
Humble Luck Ball Whitepaper



PROOF OF ENTRY (POE) PROTOCOL

TONY VERSCHUEREN AND JULIAN CAILLE

Founder and co-Founder of the Humble Luck Ball

6th of November 2020

Updated the 20th of February 2022

V.2.0.0

Table of Contents

| | |
|--|-----------|
| Blockchain Glossary | ii |
| Team and History | iv |
| 1 Summary | 1 |
| 1.1 What is Humble Luck Ball ? | 1 |
| 1.2 What is the roadmap ? | 1 |
| 1.3 Luck Ball Coin (LBC) Utility | 1 |
| 2 The Humble Luck Ball (HLB) Project | 2 |
| 2.1 General description | 2 |
| 2.2 Objective of the HLB project | 2 |
| 2.3 State of the art | 3 |
| 2.4 HLB Project Roadmap | 5 |
| 2.5 Uncertainties, technological locks and problems to be solved | 6 |
| 2.6 Applied Methodologies | 7 |
| 2.6.1 General approach | 7 |
| 2.6.2 Work completed | 7 |
| 3 Products and services of the Humble Luck Ball (HLB) project | 9 |
| 3.1 The Luck Ball Coin (LBC) token | 9 |
| 3.1.1 Token's nature | 9 |
| 3.1.2 Inflation and Halving | 9 |
| 3.2 Proof of Entry Protocol (Mainnet 1.0) | 9 |
| 3.2.1 Cycles Architecture | 9 |
| 3.2.2 Entropy | 11 |
| 3.2.3 Community Participation (CP) | 12 |
| 3.3 Humble Market exchange platform | 12 |
| 4 Humble Luck Ball Testnet | 13 |
| 4.1 Requirements | 13 |
| 4.1.1 Setting up your wallet on the Fuji network | 14 |
| 4.1.2 Acquire AVAX on Fuji | 14 |
| 4.1.3 Acquire Luck Ball Coin (LBC) on Fuji | 15 |
| 4.1.4 Approve the Humble Luck Ball to use your Luck Ball Coin (LBC) | 15 |
| 4.2 Smart Contract Interaction | 16 |
| 4.2.1 Participate to the Humble Luck Ball | 16 |
| 4.2.2 Participate through the Vault | 16 |
| 4.2.3 Add an entry to the Entropy | 16 |
| 4.3 Beta Testers Rewards | 16 |
| 4.3.1 Rewards eligibility | 16 |
| 4.3.2 Luck Ball Coin (LBC) Rewards | 17 |
| 4.3.3 NFT Reward | 17 |
| 4.4 Hex Data Participate | 18 |
| 4.5 Hex Data Pool Escrow | 19 |
| 4.6 Hex Data Withdraw | 20 |
| 5 Characteristics of the Initial Decentralized Offering (IDO) | 21 |
| 5.1 Why an IDO ? | 21 |
| 5.2 Humble Decentralized Offering (HDO) presentation | 21 |

Blockchain Glossary

| | |
|-----------------------------|---|
| Decentralized Application | Application that operates on a decentralized network, as opposed to traditional applications that depend on centralized servers. Its support is one or more smart contracts deployed on a blockchain. The front-end part (user interface), can be developed as on classic applications. In the ethereum blockchain ecosystem, decentralized applications are called dapps. |
| Avalanche | Decentralized platform under the Proof of Stake consensus and the "Snow" protocol. Avalanche is the fastest smart contracts platform in the blockchain industry, as measured by time-to-finality. |
| Bitcoin | Property transfer and verification system based on a peer-to-peer network without any central authority, designed in 2009 by a developer using the pseudonym Satoshi Nakamoto. Its unit of account is bitcoin electronic money. |
| Blockchain | Technologies allowing the storage and exchange of value on the internet without a centralized intermediary (definition of Blockchain France). They are the technological engine of cryptocurrencies, the Decentralized Web and its corollary, decentralized finance. By extension, a blockchain (literally a "chain of blocks") designates a secure and decentralized database, replicated on a very large number of nodes, and containing a set of transactions whose validity each can be verified. A blockchain can therefore be likened to a transparent, pseudonymous and tamper-proof ledger. |
| Consensus | Any cryptocurrency works thanks to a protocol, which is a set of communication rules allowing an agreement to be reached in a decentralized way. The rules that make up this protocol are called consensus rules. In the case of a blockchain, they are used to define the validity of transactions and blocks. |
| Cryptocurrency | Electronic money, exchangeable peer-to-peer (i.e. without an intermediary), based on cryptographic principles and economic incentive mechanisms for the validation of transactions and the generation of the money itself. |
| Ethereum | Decentralized platform, based on the eponymous blockchain, which aims for the advent of a decentralized web. The ethereum blockchain works with the ether cryptocurrency. Unlike the bitcoin blockchain, which focuses on the monetary aspect, the ethereum blockchain is intended to accommodate a wide variety of programs, called dapps, which work with smart contracts. We talk about the ethereum ecosystem to designate all the players who work on this platform. |
| Gossip Algorithm | A gossip protocol or algorithm designates a distributed algorithm in a peer-to-peer computer network to propagate information to all network agents. |
| ICO (Initial Coin Offering) | Fundraising method operating through the issuance of digital assets, called tokens, exchangeable for cryptocurrencies during the start-up phase of a project. |
| Ledger | A distributed ledger (also called shared ledger) is a register simultaneously recorded and synchronized on a network of computers, which evolves by the addition of new information previously validated by the entire network and intended never to be modified or deleted. |
| Mining | Use of computing power to process transactions, secure the network, and keep all system users in sync. |

| | |
|-----------------------|---|
| Miner | People (individuals or companies) who connect one or more machines to the network equipped to perform mining. Each miner is remunerated in proportion to the computing power he brings to the network. |
| Node | Computer connected to the blockchain network and using a program relaying transactions. The nodes maintain a copy of the blockchain ledger and are distributed all over the world. |
| Proof of Stake (PoS) | Method for achieving distributed consensus in a blockchain network. Unlike proof of work, proof of stake does not require users to use their computing power, but to prove ownership of a certain amount of cryptocurrency. Ethereum aims to switch to proof of stake in the medium term. |
| Proof of Work (PoW) | Method used to achieve distributed consensus in a large number of public blockchains, bitcoin in the lead. Concretely, it is the cryptographic processing allowing the validation of the blocks of transactions. Performing this processing requires computing time: in general, a single computer on the network achieves this in about ten minutes. The difficulty is regularly adapted to maintain this interval. |
| Equidistributive pRNG | A pseudo-random number generator (pRNG) is an algorithm that generates a sequence of numbers with certain random properties. For example, numbers are assumed to be sufficiently independent of each other, and it is potentially difficult to spot groups of numbers that follow a certain rule (group behaviors). |
| Scalability | Scaling up. This is the biggest challenge for blockchains today. One of the major question is: how to increase the number of transactions carried out per second, without compromising decentralization and security? Technical solutions are being designed or implemented on major protocols: the off-chain state channel solution (Lightning Network on Bitcoin, Raiden Network on Ethereum), sharding, Plasma for smart contracts on Ethereum, etc. |
| Smart Contract | Autonomous program which, once started, automatically executes conditions written upstream in the blockchain, without requiring human intervention. It works like any conditional statement of type "if - then" (if such condition is verified, then such consequence is executed). To trigger its execution, a smart contract connects to a database deemed reliable, via an oracle (a service that makes the link between the smart contract and the real world). |
| Soft Fork | A soft fork is a backward compatible modification of the consensus rules, which does not cause separation if applied by a majority of the validating power. The soft fork is essentially restrictive (adding new rules). |
| Hard Fork | A hard fork is a fork in the blockchain caused by a change in consensus rules. By extension, the term is also used to refer to any non-backwards compatible change to the protocol that may cause permanent duplication of the chain. |
| Token | Digital asset personalized by its author, issued and exchangeable on a blockchain, and having the characteristics of a cryptocurrency: tamper-proof, uniqueness, recording of exchanges in an immutable register, security of exchanges, etc. In particular, a token is transferable (and not duplicable) between two parties on the internet, without requiring the agreement of a third party. |

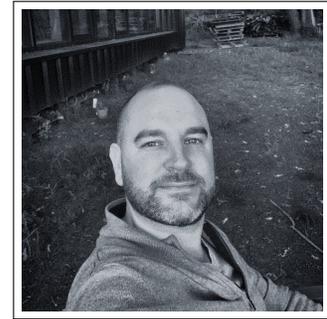
Team



Tony VERSCHUEREN
Founder & CEO, CFO



Julian CAILLE
Co-Founder & CTO



Camille SERGENT
Marketing & Communication

History

| |
|---|
| <u>2018, 2019</u> |
| Emergence of the idea Research and Development of first prototypes |
| <u>2020</u> |
| Creation of the Humble Luck Ball Company Website Humble Luck Ball available Release of Whitepaper V1.0.0 |
| <u>2021</u> |
| ICO from the 27 th of February to the 27 th of June AIBC Summit Finalist at Dubaï in May French articles CoinTribune , and Journal Du Coin Migration from Ethereum blockchain →Avalanche |
| <u>2022</u> |
| Release of Whitepaper V2.0.0 <i>Humble Market DEX Deployment</i> <i>Mainnet 1.0, Proof of Entry Protocol</i> |

1 Summary

1.1 What is Humble Luck Ball ?

The Humble Luck Ball project is developing a new blockchain consensus called Proof of Entry, with the goal of creating a blockchain that is easy and accessible to everyone without any mining or staking processes. This consensus is 100% community based and the block reward election process is non-discriminatory.

The current findings demonstrate that Proof of Work and Proof of Stake consensus constrain and/or prevent network users from obtaining block rewards easily, although it is the main cause of blockchain economic system's inflation. Indeed, it is necessary to acquire substantial mining equipment, or to stake a lot of assets in order to have sufficient weight on the network and obtain a return of investment.

The solution offered by Humble Luck Ball with its Proof of Entry consensus is a validation-by-entry solution, performed as part of an asset sacrifice for the benefit of the community. This sacrifice grants the user a weight in the protocol's non-discriminatory election system, thanks to which he can obtain a reward adapted to his participation in the network.

1.2 What is the roadmap ?

The Proof of Entry consensus development follows a Research & Development methodology. Several technical obstacles exist, and the following steps will enable the solutions defined to be validated and built upon :

- Q2 2022 →Deployment of Mainnet 1.0, Proof of Entry **Protocol**, simulated on the Avalanche blockchain.
- Q1 2023 →Deployment of Mainnet 1.5, Proof of Entry **Sub-net**, sustained by Avalanche.
- Q1 2024 →Deployment of Mainnet 2.0, Proof of Entry **consensus** on an independant, native blockchain.

1.3 Luck Ball Coin (LBC) Utility

The LBC is the digital asset of the Humble Luck Ball project. First as an ERC-20 token, it will become the native coin of the Proof of Entry based blockchain. Here are its characteristics :

- Max Supply : **300.000.000** LBCs.
- Initial deployment : **2.028.237** LBCs.
- Tokenomic : **100% to the community**.

The Luck Ball Coin is used on the Proof of Entry protocol to ensure its proper functioning, through the intrinsic validation of the blocks and the genesis of new LBCs for the user community.

Starting March 6, the LBC token can be redeemed for AVAX on the Humble Decentralized Offering (HDO), available at the following link: <https://hdo.humbleluckball.com>. The characteristics of this HDO are presented on page 21.

2 The Humble Luck Ball (HLB) Project

2.1 General description

Start-up created in September 2020, Humble Luck Ball has been designated as a finalist for the AIBC Summit¹ in May 2021 thanks to its new blockchain protocol. The **PoE** "Proof of Entry" should make it possible to overcome the main shortcomings of cryptocurrencies. The economic system of tokens **LBC** (for Luck Ball Coin) is an exception in the field of digital assets. The founders' goal is to create a 100% independent, transparent and community-based cryptocurrency through the **Humble Luck Ball** (HLB) ecosystem.

Currently, most cryptocurrencies are based on Proof of Work or Proof of Stake consensus that reward users with solicited blockchain assets.

The first consensus Proof of Work is known to consume a lot of energy and finds with Proof of Stake its limits regarding fairness towards its miners/validators. Without substantial equipment or a lot of tokens to invest in, it is almost impossible for newcomers to participate in the evolution of a blockchain. It is for these reasons that Humble Luck Ball seeks to develop a new technology based on a new blockchain consensus using a totally innovative protocol: "Proof of Entry". It is meant to make it possible to overcome the defects mentioned above while offering a system accessible to the general public.

In summary, the Proof of Entry consensus should make it easy for any user to become a participating node and eligible for system block rewards, regardless of their weight on the decentralized network. Users should thus be able to participate in a 100% community-based and scalable network.

We are going to overcome many **scientific and technical uncertainties** in order to **achieve an implementable technology and solution**. **The design of this technology requires numerous studies, trials, tests and developments**. Thus, the research & development operation currently represents all of the company's activities.

⁽¹⁾ *AIBC is one of the world's leading events for emerging technologies aimed at bringing together an elite selection of delegates, politicians and thought leaders from around the world. This international support and interest has helped propel the AIBC Summit to become a favorite on the global emerging technology conference and exhibition circuit.*

2.2 Objective of the HLB project

Blockchain is a technology that allows information to be stored and transmitted in a completely transparent and secure manner. We often talk about blockchain with cryptocurrencies such as Bitcoin (with Proof of Work) or Ethereum (future Proof of Stake).

| Proof of Work (PoW) | Proof of Stake (PoS) |
|--|---|
| Participating nodes are called miners | Participating nodes are called validators |
| Mining capacity depends on computational power | Validating capacity depends on the stake in the network |
| Mining produces new coins | No new coins are formed |
| Miners receive block rewards | Validators receive transaction fees |
| Massive energy consumption | Low to moderate energy consumption |
| Significantly prone to 51% attacks | 51% attacks are virtually impossible |

- The Proof of Work (PoW) consensus has the main drawbacks of being extremely expensive in computing power and of being reserved for individuals who have the capacity to equip themselves with a powerful and expensive computing tool.
- The Proof of Stake (PoS) consensus has the main drawbacks of restricting its economy to assets already in circulation, while requiring validators to stake their assets under a power of validation, for a fixed period of time.

Here, the Humble Luck Ball project aims to offer another blockchain protocol on which a new consensus (see glossary) will be developed: the **Proof of Entry (PoE)**.

| |
|--|
| Proof of Entry (PoE) |
| Participating nodes are called users |
| Validating capacity depends on the total number of users |
| Use of contract produces new coins |
| Users receive cycle rewards |
| Low to moderate energy consumption |
| 51% attacks are virtually impossible |

The founders want to design a system that is :

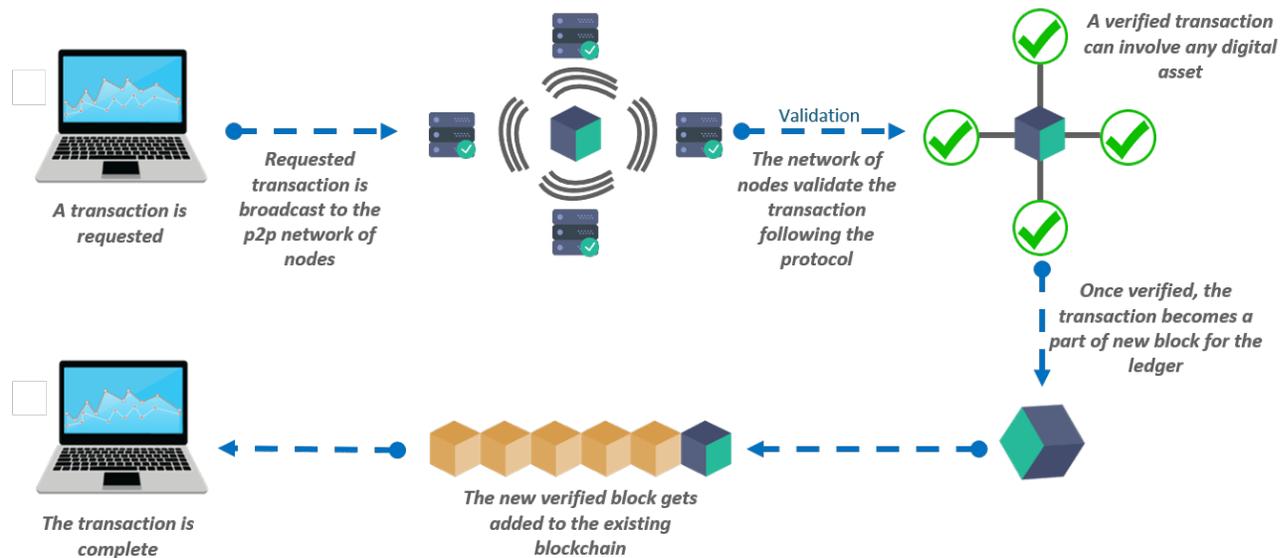
- simple to understand and use.
- based on community participation.
- decentralized from any third party.
- fair among all its users.
- secure for all its users.

The added value of this new consensus is to allow any user to easily participate as a validating node, having an impact on the issuance of new coins while obtaining a reward equal to the community contribution whose distribution is randomly and exclusively determined by the community of users.

Moreover, the Proof of Entry consensus would allow the use of 100% of the validator effort under the blockchain and thus cause no loss of effort. To achieve this, the principle is to generate rewards according to the entries made on the network and the stimulation of the blockchain, according to the number of assets sent on the election cycles. This means that the more users interact with the blockchain's cycles, the more LBC tokens are generated. All of this will be governed by a halving mechanism to avoid a shortage of supply or excessive inflation. At the end of a cycle, the system will choose the node receiving a reward by calculating the participation entries generated by the participating users, and trigger a **deterministic pRNG equidistributive allocation algorithm** to select the rewarded addresses.

2.3 State of the art

A blockchain is a totally decentralized system based on a peer-to-peer network. Each node in the network keeps a copy of the ledger (see glossary) in order to avoid having a single point of failure. All copies are updated and validated simultaneously. Although the original purpose of creating the blockchain was to solve the problem of multiple cryptocurrency (virtual currency) spending, this technology can be explored in many use cases and used as a secure means of managing and protecting of all kinds of data (monetary or not). [AYADI 2019]



Blockchain operating steps

source : [Medium](#)

Blockchain is still in the early stages of development. The first phase is Blockchain 1.0 [SWAN 2015, GATTESCHI 2018], whose most representative cryptocurrency is Bitcoin [NAKAMOTO 2008]. The appearance of smart contracts then initiated the second phase, Blockchain 2.0 [CHRISTIDIS 2016].

The next generation of blockchain will be the era of the blockchain-programmable society of things. Blockchain-related aspects could affect both human ideology and social form [LU 2018]. It is on this axis of the development of fair human interactions that Humble Luck Ball seeks to develop a new consensus, an innovative protocol and a cryptocurrency using it.

Developing a blockchain requires building 6 successive layers (see diagram below).

| Layers | Main technologies or components |
|--------------------------|---|
| Data Layer | Data block, chain structure, timestamp, Merkle tree, cryptography |
| Network Layer | P2P network, verification mechanisms, broadcast protocol |
| Consensus Layer | PoW, PoS, DPoS, PBFT, ... |
| Contract Layer | Smart Contract, scripts, incentive mechanisms |
| Service Layer | Ethereum, hyperledger, IBM Azure BaaS, ... |
| Application Layer | Crypto-currency, health, cloud service, ... |

The construction of these different layers requires the creation of new structures, new ways of recording, storing, expressing data, and above all validating them. **The consensus mechanism is the central point that defines a blockchain.** The consensus principle chosen defines the operating rules of the blockchain in question. The design of this mechanism defines the interactions between groups of nodes. Its functionality in a distributed system and its

integrity represent a real technical challenge [LU 2019].

For example, for bitcoin, the protocol generates a large amount of resources and computing power, which leads to low system throughput and long system latency [SANKAR 2017]. Privacy and scalability are also criticized as there are no privileged users, rather a participant can join the network, gain access to information available on the blockchain, and also validate new transactions. Similarly, scalability limits with reference to data size and transaction processing rate [YLI HUUMO 2016]. Privacy and security issues are major concerns in blockchains as information becomes accessible to all peers in the network.

So, although the foundation of blockchain technology is relatively mature, there are still many technical issues to be resolved. Many protocols exist but none currently succeeds in responding to all of the following issues:

- energy saving,
- cost savings,
- execution power,
- scalability power, security, fairness [ZHENG 2017]

Solving these different issues involves developing a new consensus, and therefore a new way to determine node validation and associated reward.

Defining even the structure of this equation requires study, development and testing. This equation must then be tested at scale to measure the results and ensure their consistency.

In order to study the equation behaves in face of strong variations (increase or decrease) in activity, simulations and experiments relating to the functionality are necessary, and will make it possible to evaluate and qualify the scalability of the system.

2.4 HLB Project Roadmap

In order to develop Humble Luck Ball, different bricks must be designed, developed and tested:

- The Proof of Entry (PoE) protocol.
- The Luck Ball Coin (LBC) token.
- The Humble Luck Ball (HLB) smart contract.
- The Humble Luck Ball dAPP.
- The Humble Market decentralized exchange platform.

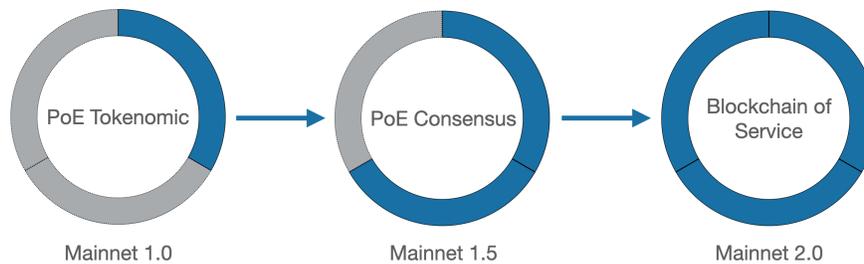
The first objective to be achieved is the deployment of the “Proof-of-Entry” (PoE) protocol available to the public with its underlying digital token: the Luck Ball Coin (LBC). The protocol is made up of a set of Smart Contracts (executable instructions on an EVM-compatible blockchain) decoupled into several services. The protocol works in a decentralized way: the management of LBC inflation and its evolution over time thanks to adaptive algorithms based on participation in protocol cycles is a critical point.

This protocol must be deployed on an EVM-compatible and public blockchain, to ensure a usable and secure Layer 1. We plan to deploy this protocol on the Avalanche “C-Chain” blockchain. A “Decentralized Application” (dAPP), allowing users to interact with PoE Smart Contracts, will be available as a web application and will simplify the actions that PoE users can perform. We want to process up to 200 blocks per PoE cycle, with no limit of participants per cycle. We call this phase Mainnet 1.0 and it allows a first emulation of the PoE consensus.

The second objective is the **creation of a “custom blockchain” featuring its native currency “Luck Ball Coin”, and hosted as a “subnet” on the Avalanche network**. This objective will make it possible to integrate the decentralized management of the “seed” necessary for the generation of decentralized pseudo-random numbers. This will also make it possible to overcome the limitations of the C-Chain in terms of data processing per block which

is currently 8 million (gas limit). A dAPP will allow access to the blockchain and native wallet management. A migration will be available for the transfer of assets present on the C-Chain to the custom blockchain. This phase will also allow the implementation of the first prototype of a Community Contributor Token (CCT) allocation algorithm for the implementation of a validation delegation system for the PoE consensus. This phase corresponds to Mainnet 1.5 and allows a transition from an emulated consensus to a native PoE consensus.

The third objective is the **deployment of a native blockchain with PoE consensus**. This blockchain of service will make it possible to offer deployments of Smart Contracts (contract layer cf. Table 3) and in particular the use of its various services offered: block rewards, use of a verifiable delayed function system, validation of transactions on the decentralized network. This step allows for greater scalability and deployment of upper-layer solutions while ensuring a low power consumption blockchain (compared to a PoW blockchain) and guaranteeing non-discriminatory access to the system’s block rewards. This phase corresponds to Mainnet 2.0. During this Mainnet 2.0 phase (starting from 2024 depending on the progress of the work), HLB will be able to open up to the public possibilities for the development of scalable and accessible decentralized algorithms, for the development of complex digital assets with rules, clauses, and personalized endorsements.



2.5 Uncertainties, technological locks and problems to be solved

As mentioned in the previous sections, various locks must be overcome to develop this new consensus:

- **To conciliate the system for assigning trust weights to Proof of Entry participating nodes and their participation on the network as validators or delegators.**

Developing a new protocol requires finding the rules that allow the operation of the system while guaranteeing the fairness of the system, its security, and its scalability for example. You have to be able to develop a protocol that assigns the right trust weights, and that ensures that even if the attribution is granted to a malicious actor, it does not weaken the execution of the system. A gossip algorithm (see glossary for definition) must be developed in order to be able to decide between users and decide whether or not to validate a cycle.

The major technical problem of the project generating the bulk of the **technical lock** therefore lies in the following question: "While the principle of the blockchain is that all data is public and available, how to generate verifiable data at all moments, without being known to the participants before being available on the blockchain"?

- **Ensure the stability and security of a temporary PoE Layer 2 data retention protocol while the consensus is immutable over time on a public blockchain**
- **Ensuring scalability and speed of information processing without centralization by reconciling the various meta-transactions of the system necessary for the existence of HLB applications**
- **Keep sufficient parameterization** to mitigate the hardfork needs (see glossary) of the blockchain and couple it to a decentralized voting system to avoid underlying governance or consensus update problems **without diminishing the security of the system** (without exceeding the threshold of tolerance of malicious actors).

2.6 Applied Methodologies

2.6.1 General approach

Each stage of development of our decentralized solutions undergoes the following steps:

1. Design POC (Proof Of Concept) and Unit Tests: Unit tests make it possible to ensure non-regression of what the development or update of functionalities could bring.
2. Local Simulation / Benchmarking: Local simulation and benchmarking allow monitoring and verification of the scalability of the system before deployment on the Testnet.
3. Testnet: The testnet allows testing in a “real” situation with non-simulated users for a preview of new features before their “stable” release on the “Mainnet” production network.

In order to qualify the success of each step of the protocol, the modules are continuously checked and updated with CI/CD processes. An automatic dependency check is also done to check for potential vulnerabilities.

2.6.2 Work completed

The research & development work that has been carried out has made it possible to develop the first bricks of the Humble Luck Ball blockchain.

We first conceptualized the PoE protocol by performing theoretical calculations and architecture diagrams. This step allowed us to delimit and architect the functionalities necessary for the development of the PoE protocol on an EVM-compatible blockchain. This allowed us to create a first prototype of the PoE protocol decoupled into several services. However, it was imperfect and we were able to optimize certain factors to ensure several things:

- Better equiprobability of participant elections
- User participations at a constant cost regardless of the number of LBCs sent to the cycle ($O(n) \rightarrow O(1)$)
- Purification of the system while maintaining sufficient modularity in the event of contract upgrades

Some stages were particularly complex during 2021 :

These steps represent the foundation upon which all other future elements of Proof of Entry consensus development are built. Arbitrary decision-making has been decided on purely hypothetical bases of what we imagine will be the consensus of tomorrow, so there is no certainty that all of these hypotheses will make it possible to develop the HLB blockchain.

- **Development of smart contracts including the Proof of Entry protocol, deployment of these on a blockchain available on a testnet called Rinkeby (Ethereum blockchain).**

Regarding the deployment of the PoE protocol and its underlying digital token the LBC, we first had to create a digital asset that met an established security standard (ERC) that could be used as imagined on the HLB protocol.

- **Deployment of the Humble Luck Ball protocol on the Ethereum blockchain because of incompatibility between necessary resources and performance for the user/Humble Luck Ball:**

This incompatibility comes in particular from the amount of Ether (ETH) to be spent on the Ethereum blockchain for any transaction, contract interaction, and use of the HLB protocol by future users. It would be incongruous to imagine a protocol requiring a cost greater than the possible return generated by the inflation of LBCs as they are dynamically generated thanks to the protocol’s use by users.

In addition, the Ethereum blockchain limits us in the initially imagined interactions of the Proof of Entry protocol by the “block gas limit”, which limits the potential number of users in an HLB cycle.

- Optimization of gas costs related to the use of the Humble Luck Ball protocol for users.
- Optimization of the internal gas costs of the different election algorithms and processing of block rewards/participations in cycles.

- Optimization of the protocol architecture for better data processing efficiency, memory footprint, and transactional purpose.

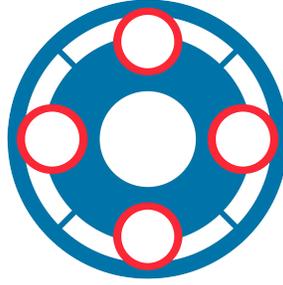
Subsequently, we were able to consider the development and deployment of the HLB (Humble Luck Ball) protocol including the PoE (Proof of Entry) protocol. As such, we have:

- Performed the following tests :
 1. Test of the correct reception of the LBC digital asset on the HLB protocol via local blockchain and test Ethereum blockchain (Rinkeby).
 2. Testing the call match between all smart contracts composing the HLB protocol.
 3. Test of the total independence of smart contracts from external use.
 4. Public test (real testnet condition) to visualize the reaction of the dynamic algorithms built into the HLB protocol. (18 Cycles on the Rinkeby test Ethereum blockchain, currently 85 Cycles on the Fuji test Avalanche blockchain)
- Fixed the following failures :
 1. The impossibility of adapting the contracts making up the HLB protocol once they have been deployed. →Solved.
 2. The impossibility of deploying the HLB protocol on the Ethereum blockchain given the restrictions on holdings →Migration on Avalanche.
- **Development of smart contracts for the migration of the digital asset from the Proof of Entry protocol, the LBC, from the Ethereum blockchain to the Avalanche blockchain (in progress) and the communication bridge between these two blockchains.**

Given the development difficulties intrinsic to the Ethereum blockchain, it was deemed necessary to migrate the technology to another blockchain: the Avalanche blockchain.

The Avalanche migration requires checking, rethinking, redeveloping the operation of HLB. In this case, reconciling the system of assigning trust weights to Proof of Entry participating nodes and their participation on the network as validator or delegator required additional effort, and we have:

- Performed the following tests :
 1. Testnet of HLB protocol for 18 Cycles on Rinkeby and currently 85 Cycles on Fuji. (More than 15 Million test LBCs generated thanks to the daily participation of hundreds of users).
 2. Test of the equidistribution of cycle rewards carried out among participants.
 3. Test of the LBC inflation system as a result of user participations.
 4. Test of the rate of cycles opening and closing operations and the duration of the latter on the HLB protocol.
 5. Test of the difficulty inherent to participating in a cycle, as a result of the use made of the HLB protocol.
- Fixed the following failures :
 1. The impossibility of testing more elements allowing us to respond to this technical lock on the Avalanche network. →Requires Avalanche Subnet scheduled for Q1 2023.
 2. The inability to make the number of block rewards per cycle dynamic. →Limited to 200 rewards per cycle due to the Block Gas Limit of the Avalanche blockchain.



3 Products and services of the Humble Luck Ball (HLB) project

3.1 The Luck Ball Coin (LBC) token

3.1.1 Token's nature

The Luck Ball Coin (LBC) token is a utility token that respects the ERC-20 Standard [Ethereum Request for Comment n°20](#).

This token is deployed by the Humble Luck Ball company. An initial deployment of 811,925.09LBCs were minted from the 27th of February to the 27th of June 2021 through 205 holders participating to the ICO (cf. lexicon). During July 2021, we have updated the tokenomic as to adjust the number of LBCs in circulating supply by a 1.5 times multiplier. At the date of migration from the Ethereum to the Avalanche blockchain, the total number of LBCs were 2,028,237.73LBCs held by 210 wallets.

Initially deployed on the Ethereum blockchain, a migration to the Avalanche blockchain is available since the 19th of December 2021. Today, the LBC token is undergoing anIDO later presented in this document as to deploy the Mainnet 1.0. (Proof of Entry protocol).

The deployment of new LBC tokens is exclusively regulated by the community of users and investors. Indeed, the exclusive feature of the LBC token's inflation process is to be directly influenced by the Proof of Entry (PoE) concept.

3.1.2 Inflation and Halving

The Proof of Entry protocol insures the LBC's inflation as a **Cycle** ends. The generated LBCs will supply the **Humble Pool**; a Vault within the Proof of Entry protocol from where bloc rewards are drawn.

The number of LBC deployed through the Proof of Entry protocol is exclusively determined by the active participation of the community of users for entries made on the Humble Luck Ball smart contract.

When a certain amount of Luck Ball Coin tokens are in circulating supply, a Halving process is operated to the equation governing the inflation calculation.

3.2 Proof of Entry Protocol (Mainnet 1.0)

The Proof of Entry protocol is a new and unique 100% community-driven protocol which makes the block reward accessible to everyone. Performed by sending LBC, an Entry grants the user a weight in a non-discriminatory election system, thanks to which he can obtain a block reward in LBC.

This protocol is part of an ecosystem comprising six smart contracts interacting together : Humble Luck Ball, Cycles Manager, Participants Vault, Pool Escrow, Xoshiro256ss, and Proof of Entry.

The Humble Luck Ball (HLB) smart contract is the main element of this ecosystem. When users wish to make an Entry, the algorithm contained in the HLB contract follows a number of steps. A **Cycle** is performed when all steps are complete.

3.2.1 Cycles Architecture



Humble Luck Ball Contract

This contract is the core module of Humble Luck Ball. It interacts with the different services to create the Proof of Entry protocol on Avalanche

- Repeat
- 1 Humble Luck Ball Contract initialize a cycle and retrieves a hash of the community generated Seed for verification before election. Participations are now open
 - 2 Users can participate to the Cycle by sending a desired amount of LBC to get an allocated number of entries. The number of LBC per entry depends on the PoE protocol's difficulty
 - 3 Participations are closed and the community generated Seed is sent to the Humble Luck Ball Contract. It is verified and initialized to setup the Deterministic RNG
 - 4 After the Election process, Proof of Entry computes the system's inflation, adjusts difficulty and next block reward
 - 5 Users can withdraw their earnings at any moment from their personal vault inside the Proof of entry's safe. The Cycle is now complete and a new Cycle is started

2



Participants Vault

This service takes care of users' participations to PoE cycles

3



Deterministic RNG

This deterministic RNG contract helps determining rewarded users based on the community generated Seed

4



Proof Of Entry Contract

This is where all the protocol's difficulty, inflation and block rewards are computed and set

5



Proof of Entry's safe

This safe holds the Humble Pool and all users' balances and earnings from the PoE



HLB Proxy Contract

Users interact with the Humble Luck Ball Smartcontract through a seamless proxy contract

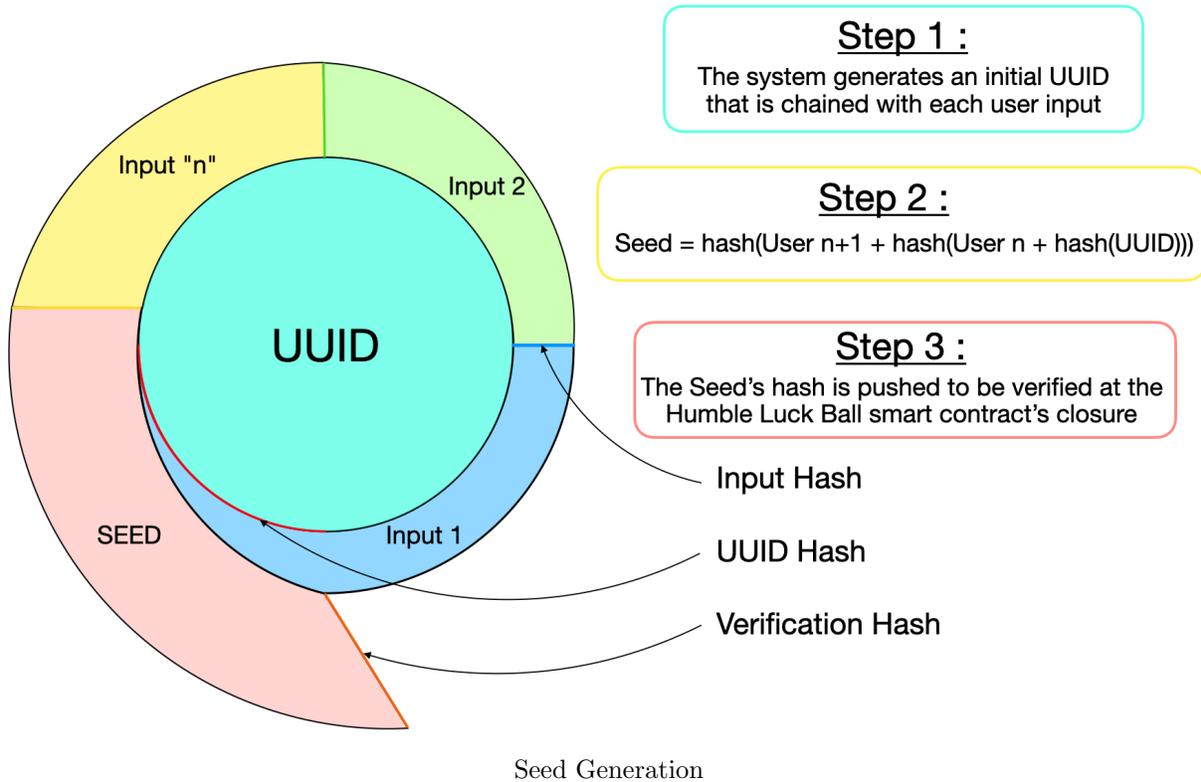


Safe Proxy Contract

Users can withdraw their LBC earnings through another seamless proxy contract



3.2.2 Entropy



Seed Generation

Before the Cycle's initialization, a value for the pRNG algorithm called the Seed is powered by the users on the Humble Luck Ball Platform. Users participate in the entropy.

The system generated an initial *Universally Unique Identifier (UUID)* which is chained by a hash set with each input made by users in chronological order.

A hash is a special function which, from data supplied as input, calculates a digital fingerprint used to identify the initial data.

When the HLB initializes a cycle, the Seed's hash is pushed to the contract in order to be verified at the cycle's end.

The participation of users to the seed generation is optional, but it guarantees the entropy for the block reward's election process.

Seed Verification

When the HLB cycle is initialized, only the Hash of the Seed generated is sent to the HLB contract. This Hash is therefore made public while keeping the original Seed private.

The HLB cycle can only end if the original Seed is sent to the HLB contract. The result of the Hash of this Seed is verified to be the Seed Hash that was originally sent publicly. The pRNG solution can then operate.

The Seed verification makes it possible to confirm that its generation was indeed carried out by the community of users, and that no third party was involved to contribute to the selection of elected users by the pRNG solution.

3.2.3 Community Participation (CP)

Community Participation (PC) is an event linked to the initial deployment of LBCs through the ICO, which ended the 27th of June 2021.

To drive the community of users, a 5% share of the deployment planned by the ICO supplies the Humble Pool for the first three cycles of the HLB contract.

- **2,028,237LBC** were deployed for participants.
- **101,410LBC** are deployed for PC :
 - ◊ Humble Pool of cycle 1 : 33,803LBC
 - ◊ Humble Pool of cycle 2 : 33,803LBC + LBC collected during cycle 1 + PoE
 - ◊ Humble Pool of cycle 3 : 33,803LBC + LBC collected during cycle 2 + PoE

Thanks to CPs, the PoE contained inside the HLB contract will be solicited and will trigger LBC inflation.

3.3 Humble Market exchange platform

The Humble Market exchange platform is a decentralized exchange platform, or DEX, based on buy or sell orders in AVAX or LBC.

The Humble Market's goal is to allow dilution of LBCs deployed through the PoE for new incoming users. These LBCs will be exchanged for AVAX at the market's value, set by the trades performed between users.

The Humble Market dAPP allows its connected users to :

- To deposit/withdraw AVAX.
- To deposit/withdraw LBC.
- To accept a buy or sell order.
- To place a buy or sell order.
- To cancel their buy or sell order.

The Humble Luck Ball company will provide a great way to maintain a fair LBC price at all times, based on weekly availability stocks thanks to Proof of Entry. It is both designed as a way for our users to get the best available price for LBC, while also to limit speculation from last minute participation's valuation on the Humble Luck Ball smart contract.

The number of LBCs deployed through Proof of Entry for the Humble Market exchange platform is not yet defined.

4 Humble Luck Ball Testnet

| Contract | Fuji Address |
|--------------------|--|
| 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 Requirements



Humble Luck Ball

Testnet Network : *Fuji!*



Add the new RPC on metamask:

1 - Select Custom RPC: 

2 - Fill out the following fields:

Avalanche FUJI C-Chain →

https://api.avax-test.network/ext/bc/C/rpc →

43113 →

AVAX →

https://cchain.explorer.avax-test.network →

3 - Save the settings

How to set up Metamask for Fuji Network?

4.1.1 Setting up your wallet on the Fuji network

Some Avalanche wallets are making the access to testnet networks relatively easy. For example on the MetaMask wallet, here are the steps to follow :

- Click on "Ethereum Main Network" at the top of the extension.
- Select Custom RPC.
- Fill out the following fields :
 - ◊ 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 Acquire AVAX on Fuji

The screenshot shows the interface for the Humble Luck Ball AVAX Fuji Testnet Faucet. At the top, there is a blue banner with the Humble Luck Ball logo and the text "Humble Luck Ball". Below this, it says "Testnet Network : *Fuji!*". A button labeled "Avalanche FUJI C-Chain" is visible. A blue banner with white text reads "Ask AVAX Fuji Testnet Faucet for test AVAX". The URL <https://faucet.avax-test.network> is displayed. To the right is a red box with the AVAX logo. Below the URL, there are three instructions: "- Paste your wallet address", "- Solve the CAPTCHA", and "- Request your test AVAX". A blue button labeled "*It's done!*" is shown. On the right side, the "AVAX Fuji Testnet Faucet" interface is shown, including a text input field for the address, a CAPTCHA verification box, a warning message "This is a beta faucet. Funds are not real.", and a "REQUEST 2 AVAX" button. At the bottom, a blue banner contains the text "How to get free test AVAX for the testnet?".

The Fuji Network proposes a [Faucet](#) for which you need to paste your wallet address and click on the button to retrieve 10 test AVAX. You can only do this step once per hour.

4.2 Smart Contract Interaction

A user can participate to the Humble Luck Ball in two ways : from his wallet, or from his vault. Only one unique participation is allowed per cycle.

4.2.1 Participate to the Humble Luck Ball

A User can interact with the *Participate* function by sending Luck Ball Coin (LBC) tokens into the Humble Luck Ball (HLB) Smart Contract. A user can find below the Humble Luck Ball smart contract's address, and check the Hex Data to participate :

- **HLB Contract** : 0xb83a176204e993d78CC305B85F8CEA8750542f79
 - ◊ **Hex Data Participate** : Page 18

This function allocates a number of entries based on the User's participation in LBC. If the RNG solution elects the User, he will be rewarded with a Block Reward sent directly into his **Vault**.

4.2.2 Participate through the Vault

A User will receive the Block Reward's LBCs directly into his Vault if the latter has been selected thanks to the RNG solution. A User can then decide to either participate to the Humble Luck Ball again with LBCs contained inside his Vault, withdraw a specific amount of LBC from his Vault or withdraw all LBC tokens contained inside the Vault.

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

4.2.3 Add an entry to the Entropy

Coming Soon

4.3 Beta Testers Rewards

4.3.1 Rewards eligibility

An incentive has been proposed to Beta Testers in order to attract adoption of the Humble Luck Ball smart contracts and its Proof of Entry protocol.

Here are the four requirements for the Beta Testers reward eligibility :

- Participate to the Humble Luck Ball
- Participate to the Humble Luck Ball through the Vault
- Add and entry to the Entropy
- Own at least 500LBCs

A User has to have acquired at least 500 LBCs on the Avalanche Mainnet blockchain as to be eligible for the Beta Testers reward before the Mainnet deployment. This includes and is limited to acquiring Luck Ball Coin through the migration of existing assets from the Ethereum blockchain or buying them through the Humble Decentralized Offering (HDO).

4.3.2 Luck Ball Coin (LBC) Rewards

Following the community pool of August 2nd, 2021, where 84% of voters were in favor of a financial incentive to participate to the Proof of Entry Testnet protocol, 150.000 LBCs were minted for the distribution of 500 LBCs to the first 300 Beta Testers which met the eligibility criteria described above.

This reward can be retrieved from a special dAPP available shortly after the release of Mainnet 1.0, which will mark the Proof of Entry protocol's deployment on the Avalanche blockchain.

4.3.3 NFT Reward

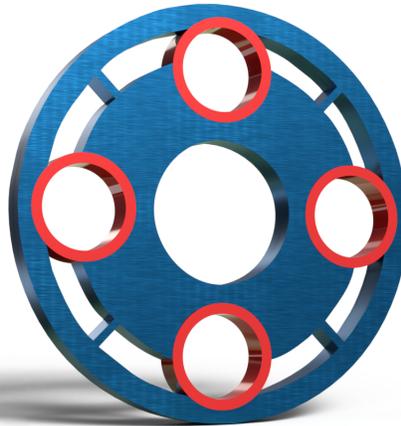
Considered as a store of value thanks to their rarity, NFTs are a marker of an era that is definitely part of the blockchain experience. The rise and adoption of NFTs are undeniably linked to a strong emotion : the sense of belonging to a community for those who possess it.

It is in that regard that the very first investors, as well as the Beta Testers of the HLB contracts, will be rewarded with unique and nominative NFTs linked to their exclusive and personal experience of the HLB adventure.

The selected events are :

- The ICO participation
- The Rinkeby Testnet participation
- The Fuji Testnet participation
- The Humble Decentralized Offering participation

These NFTs will be distributed individually to each person proving their participation by the address used at these key stages of the HLB adventure once the Proof of Entry protocol is deployed under Mainnet 1.0.



NFT Luck Ball Coin of Fuji Testnet



5 Characteristics of the Initial Decentralized Offering (IDO)

5.1 Why an IDO ?

The Humble Luck Ball company continues its deployment of Luck Ball Coin (LBC) tokens through an initial Decentralized Offering whose characteristics are fully linked with the values of the Proof of Entry protocol.

Indeed, it ensures the successful launch of the Proof of Entry protocol for an IDO allows :

- To increase the number of LBC tokens in circulation.
- To guarantee an initial value of the LBC token thanks to liquidity.
- To make the acquisition of LBC tokens accessible to incoming users.

This also makes possible the financing of the Research & Development work of the Humble Luck Ball, through the investments for :

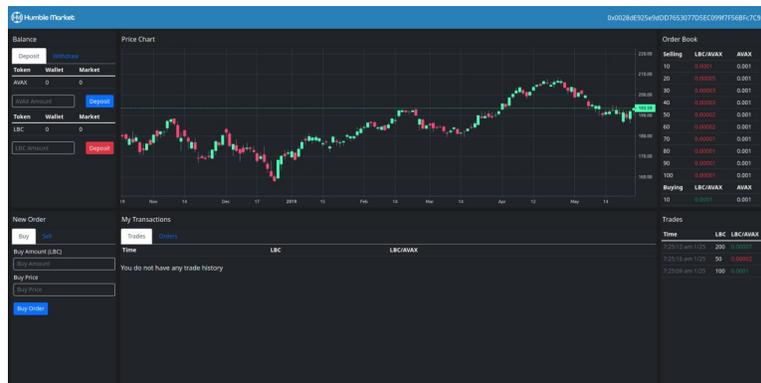
- Recruiting qualified developers and employees.
- Operate an Avalanche validator node for the Humble Luck Ball Avalanche Sub-net.
- Actively communicate internationally and make the project accessible.

5.2 Humble Decentralized Offering (HDO) presentation

The Humble Luck Ball company is proud to deploy its Luck Ball Coin token offering from its native decentralized exchange platform, the Humble Market. This offer, called the Humble Decentralized Offering, allows to acquire Luck Ball Coin (LBC) tokens in exchange for AVAX. This dAPP is hosted on <https://hdo.humbleluckball.com>.

The number of tokens available through this offer is 2,515,000 LBCs, per stocks of 20,120 LBCs smoothed over 125 levels, valuing the token with an AVAX equivalence of \$0,01 per level.

Thanks to its intuitive user experience, this DEX allows the HLB community to master the future medium to buy and sell their LBC.



Humble Decentralized Offering

| Cap | Price in \$ | LBC Stock | Stock in \$ |
|-----|-------------|-----------|-------------|
| 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 | Price in \$ | LBC Stock | Stock in \$ |
|-----|-------------|-----------|-------------|
| 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 | Price in \$ | LBC Stock | Stock in \$ |
|----------|-------------|-----------|-------------|
| 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 | Price in \$ | LBC Stock | Stock in \$ |
|----------|-------------|-----------|-------------|
| 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 | | | |