentialité et de sécurité sont les préoccupations majeures dans les blockchains au fur et à mesure que l'information devient accessible à tous les pairs du réseau.

Ainsi, bien que la base de la technologie blockchain soit relativement mature, il reste encore de nombreux problèmes techniques à résoudre. De nombreux protocoles existent mais aucun ne réussit actuellement à répondre à l'ensemble des enjeux suivants :

- économie d'énergie,
- économie de coûts,
- puissance d'exécution,
- puissance d'évolutivité, sécurité, équité [ZHENG 2017]

Répondre à ces différentes problématiques implique de développer un nouveau consensus, et donc une nouvelle manière de déterminer la validation des nœuds et la récompense associée.

**Définir, ne serait-ce que la structure de cette équation nécessite de l'étude, des développements et essais. Cette équation doit ensuite être testée à l'échelle pour mesurer les résultats, et s'assurer de leur cohérence.**

**Afin d'étudier comment l'équation se comporte face à de fortes variations (hausse ou baisse) d'activité, des simulations et expérimentations portant sur la fonctionnalité sont nécessaires, et permettront d'évaluer et qualifier la scalabilité et l'évolutivité du système.**

## 2.4 Feuille de route du projet HLB

Afin de développer Humble Luck Ball, différentes briques doivent être conçues, développées et testées :

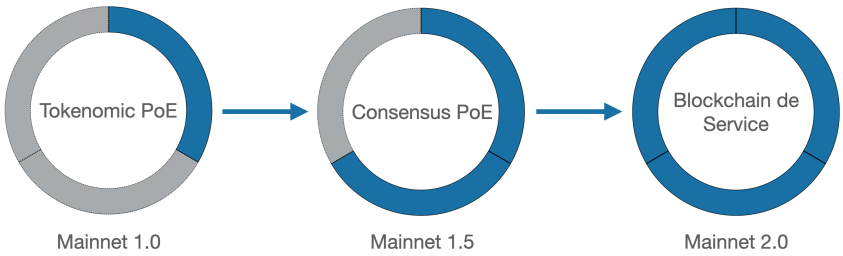
- Le protocole de Preuve d'Entrée, Proof of Entry (PoE)
- Le jeton Luck Ball Coin (LBC)
- Le contrat intelligent Humble Luck Ball (HLB)
- La dAPP Humble Luck Ball
- La plateforme d'échange Humble Market

Le premier objectif à atteindre est le déploiement du protocole "Proof-of-Entry" (PoE) disponible au public et son jeton numérique sous-jacent : le Luck Ball Coin (LBC). Le protocole est composé d'un ensemble de Smart Contracts (instructions exécutables sur une blockchain compatible EVM) découplés en plusieurs services. Le protocole fonctionne de façon décentralisée : la gestion de l'inflation du LBC et son évolution dans le temps, grâce à des algorithmes adaptatifs basés sur les participations aux cycles du protocole est un point critique.

Ce protocole doit être déployé sur une blockchain compatible EVM et publique, pour assurer un Layer 1 utilisable et sécurisé. Nous envisageons de déployer ce protocole sur la blockchain "C-Chain" d'Avalanche. Une "Decentralized Application" (dAPP), permettant aux utilisateurs d'interagir avec les Smart Contracts de la PoE, sera disponible sous la forme d'une application web et simplifiera les actions que pourront effectuer les utilisateurs de la PoE. Nous souhaitons atteindre un traitement de 200 blocks par cycle PoE, sans limite de participants par cycle. Nous nommons cette phase Mainnet 1.0 et elle permet une première émulation du consensus PoE.

Le deuxième objectif est la **création d'une "blockchain custom" comportant sa monnaie native "Luck Ball Coin", et hébergée en tant que "subnet" sur le réseau Avalanche**. Cet objectif permettra d'intégrer la gestion décentralisée de la "seed" nécessaire à la génération de nombre pseudo-aléatoires décentralisée. Cela permettra aussi de s'affranchir à termes des limitations de la C-Chain en termes de traitement de données par block qui est actuellement de 8 million (gas limit). Une dAPP permettra l'accès à la blockchain et à la gestion du portefeuille natif. Une migration sera disponible pour le transfert des assets présents sur la C-Chain vers la blockchain custom. Cette phase permettra aussi la mise en place d'un premier prototype d'algorithme d'attribution d'un Community Contributor Token (CCT) pour la mise en place d'un système de délégation de validation pour le consensus PoE. Cette phase correspond au Mainnet 1.5 et permet une transition entre un consensus émulé vers un consensus natif PoE.

Le troisième objectif est le **déploiement d'une blockchain native avec consensus PoE**. Cette blockchain permettra de proposer des déploiements de Smart Contracts (couche contrat cf. Table 3) et notamment de l'utilisation de ses différents services proposés : blocks rewards, utilisation d'un système de verifiable delayed function, validation des transactions sur le réseau décentralisé. Cette étape permet une plus grande scalabilité et déploiement de solutions en couche supérieure, tout en assurant une blockchain à basse consommation électrique (comparée à une blockchain PoW) et en garantissant un accès non-discriminatoire aux récompenses de block du système. Cette phase correspond au Mainnet 2.0. Lors de cette phase Mainnet 2.0 (engagée à partir de 2024 en fonction de l'avancée des travaux), HLB pourra ouvrir au public des possibilités de développement d'algorithmes décentralisés évolutifs et accessibles, de développement d'actifs numériques complexes avec règles, clauses et avenants personnalisés.




## 2.5 Incertitudes, verrous technologiques et problèmes à résoudre

Comme évoqué dans les parties précédentes, différents verrous doivent être dépassés pour développer ce nouveau consensus :

- **Concilier le système d'attribution de poids de confiance aux nœuds participants de la Preuve d'Entrée et leurs participations sur le réseau en tant que validateur ou délégateur.**

Développer un nouveau protocole nécessite de trouver les règles qui permettent le fonctionnement du système, tout en garantissant l'équité du système, sa sécurité ou sa scalabilité par exemple. Il faut être en mesure de développer un protocole qui attribue les bons poids de confiance, et qui assure que même si l'attribution est accordée à un acteur malicieux, cela ne fragilise pas l'exécution du système. Un gossip algorithm (cf. lexique pour définition) doit être développé afin de pouvoir départager les utilisateurs et trancher sur la validation ou non d'un cycle.

**La problématique technique majeure** du projet générant l'essentiel du **verrou technique** réside donc dans la question suivante : "Alors que le principe de la blockchain est que toutes les données sont publiques et disponibles, comment générer une data vérifiable à tout moment, sans être connue des participants avant d'être disponible sur la blockchain" ?

- **Assurer la stabilité et la sécurité d'un protocole de rétention de données provisoire en Layer 2 de la PoE alors que le consensus est immuable dans le temps sur une blockchain publique**
- **Assurer une scalabilité et une vitesse de traitement de l'information sans organe de contrôle en conciliant les différentes méta-transactions du système nécessaires à l'existence des applications de HLB**

- **Garder une paramétrisation suffisante** pour mitiger les besoins de hardfork (cf. lexique) de la blockchain et la coupler à un système de vote décentralisé pour éviter une gouvernance sous-jacente ou des problèmes de mise à jour du consensus **sans diminuer la sécurité du système** (sans dépasser le seuil de tolérance d'acteurs malicieux).

## 2.6 Méthodologies appliquées

### 2.6.1 Démarche générale

Chaque étape de développement de nos solutions décentralisées suit les étapes suivantes :

1. Conception POC (Proof Of Concept) et Tests Unitaires : Les tests unitaires permettent de s'assurer des non-régressions que pourraient apporter le développement ou mise à jour de fonctionnalités.
2. Simulation Locale / Benchmarking : La simulation locale et benchmarking permettent un suivi et une vérification de la scalabilité du système avant déploiement sur le testnet.
3. Testnet : Le testnet permet le test en situation "réelle" avec des utilisateurs non-simulés pour une découverte en avant première des nouvelles fonctionnalités avant leur passage "stable" sur le réseau de production "mainnet".

Afin de qualifier la réussite de chaque étape du protocole, les modules sont continuellement vérifiés et mis à jour avec des processus de CI/CD. Une vérification automatique des dépendances est aussi faite pour vérifier les vulnérabilités potentielles.

### 2.6.2 Travaux réalisés

Les travaux de recherche qui ont été menés ont notamment permis de développer les premières briques de la blockchain Humble Luck Ball.

Nous avons d'abord conceptualisé le protocole PoE en effectuant des calculs théoriques et des diagrammes d'architecture. Cette étape nous a permis de délimiter et d'architecturer les fonctionnalités nécessaires au développement du protocole PoE sur une blockchain compatible EVM. Cela nous a permis de créer un premier prototype du protocole PoE découplé en plusieurs services. Il était cependant imparfait et nous avons pu optimiser certains facteurs pour assurer plusieurs choses :

- Une meilleure équiprobabilité des élections des participants
- Des participations utilisateurs à frais constant peu importe le nombre de LBC envoyé au cycle (O(n) $\rightarrow$O(1))
- Une épuration du système tout en gardant une modularité suffisante en cas d'upgrade des contrats

**Certaines étapes ont été particulièrement complexes au cours de l'année 2021 :**

Ces étapes représentent les fondations sur lesquels se basent tous les autres éléments futurs du développement du consensus de Proof of Entry. Des prises de décision arbitraires ont été décidées sur des bases purement hypothétiques de ce que nous imaginons être le consensus de demain, ainsi il n'y a aucune certitude quant au fait que l'ensemble de ces hypothèses permettra de développer la blockchain HLB.

- **Développement des contrats intelligents comprenant le protocole de Preuve d'Entrée, déploiement de ces derniers sur une blockchain disponible sur un testnet appelé Rinkeby (blockchain Ethereum).**

Concernant le déploiement du protocole PoE et de son jeton numérique sous-jacent le LBC, nous devions tout d'abord créer un actif numérique répondant à une norme de sécurité établie (ERC) pouvant être utilisé comme nous l'imaginions sur le protocole HLB.

- **Déploiement du protocole Humble Luck Ball sur la blockchain Ethereum car incompatibilité entre ressources nécessaires et rendement pour l'utilisateur/Humble Luck Ball :**

Cette incompatibilité vient notamment du montant en Ether (ETH) à dépenser sur la blockchain Ethereum pour toute transaction, interaction de contrat, et utilisation du protocole HLB par les futurs utilisateurs. Il serait incongru d'imaginer un protocole nécessitant un coût supérieur au rendement éventuel généré par l'inflation d'un nombre de LBC étant dynamiquement généré par l'utilisation faite du protocole par les utilisateurs.

Par ailleurs, la blockchain Ethereum nous limite dans les interactions initialement imaginées du protocole de Proof of Entry par le "block gas limit", qui limite le nombre potentiel d'utilisateurs dans un cycle HLB.

- Optimisation des frais de gas liés à l'utilisation du protocole Humble Luck Ball pour les utilisateurs.
- Optimisation des frais de gas internes des différents algorithmes d'élection et de traitement des blocks rewards/participations aux cycles.
- Optimisation de l'architecture du protocole pour une meilleure efficacité de traitement de données, memory footprint et finalité transactionnelle.

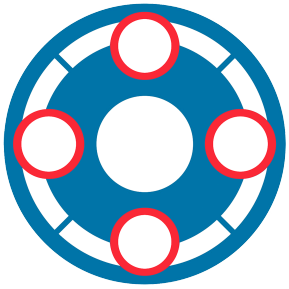
Par la suite, nous avons pu envisager le développement et le déploiement du protocole HLB (Humble Luck Ball) comprenant le protocole de PoE (Proof of Entry). À ce titre, nous avons :

- Effectué les tests suivants :
    1. Test de la bonne réception de l'actif numérique LBC sur le protocole HLB via blockchain locale et blockchain Ethereum de test (Rinkeby).
    2. Test de la concordance des appels entre tous les contrats intelligents composant le protocole HLB.
    3. Test de l'indépendance totale des contrats intelligents face à une utilisation extérieure.
    4. Test publique (condition réelle de testnet) pour visualiser la réaction des algorithmes dynamiques intégrés au protocole HLB. (18 Cycles sur la blockchain Ethereum de test Rinkeby, actuellement 85 Cycles sur la blockchain Avalanche de test Fuji)
- Répondu aux échecs suivants :
    1. L'impossibilité d'adapter les contrats composant le protocole HLB une fois ces derniers déployés. →Résolu.
    2. L'impossibilité de déployer le protocole HLB sur la blockchain Ethereum au vu des restrictions sur les participations →Migration Avalanche.
- **Développement des contrats intelligents de migration de l'actif numérique du protocole de Preuve d'Entrée, le LBC, de la blockchain Ethereum à la blockchain Avalanche (en cours) et du bridge de communication entre ces deux blockchains.**

Compte tenu des difficultés de développement intrinsèques à la blockchain Ethereum, il est nécessaire d'effectuer une migration de la technologie sur une autre blockchain : la blockchain Avalanche.

La migration sur Avalanche nécessite de vérifier, repenser, redévelopper le fonctionnement de HLB. En l'occurrence, concilier le système d'attribution de poids de confiance aux noeuds participants de la Preuve d'Entrée et leurs participations sur le réseau en tant que validateur ou délégateur a nécessité des efforts supplémentaires, et nous avons :

- Effectué les tests suivants :
    1. Testnet du protocole HLB pendant 18 Cycles sur Rinkeby et actuellement 85 Cycles sur Fuji. (Plus de 15 Million de LBC de test générés grâce aux participations quotidiennes de centaines d'utilisateurs).
    2. Test de l'équidistribution des récompenses de cycles effectués auprès des participants.
    3. Test du système d'inflation du LBC en conséquence des participations des utilisateurs.
    4. Test du rythme d'ouverture et de fermeture des cycles et de la durée de ces derniers sur le protocole HLB.
    5. Test de la difficulté inhérente à la participation à un cycle, en conséquence de l'utilisation faite du protocole HLB.
- Répondu aux échecs suivants :
    1. L'impossibilité de tester davantage d'éléments nous permettant de répondre à ce verrou technique sur le réseau Avalanche. →Nécessite un Subnet Avalanche prévu pour Q1 2023.
    2. L'impossibilité de rendre dynamique le nombre de récompense de bloc par cycle. →Limité à 200 récompenses par cycle du au Block Gas Limit de la blockchain Avalanche.



# 3 Produits et services du projet Humble Luck Ball (HLB)

## 3.1 Le jeton Luck Ball Coin (LBC)

### 3.1.1 Nature du Jeton

Le jeton Luck Ball Coin (LBC) est un jeton utilitaire respectant le standard ERC-20 Ethereum Request for Comment n°20.

Ce jeton est déployé par la société Humble Luck Ball. Il a fait l'objet d'une ICO (cf. lexique) du 27 Février au 27 Juin 2021 résultant à un déploiement de 811,295.09LBCs auprès de 205 détenteurs. Courant Juillet 2021, nous avons orchestré un ajustement de la tokenomic, résultant à la multiplication par x1,5 le nombre de jetons LBCs de chaque participant à l'ICO. A la date de migration du jeton LBC de la blockchain Ethereum à Avalanche, le nombre total de LBC est de 2,028,237.73LBCs auprès de 210 détenteurs.

Initialement déployé sur la blockchain Ethereum, une migration sur la blockchain Avalanche est disponible depuis le 19 Décembre 2021. Aujourd'hui, le jeton LBC fait l'objet d'une IDO présentée plus tard dans ce document en vue du déploiement du Mainnet 1.0. (protocole de Preuve d'Entrée).

Le déploiement de nouveaux jetons LBC est exclusivement régulé par la communauté d'utilisateurs et d'investisseurs. En effet, la particularité du LBC est que son inflation est directement influencée par le concept de Proof of Entry (PoE).

### 3.1.2 Inflation et Halving

Le protocole de Preuve d'Entrée assure l'inflation du LBC lorsqu'un **Cycle** se termine. Les LBCs générés alimentent directement la **Humble Pool**; Coffre-fort de la Preuve d'Entrée d'où les récompenses de cycles sont puisées.

Le nombre de LBC déployés à travers le protocole de Preuve d'Entrée est exclusivement déterminé par l'activité de la communauté d'utilisateurs grâce à leurs participations au contrat Humble Luck Ball.

Lorsque le jeton Luck Ball Coin atteint un certain nombre d'actif en circulation, un Halving est opéré sur le quotient de l'équation régissant le calcul de l'inflation.

## 3.2 Le protocole de Preuve d'Entrée (Mainnet 1.0)

Le protocole de Preuve d'Entrée (PoE) est un nouveau protocole 100% communautaire qui rend la récompense de bloc accessible à tous. Effectuée par l'envoie de LBC, une Entrée octroie à l'utilisateur un poids dans un système d'élection non-discriminatoire, grâce auquel il peut obtenir une récompense de bloc en LBC.

Ce protocole fait parti d'un écosystème comprenant six contrats intelligent interagissant ensemble : Humble Luck Ball, Cycles Manager, Participants Vault, Pool Escrow, Xoshiro256ss, et Proof of Entry.

Le contrat intelligent Humble Luck Ball (HLB) est l'élément principal de cet écosystème. Lorsque des utilisateurs souhaitent effectuer une Entrée, l'algorithme contenu dans le contrat HLB suit un nombre d'étapes. Un **cycle** est réalisé lorsque toutes les étapes sont terminées.

### 3.2.1 Architecture des Cycles du protocole

# ARCHITECTURE DES CYCLES

## Le Contrat Humble Luck Ball

Ce contrat est le coeur de Humble Luck Ball. Il interagit avec les différents services pour créer le protocole de Proof of Entry sur Avalanche.

Répéter

1. Le Contrat Humble Luck Ball initialise un cycle et récupère un hash de la seed générée par la communauté pour vérification avant l'élection. Les participations sont ouvertes.
2. Les utilisateurs participent au Cycle en envoyant le montant désiré en LBC pour être alloué d'un nombre d'entrées. Le nombre de LBC par entrée dépend de la difficulté du protocole.
3. Les participations sont fermées et la Seed générée par la communauté est envoyée au contrat Humble Luck Ball. Elle est vérifiée et initialisée dans la RNG Déterministe.
4. Après le processus d'Election, la Proof of Entry calcule le système d'inflation, ajuste sa difficulté et détermine la prochaine récompense de block.
5. Les utilisateurs peuvent retirer leur gains à tout moment depuis leur Coffre-Fort personnel à l'intérieur du Coffre-Fort de la Proof of Entry. Le Cycle est maintenant complet et un nouveau Cycle démarre.

2 **Chambre Forte des Participants**

Ce service s'occupe des participations des utilisateurs aux cycles de la Proof of Entry

3 **RNG Déterministe**

Ce contrat à RNG déterministe aide à déterminer les utilisateurs récompensés à partir de la Seed générée par la communauté

4 **Contrat de la Proof of Entry**

C'est là où la difficulté du protocole, l'inflation, et les récompenses de block sont calculées et fixées

5 **Coffre-Fort de la Proof of Entry**

Ce Coffre-Fort contient la Humble Pool et tous les soldes et les gains des utilisateurs issus de la PoE

**Contrat Proxy HLB**

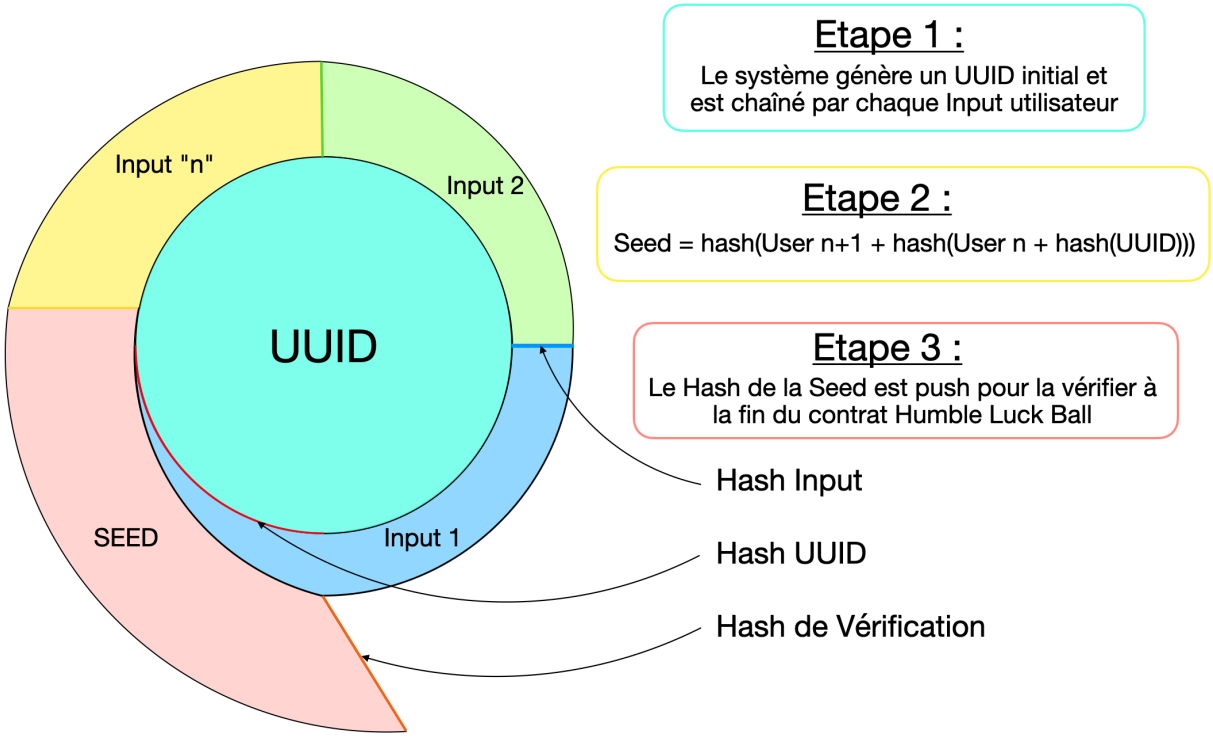
Les utilisateurs interagissent avec le contrat intelligent HLB à travers un contrat proxy transparent.

**Contrat Proxy Coffre-Fort**

Les utilisateurs peuvent retirer leurs gains en LBC grâce à un autre contrat proxy transparent.

Utilisateur

### 3.2.2 Entropie




Génération d'une Seed

**Génération d'une Seed**

Précédant l'initialisation d'un cycle, une valeur de l'algorithme de pRNG, nommée la Seed, est générée par les utilisateurs sur notre dAPP Humble Luck Ball. Les utilisateurs participent à l'entropie.

Le système génère un *Universally Unique IDentifier* initial, ou UUID, qui est chaîné grâce à un Hash par les *Inputs*, ou entrées, effectués par les utilisateurs dans un ordre chronologique.

Un Hash est une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier la donnée initiale.

Lorsque le contrat HLB confirme l'initialisation d'un cycle, le Hash de cette Seed est communiqué au contrat HLB pour être vérifié en fin de cycle.

La participation des utilisateurs à cette génération de Seed est facultative, mais garantie l'entropie de la sélection des récompenses de blocs.

**Vérification de la Seed**

Lors de l'initialisation d'un cycle, seul le Hash de la Seed généré est communiqué au contrat HLB. Ce Hash est donc rendu publique tout en gardant la Seed originelle privée.

Un cycle ne peut être fermé que si la Seed originelle est communiquée au contrat HLB. Le résultat du Hash de cette Seed se doit être similaire au Hash de la Seed communiqué à l'initialisation du cycle. La solution de pRNG peut alors opérer.

La vérification de la Seed permet de confirmer que sa génération a bien été effectuée par la communauté d'utilisateurs, et qu'aucun intervenant externe n'a pu concourir à la sélection des récompenses de blocs par la Solution de pRNG.

### 3.2.3 La Participation Communautaire (PC)

La Participation Communautaire (PC) est un évènement lié au déploiement initial des LBC par l'ICO, terminée le 27 Juin 2021.

Dans le but d'animer une communauté d'utilisateurs, 5% du montant investis par les souscripteurs lors de l'ICO alimentent en LBC la Humble Pool des trois premiers cycles du contrat HLB.

- **2,028,237LBC** ont été déployés aux souscripteurs.
- **101,410LBC** sont déployés pour les PC :
  - ◇ Humble Pool du cycle 1 : 33,803LBC
  - ◇ Humble Pool du cycle 2 : 33,803LBC + LBC recueillis lors du cycle 1 + PoE
  - ◇ Humble Pool du cycle 3 : 33,803LBC + LBC recueillis lors du cycle 2 + PoE

Grâce aux PC, la PoE contenue dans le contrat HLB sera sollicitée et enclenchera l'inflation du LBC.

## 3.3 Plateforme d'échange Humble Market

La plateforme d'échange Humble Market est une dAPP d'échange décentralisée, ou DEX, basé sur le placement d'ordres d'achat ou de vente d'AVAX en LBC.

L'objectif du Humble Market est de permettre la dilution des LBC déployés par la PoE auprès de nouveaux utilisateurs entrants. Ces LBC seront échangés contre de l'AVAX à valeur spéculative déterminé par les échanges effectués entre utilisateurs.

La dAPP Humble Market permet aux utilisateurs ayant connecté leur portefeuille :

- De déposer/retirer de l'AVAX.
- De déposer/retirer du LBC.
- D'accepter un ordre d'achat ou de vente.
- D'effectuer un ordre d'achat ou de vente.
- D'annuler son ordre d'achat ou de vente.

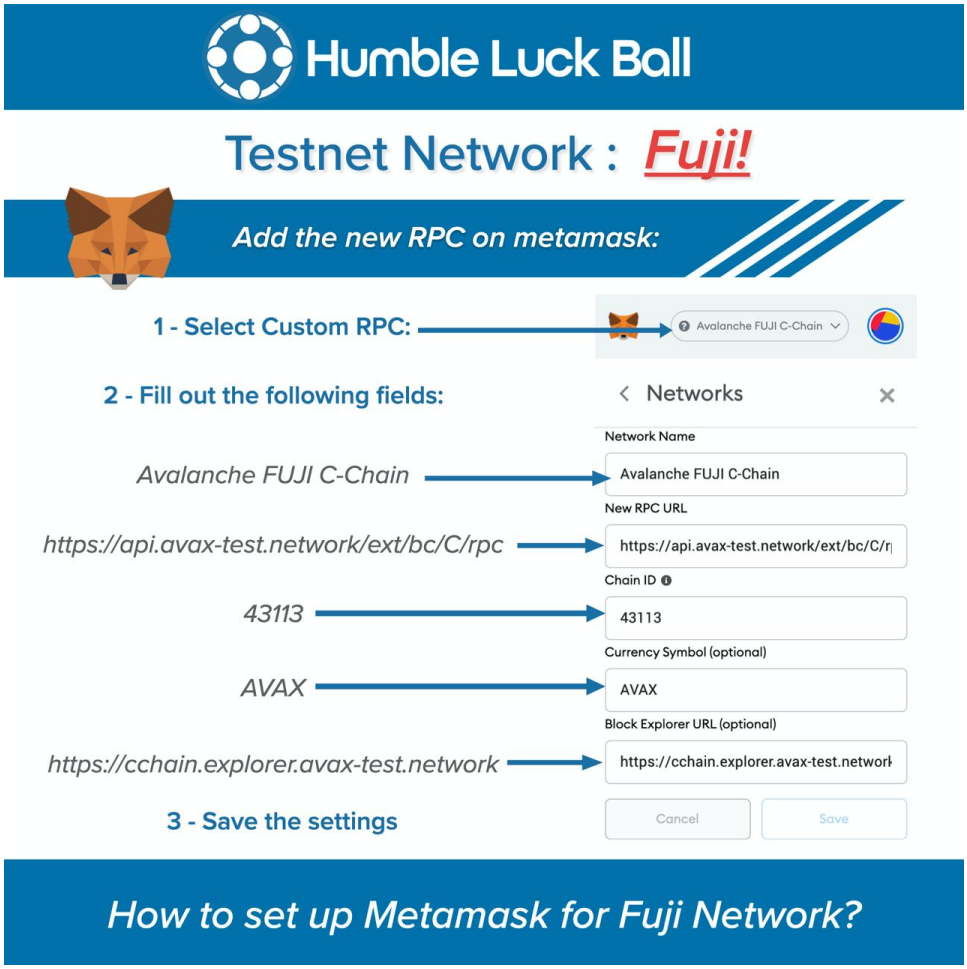
La société Humble Luck Ball fournira un excellent moyen de maintenir un prix équitable du LBC à tout moment, basé sur un stock de disponibilité hebdomadaire grâce à la Preuve d'Entrée. Il est à la fois conçu comme un moyen pour nos utilisateurs d'obtenir le meilleur prix disponible pour le LBC, mais aussi pour limiter les spéculations des participations de dernières minutes sur le contrat intelligent Humble Luck Ball.

Le nombre de LBC déployés grâce à la Preuve d'Entrée pour la plateforme d'échange Humble Market n'est pas encore défini.

# 4 Testnet Humble Luck Ball

| Contrat | Adresse Fuji |
|---|---|
| **Luck Ball Coin** | 0xfAD507f3C6F2FB687a99C5Ae926535410D554a6d |
| **Pool Escrow** | 0xf2e74b777CdE389d99f02DCAA5A844049E4ed618 |
| **Cycles Manager** | 0x9eDa89303FA8D56Ded2F53095A9F8c2FA5d4fef6 |
| **RNG** | 0x34262240cc7c15C739D25e881EEEbd2397ca5a87 |
| **Proof of Entry** | 0x11A1137a5bC5D6716Ac1Da5a25c10640dE033a23 |
| **Participants Vault** | 0x4DDF0C88B4fFd3c78fBbcfC14C4F014aD35336d4 |
| **Humble Luck Ball** | 0xb83a176204e993d78CC305B85F8CEA8750542f79 |

## 4.1 Pré-requis

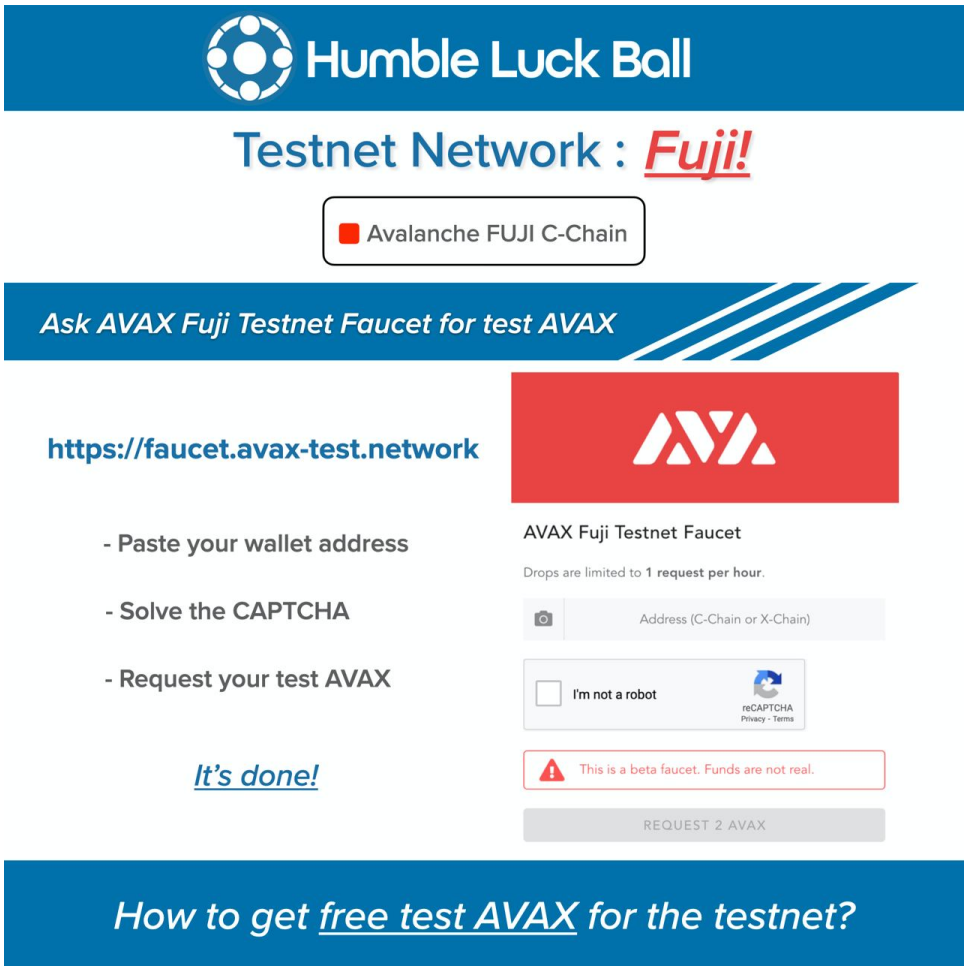


### 4.1.1 Mise en place du portefeuille sur le réseau Avalanche

Certains portefeuilles Avalanche rendent l'accès aux réseaux testnet relativement simple. Par exemple sur le portefeuille MetaMask, voici les étapes à effectuer :

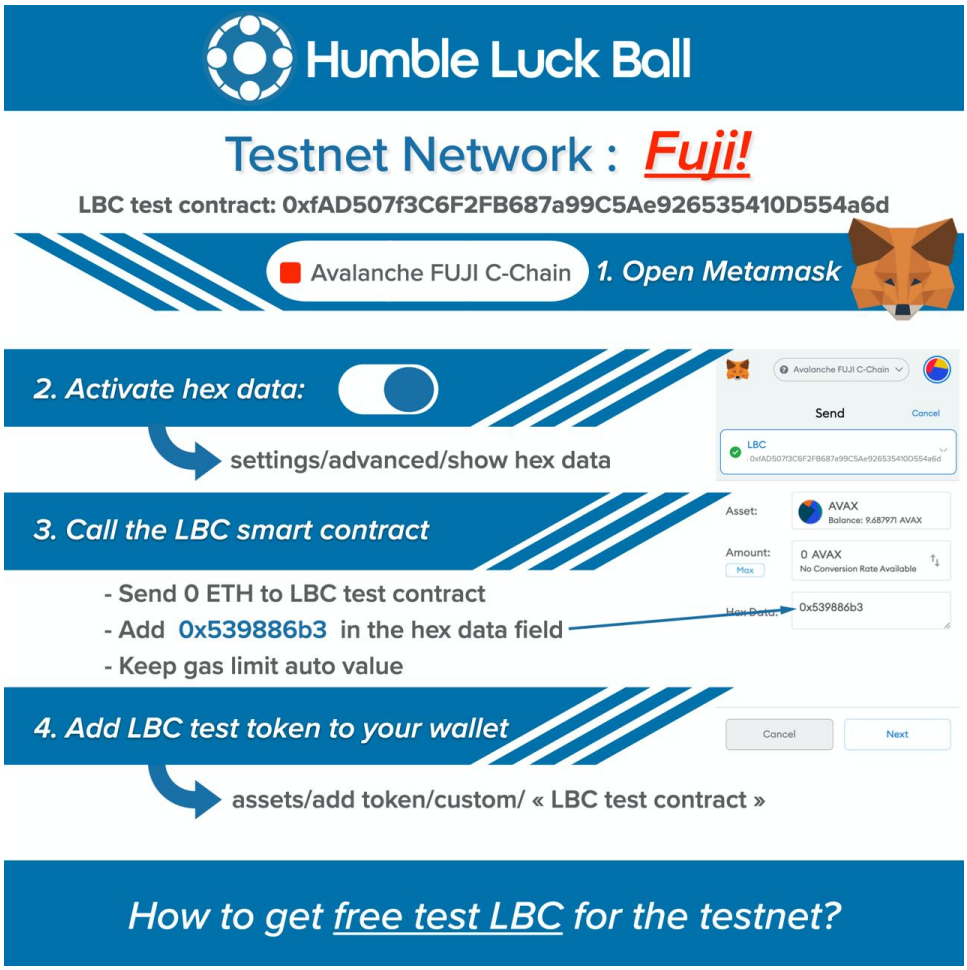
- Cliquer sur "Réseau Principal Ethereum" en haut de l'extension.
- Sélectionner Custom RPC.
- Remplir les cases suivantes :
  - ◇ Network Name : Avalanche FUJI C-Chain
  - ◇ New RPC URL : https://api.avax-test.network/ext/bc/C/rpc
  - ◇ Chain ID : 43113
  - ◇ Currency Symbol : AVAX
  - ◇ Block Explorer URL : https://cchain.explorer.avax-test.network

### 4.1.2 Acquérir de l'AVAX sur Fuji




Le Réseau Fuji propose un Faucet pour lequel vous devez renseigner votre adresse de portefeuille et cliquer sur le bouton.

### 4.1.3 Acquérir des jetons Luck Ball Coin (LBC) sur Fuji




Le contrat intelligent Luck Ball Coin (LBC) qui est déployé sur le réseau de Testnet Fuji fonctionne également comme un Faucet. L'envoi de 0 AVAX avec les Données Hexadécimales (Hex Data) suivantes au contrat vous accordera 100 LBC. Cela ne fonctionne qu'une seule fois par adresse :

- **Contrat LBC :** 0xfAD507f3C6F2FB687a99C5Ae926535410D554a6d
  - ◇ **Hex Data (Ask Faucet) :** 0x539886b3

### 4.1.4 Approuver l'utilisation de Luck Ball Coin (LBC) pour l'écosystème Humble Luck Ball

L'écosystème Humble Luck Ball est composé de plusieurs contrats intelligents qui interagissent les uns avec les autres. Pour que l'écosystème reçoive, stocke et utilise vos jetons Luck Ball Coin (LBC), une approbation est requise. L'envoi de 0 AVAX avec les Données Hexadécimales (Hex Data) suivantes au contrat autorisera l'écosystème Humble Luck Ball à accepter vos participations :

- **Contrat LBC :** 0xfAD507f3C6F2FB687a99C5Ae926535410D554a6d
  - ◇ **Hex Data (Approve) :** 0x095ea7b30000000000000000000000000f2e74b777cde389d99f02dcaa5a844049e4ed6180000000000000000000000000000000000000000000000000d3c21bcecceda1000000

## 4.2 Interaction avec les Contrats Intelligents

Un utilisateur peut participer au contrat Humble Luck Ball de deux façons : depuis son portefeuille, ou depuis son coffre-fort. **Une seule participation unique est possible par utilisateur et par cycle.**

### 4.2.1 Participer au Humble Luck Ball

Un utilisateur peut interagir avec la fonction *Participer* en envoyant des jetons Luck Ball Coin (LBC) dans le contrat intelligent Humble Luck Ball (HLB). Un utilisateur peut trouver ci-dessous l'adresse du contrat intelligent Humble Luck Ball, et vérifier les Données Hexadécimales (Hex Data) pour participer :

- **Contrat HLB :** 0xb83a176204e993d78CC305B85F8CEA8750542f79
  - ◇ **Hex Data Participate :** Page 18

Cette fonction attribue un nombre d'entrées en fonction de la participation en LBC d'un Utilisateur. Si la solution RNG sélectionne l'Utilisateur, il se verra attribué d'une Récompense de Bloc directement dans son **Coffre-Fort**.

### 4.2.2 Participer depuis le Coffre-Fort

Un Utilisateur recevra les LBC des Récompenses de Bloc directement dans son Coffre-Fort si ce dernier a été sélectionné grâce à la solution RNG. Un Utilisateur peut alors décider de participer à nouveau au Humble Luck Ball avec des LBC contenus dans son Coffre-Fort, de retirer une quantité de LBC de son Coffre-Fort ou de retirer tous les jetons LBC contenus dans le Coffre-Fort.

- **Contrat HLB :** 0xb83a176204e993d78CC305B85F8CEA8750542f79
  - ◇ **Hex Data Pool Escrow :** Page 19
- **Contrat Pool Escrow :** 0xf2e74b777CdE389d99f02DCAA5A844049E4ed618
  - ◇ **Hex Data Withdraw :** Page 20
  - ◇ **Hex Data (Withdraw All) :** 0x853828b6

### 4.2.3 Ajouter une entrée à l'Entropie

*Disponible prochainement*

## 4.3 Récompenses pour les Beta Testers

### 4.3.1 Eligibilité des récompenses

Une incitation est proposée aux bêta-testeurs afin que les contrats intelligents Humble Luck Ball et son protocole de preuve d'entrée soient utilisés et adoptés.

Voici les quatre exigences pour être éligible aux récompenses des bêta-testeurs :

- Participer au Humble Luck Ball
- Participer au Humble Luck Ball depuis le Coffre-Fort
- Ajouter une entrée à l'Entropie
- Posséder au moins 500LBCs

Un utilisateur doit avoir acquis au moins 500 LBC sur la blockchain principale Avalanche pour être éligible à la récompense des bêta-testeurs avant le déploiement du protocole de Proof of Entry sur le réseau principal. Cela inclut et est limité à la possession de jetons Luck Ball Coin suite à la migration des actifs présents sur la blockchain Ethereum ou via l'achat d'actifs depuis la Humble Decentralized Offering (HDO).

### 4.3.2 Récompense en Luck Ball Coin (LBC)

Suite au vote de la communauté d'utilisateurs le 2 Août 2021, où 84% des votants furent favorables à une incitation financière à la participation au Testnet du protocole de Preuve d'Entrée, 150.000 LBCs ont été minés en vue d'une distribution de 500 LBCs aux 300 premiers Beta Testers ayant rempli les quatre critères d'éligibilité décrits précédemment.

Cette récompense pourra être récupérée depuis une dAPP spéciale et sera disponible peu après le lancement du Mainnet 1.0, marquant le déploiement du protocole de Preuve d'Entrée.

### 4.3.3 Récompense en Non-Fungible Token (NFT)

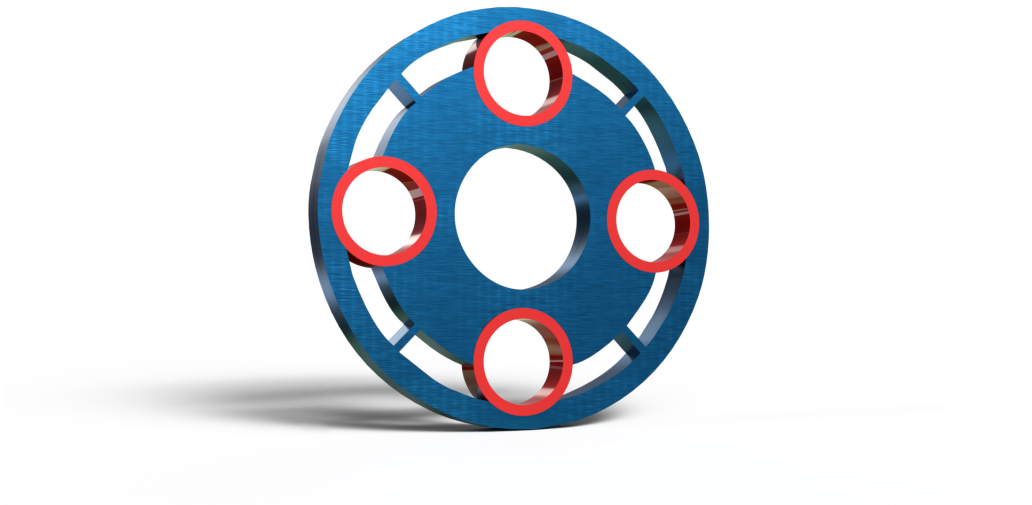
Pouvant être considéré comme réserve de valeur de par sa rareté, ce marqueur d'une époque s'inscrit définitivement dans la blockchain. L'essor et l'adoption des NFTs sont indéniablement liés à un sentiment fort : le symbole d'appartenance à une communauté pour celui qui le possède.

C'est en ce sens que les tout premiers investisseurs, ainsi que les Beta Testers des contrats HLB seront récompensés par des NFTs uniques et nominatifs liés à leur expérience exclusive et personnelle de l'aventure HLB.

Les moments choisis sont:

- la participation à l'ICO
- la participation au Testnet Rinkeby
- la participation au Testnet Fuji
- la participation à la Humble Decentralized Offering

Ces NFTs seront distribués individuellement à chaque personne faisant la preuve de sa participation de par l'adresse utilisée à ces étapes clés de l'aventure HLB une fois le protocole de Preuve d'Entrée déployé au titre du Mainnet 1.0.



NFT Luck Ball Coin du Testnet Fuji

## 4.4 Hex Data Participer

Table 1: Hex Data Participate

| | |
|---|---|
| 10 LBC | 845c9306000000000000000000000000000000000000000000000008ac7230489e80000 |
| 20 LBC | 845c93060000000000000000000000000000000000000000000001158e460913d00000 |
| 30 LBC | 845c930600000000000000000000000000000000000000000000001a055690d9db80000 |
| 40 LBC | 845c9306000000000000000000000000000000000000000000022b1c8c1227a00000 |
| 50 LBC | 845c930600000000000000000000000000000000000000000002b5e3af16b1880000 |
| 60 LBC | 845c9306000000000000000000000000000000000000000000340aad21b3b700000 |
| 70 LBC | 845c930600000000000000000000000000000000000000000003cb71f51fc5580000 |
| 80 LBC | 845c9306000000000000000000000000000000000000000004563918244f400000 |
| 90 LBC | 845c930600000000000000000000000000000000000000000004e1003b28d9280000 |
| 100 LBC | 845c9306000000000000000000000000000000000000000056bc75e2d63100000 |
| 200 LBC | 845c930600000000000000000000000000000000000000000ad78ebc5ac6200000 |
| 300 LBC | 845c9306000000000000000000000000000000000000000001043561a8829300000 |
| 400 LBC | 845c930600000000000000000000000000000000000000015af1d78b58c400000 |
| 500 LBC | 845c9306000000000000000000000000000000000000001b1ae4d6e2ef500000 |
| 600 LBC | 845c930600000000000000000000000000000000000002086ac351052600000 |
| 700 LBC | 845c9306000000000000000000000000000000000000025f273933db5700000 |
| 800 LBC | 845c930600000000000000000000000000000000000002b5e3af16b18800000 |
| 900 LBC | 845c9306000000000000000000000000000000000000030ca024f987b900000 |
| 1000 LBC | 845c930600000000000000000000000000000000000003635c9adc5dea00000 |
| 1100 LBC | 845c9306000000000000000000000000000000000003ba1910bf341b00000 |
| 1200 LBC | 845c930600000000000000000000000000000000000410d586a20a4c00000 |
| 1300 LBC | 845c9306000000000000000000000000000000000046791fc84e07d00000 |
| 1400 LBC | 845c930600000000000000000000000000000000004be4e7267b6ae00000 |
| 1500 LBC | 845c9306000000000000000000000000000000000005150ae84a8cdf00000 |
| 1600 LBC | 845c930600000000000000000000000000000000056bc75e2d631000000 |
| 1700 LBC | 845c9306000000000000000000000000000000000005c283d410394100000 |
| 1800 LBC | 845c930600000000000000000000000000000000006194049f30f7200000 |
| 1900 LBC | 845c9306000000000000000000000000000000000066ffcbfd5e5a300000 |
| 2000 LBC | 845c930600000000000000000000000000000000006c6b935b8bbd400000 |
| 2100 LBC | 845c9306000000000000000000000000000000000071d75ab9b920500000 |

### 4.5 Hex Data Pool Escrow

Table 2: Hex Data Participate From Vault

| | |
|---|---|
| 10 LBC | 21340e5d00000000000000000000000000000000000000000000008ac7230489e80000 |
| 20 LBC | 21340e5d00000000000000000000000000000000000000000000001158e460913d00000 |
| 30 LBC | 21340e5d00000000000000000000000000000000000000000000001a055690d9db80000 |
| 40 LBC | 21340e5d00000000000000000000000000000000000000000000022b1c8c1227a00000 |
| 50 LBC | 21340e5d00000000000000000000000000000000000000000000002b5e3af16b1880000 |
| 60 LBC | 21340e5d00000000000000000000000000000000000000000000340aad21b3b700000 |
| 70 LBC | 21340e5d00000000000000000000000000000000000000000003cb71f51fc5580000 |
| 80 LBC | 21340e5d00000000000000000000000000000000000000000004563918244f400000 |
| 90 LBC | 21340e5d00000000000000000000000000000000000000000004e1003b28d9280000 |
| 100 LBC | 21340e5d00000000000000000000000000000000000000000056bc75e2d63100000 |
| 200 LBC | 21340e5d00000000000000000000000000000000000000000ad78ebc5ac6200000 |
| 300 LBC | 21340e5d00000000000000000000000000000000000000001043561a8829300000 |
| 400 LBC | 21340e5d00000000000000000000000000000000000000015af1d78b58c400000 |
| 500 LBC | 21340e5d00000000000000000000000000000000000001b1ae4d6e2ef500000 |
| 600 LBC | 21340e5d00000000000000000000000000000000000002086ac351052600000 |
| 700 LBC | 21340e5d00000000000000000000000000000000000025f273933db5700000 |
| 800 LBC | 21340e5d00000000000000000000000000000000002b5e3af16b18800000 |
| 900 LBC | 21340e5d00000000000000000000000000000000030ca024f987b900000 |
| 1000 LBC | 21340e5d00000000000000000000000000000000003635c9adc5dea00000 |
| 1100 LBC | 21340e5d00000000000000000000000000000003ba1910bf341b00000 |
| 1200 LBC | 21340e5d00000000000000000000000000000000410d586a20a4c00000 |
| 1300 LBC | 21340e5d00000000000000000000000000000046791fc84e07d00000 |
| 1400 LBC | 21340e5d00000000000000000000000000000004be4e7267b6ae00000 |
| 1500 LBC | 21340e5d00000000000000000000000000000005150ae84a8cdf00000 |
| 1600 LBC | 21340e5d00000000000000000000000000000056bc75e2d631000000 |
| 1700 LBC | 21340e5d00000000000000000000000000000005c283d410394100000 |
| 1800 LBC | 21340e5d00000000000000000000000000000006194049f30f7200000 |
| 1900 LBC | 21340e5d00000000000000000000000000000066ffcbfd5e5a300000 |
| 2000 LBC | 21340e5d00000000000000000000000000000006c6b935b8bbd400000 |
| 2100 LBC | 21340e5d00000000000000000000000000000071d75ab9b920500000 |

## 4.6 Hex Data Withdraw

Table 3: Hex Data Withdraw

| | |
|---|---|
| 1 LBC | 2e1a7d4d0000000000000000000000000000000000000000000000000de0b6b3a7640000 |
| 2 LBC | 2e1a7d4d00000000000000000000000000000000000000000000000001bc16d674ec80000 |
| 3 LBC | 2e1a7d4d000000000000000000000000000000000000000000000000029a2241af62c0000 |
| 4 LBC | 2e1a7d4d0000000000000000000000000000000000000000000000003782dace9d900000 |
| 5 LBC | 2e1a7d4d00000000000000000000000000000000000000000000004563918244f40000 |
| 6 LBC | 2e1a7d4d000000000000000000000000000000000000000000000053444835ec580000 |
| 7 LBC | 2e1a7d4d0000000000000000000000000000000000000000000006124fee993bc0000 |
| 8 LBC | 2e1a7d4d00000000000000000000000000000000000000000000006f05b59d3b200000 |
| 9 LBC | 2e1a7d4d000000000000000000000000000000000000000000007ce66c50e2840000 |
| 10 LBC | 2e1a7d4d0000000000000000000000000000000000000000000008ac7230489e80000 |
| 20 LBC | 2e1a7d4d00000000000000000000000000000000000000000001158e460913d00000 |
| 30 LBC | 2e1a7d4d000000000000000000000000000000000000000000001a055690d9db80000 |
| 40 LBC | 2e1a7d4d00000000000000000000000000000000000000000022b1c8c1227a00000 |
| 50 LBC | 2e1a7d4d000000000000000000000000000000000000000002b5e3af16b1880000 |
| 60 LBC | 2e1a7d4d0000000000000000000000000000000000000000340aad21b3b700000 |
| 70 LBC | 2e1a7d4d00000000000000000000000000000000000000003cb71f51fc5580000 |
| 80 LBC | 2e1a7d4d0000000000000000000000000000000000000004563918244f400000 |
| 90 LBC | 2e1a7d4d000000000000000000000000000000000000000004e1003b28d9280000 |
| 100 LBC | 2e1a7d4d00000000000000000000000000000000000000056bc75e2d63100000 |
| 200 LBC | 2e1a7d4d0000000000000000000000000000000000000000ad78ebc5ac6200000 |
| 300 LBC | 2e1a7d4d000000000000000000000000000000000000001043561a8829300000 |
| 400 LBC | 2e1a7d4d00000000000000000000000000000000000000015af1d78b58c400000 |
| 500 LBC | 2e1a7d4d0000000000000000000000000000000000000001b1ae4d6e2ef500000 |
| 600 LBC | 2e1a7d4d00000000000000000000000000000000000000002086ac351052600000 |
| 700 LBC | 2e1a7d4d0000000000000000000000000000000000000025f273933db5700000 |
| 800 LBC | 2e1a7d4d000000000000000000000000000000000000002b5e3af16b18800000 |
| 900 LBC | 2e1a7d4d0000000000000000000000000000000000000030ca024f987b900000 |
| 1000 LBC | 2e1a7d4d00000000000000000000000000000000000003635c9adc5dea00000 |

# 5 Caractéristiques de l'Initial Decentralized Offering (IDO)

## 5.1 Pourquoi une IDO ?

La société Humble Luck Ball continue son déploiement de jetons Luck Ball Coin (LBC) à travers une Initial Decentralized Offering dont les caractéristiques sont en cohérence avec les valeurs du protocole de Proof of Entry.

En effet, cela assure le succès du lancement du protocole de Proof of Entry car une IDO permet :

- D'augmenter le nombre de jeton LBC en circulation.
- De garantir une valeur initiale du jeton LBC grâce à la présence d'une liquidité.
- De rendre accessible l'acquisition du jeton LBC auprès d'utilisateurs entrants.

Cela permet aussi de financer les travaux de Recherche & Développement de la société Humble Luck Ball, à travers des investissements pour :

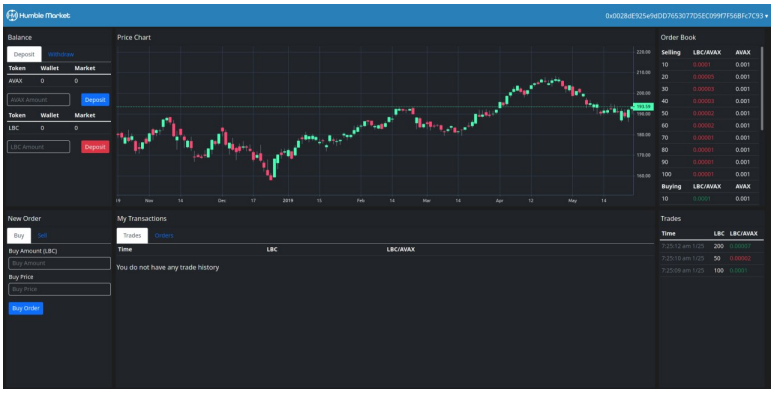
- Recruter des cadres et employés qualifiés.
- Opérer des noeuds validateurs Avalanche pour le sous-réseau Humble Luck Ball.
- Communiquer activement à l'international et rendre le projet accessible.

## 5.2 Présentation de la Humble Decentralized Offering (HDO)

La société Humble Luck Ball est fière de déployer son offre de jeton Luck Ball Coin depuis sa plateforme d'échange décentralisée native, le Humble Market. Cette offre, appelée la Humble Decentralized Offering, permet d'acquérir des jetons Luck Ball Coin (LBC) en échange d'AVAX. La dAPP est hébergée sur https://ido.humbleluckball.com.

Le nombre de jetons disponibles à travers cette offre est de 2,515,000 LBCs, par stocks de 20,120 LBCs lissés sur 125 paliers valorisant le jeton d'une équivalence en AVAX de $0,01 par palier comme présenté sur les pages suivantes.

D'un fonctionnement intuitif, ce DEX permet à la communauté de maîtriser le futur médium d'achat et de vente du LBC.




Humble Decentralized Offering

| Cap | Prix en $ | Stock LBC | Stock en $ |
|---|---|---|---|
| **1** | 0.26 | 20120 | 5231.2 |
| **2** | 0.27 | 20120 | 5432.4 |
| **3** | 0.28 | 20120 | 5633.6 |
| **4** | 0.29 | 20120 | 5834.8 |
| **5** | 0.3 | 20120 | 6036 |
| **6** | 0.31 | 20120 | 6237.2 |
| **7** | 0.32 | 20120 | 6438.4 |
| **8** | 0.33 | 20120 | 6639.6 |
| **9** | 0.34 | 20120 | 6840.8 |
| **10** | 0.35 | 20120 | 7042 |
| **11** | 0.36 | 20120 | 7243.2 |
| **12** | 0.37 | 20120 | 7444.4 |
| **13** | 0.38 | 20120 | 7645.6 |
| **14** | 0.39 | 20120 | 7846.8 |
| **15** | 0.4 | 20120 | 8048 |
| **16** | 0.41 | 20120 | 8249.2 |
| **17** | 0.42 | 20120 | 8450.4 |
| **18** | 0.43 | 20120 | 8651.6 |
| **19** | 0.44 | 20120 | 8852.8 |
| **20** | 0.45 | 20120 | 9054 |
| **21** | 0.46 | 20120 | 9255.2 |
| **22** | 0.47 | 20120 | 9456.4 |
| **23** | 0.48 | 20120 | 9657.6 |
| **24** | 0.49 | 20120 | 9858.8 |
| **25** | 0.5 | 20120 | 10060 |
| **26** | 0.51 | 20120 | 10261.2 |
| **27** | 0.52 | 20120 | 10462.4 |
| **28** | 0.53 | 20120 | 10663.6 |
| **29** | 0.54 | 20120 | 10864.8 |
| **30** | 0.55 | 20120 | 11066 |
| **31** | 0.56 | 20120 | 11267.2 |
| **32** | 0.57 | 20120 | 11468.4 |

| Cap | Prix en $ | Stock LBC | Stock en $ |
|---|---|---|---|
| **33** | 0.58 | 20120 | 11669.6 |
| **34** | 0.59 | 20120 | 11870.8 |
| **35** | 0.6 | 20120 | 12072 |
| **36** | 0.61 | 20120 | 12273.2 |
| **37** | 0.62 | 20120 | 12474.4 |
| **38** | 0.63 | 20120 | 12675.6 |
| **39** | 0.64 | 20120 | 12876.8 |
| **40** | 0.65 | 20120 | 13078 |
| **41** | 0.66 | 20120 | 13279.2 |
| **42** | 0.67 | 20120 | 13480.4 |
| **43** | 0.68 | 20120 | 13681.6 |
| **44** | 0.69 | 20120 | 13882.8 |
| **45** | 0.7 | 20120 | 14084 |
| **46** | 0.71 | 20120 | 14285.2 |
| **47** | 0.72 | 20120 | 14486.4 |
| **48** | 0.73 | 20120 | 14687.6 |
| **49** | 0.74 | 20120 | 14888.8 |
| **50** | 0.75 | 20120 | 15090 |
| **51** | 0.76 | 20120 | 15291.2 |
| **52** | 0.77 | 20120 | 15492.4 |
| **53** | 0.78 | 20120 | 15693.6 |
| **54** | 0.79 | 20120 | 15894.8 |
| **55** | 0.8 | 20120 | 16096 |
| **56** | 0.81 | 20120 | 16297.2 |
| **57** | 0.82 | 20120 | 16498.4 |
| **58** | 0.83 | 20120 | 16699.6 |
| **59** | 0.84 | 20120 | 16900.8 |
| **60** | 0.85 | 20120 | 17102 |
| **61** | 0.86 | 20120 | 17303.2 |
| **62** | 0.87 | 20120 | 17504.4 |
| **63** | 0.88 | 20120 | 17705.6 |
| **64** | 0.89 | 20120 | 17906.8 |

| Cap | Prix en $ | Stock LBC | Stock en $ |
|---|---|---|---|
| **65** | 0.9 | 20120 | 18108 |
| **66** | 0.91 | 20120 | 18309.2 |
| **67** | 0.92 | 20120 | 18510.4 |
| **68** | 0.93 | 20120 | 18711.6 |
| **69** | 0.94 | 20120 | 18912.8 |
| **70** | 0.95 | 20120 | 19114 |
| **71** | 0.96 | 20120 | 19315.2 |
| **72** | 0.97 | 20120 | 19516.4 |
| **73** | 0.98 | 20120 | 19717.6 |
| **74** | 0.99 | 20120 | 19918.8 |
| **Soft Cap** | | | |
| **75** | 1 | 20120 | 20120 |
| **76** | 1.01 | 20120 | 20321.2 |
| **77** | 1.02 | 20120 | 20522.4 |
| **78** | 1.03 | 20120 | 20723.6 |
| **79** | 1.04 | 20120 | 20924.8 |
| **80** | 1.05 | 20120 | 21126 |
| **81** | 1.06 | 20120 | 21327.2 |
| **82** | 1.07 | 20120 | 21528.4 |
| **83** | 1.08 | 20120 | 21729.6 |
| **84** | 1.09 | 20120 | 21930.8 |
| **85** | 1.1 | 20120 | 22132 |
| **86** | 1.11 | 20120 | 22333.2 |
| **87** | 1.12 | 20120 | 22534.4 |
| **88** | 1.13 | 20120 | 22735.6 |
| **89** | 1.14 | 20120 | 22936.8 |
| **90** | 1.15 | 20120 | 23138 |
| **91** | 1.16 | 20120 | 23339.2 |
| **92** | 1.17 | 20120 | 23540.4 |
| **93** | 1.18 | 20120 | 23741.6 |
| **94** | 1.19 | 20120 | 23942.8 |
| **95** | 1.2 | 20120 | 24144 |

| Cap | Prix en $ | Stock LBC | Stock en $ |
|---|---|---|---|
| **96** | 1.21 | 20120 | 24345.2 |
| **97** | 1.22 | 20120 | 24546.4 |
| **98** | 1.23 | 20120 | 24747.6 |
| **99** | 1.24 | 20120 | 24948.8 |
| **Mid Cap** | | | |
| **100** | 1.25 | 20120 | 25150 |
| **101** | 1.26 | 20120 | 25351.2 |
| **102** | 1.27 | 20120 | 25552.4 |
| **103** | 1.28 | 20120 | 25753.6 |
| **104** | 1.29 | 20120 | 25954.8 |
| **105** | 1.3 | 20120 | 26156 |
| **106** | 1.31 | 20120 | 26357.2 |
| **107** | 1.32 | 20120 | 26558.4 |
| **108** | 1.33 | 20120 | 26759.6 |
| **109** | 1.34 | 20120 | 26960.8 |
| **110** | 1.35 | 20120 | 27162 |
| **111** | 1.36 | 20120 | 27363.2 |
| **112** | 1.37 | 20120 | 27564.4 |
| **113** | 1.38 | 20120 | 27765.6 |
| **114** | 1.39 | 20120 | 27966.8 |
| **115** | 1.4 | 20120 | 28168 |
| **116** | 1.41 | 20120 | 28369.2 |
| **117** | 1.42 | 20120 | 28570.4 |
| **118** | 1.43 | 20120 | 28771.6 |
| **119** | 1.44 | 20120 | 28972.8 |
| **120** | 1.45 | 20120 | 29174 |
| **121** | 1.46 | 20120 | 29375.2 |
| **122** | 1.47 | 20120 | 29576.4 |
| **123** | 1.48 | 20120 | 29777.6 |
| **124** | 1.49 | 20120 | 29978.8 |
| **125** | 1.5 | 20120 | 30180 |
| **Hard Cap** | | | |