2024

Herb Coin Whitepaper

A Herb Payments-Focused Cryptocurrency

VERSION 1.2.0   PUBLISHED DATE: 8-JULY-2024

Table of Contents

1. Introduction

Bitcoin is a cryptocurrency that has emerged as a popular medium of exchange and is the first digital currency that has attracted a substantial number of users. The idea behind Bitcoin was to eliminate the central authorities such as banks with a new peer to peer electronic cash system. The system was elegant and transparent, every transaction made in the system is recorded in the blocks and anyone could track them down, besides, it was not revealing anyone's identity since the addresses were not coupled with any real people. These features attracted more people in time and in the recent years many blockchain systems have emerged. Since its inception in 2009, Bitcoin has been rapidly growing in mainstream adoption and merchant usage. Focusing on the peer-to-peer usage in payment aspect, a main issue with the acceptance of Bitcoin in point-of-sale (POS) situations is the time required to wait for the network to confirm the transaction made is valid. Some payment processors have created methods to allow vendors to take zero-confirmation transactions, but these solutions utilize a trusted counterparty to mediate the transaction outside of the protocol.

Bitcoin provides pseudonymous transactions in a public ledger, with a one-to-one relationship between sender and receiver. This provides a permanent record of all transactions that have ever taken place on the network. Bitcoin is widely known in academic circles to provide a low level of privacy, although with this limitation many people still entrust their financial history to its blockchain.

Later on, talented people created Ethereum which united the contracts with Blockchain and smart contracts were born. That became a gateway for developers to create their own tokens and smart contracts. Today, a lot of cryptocurrencies are using Ethereum platform and that proves Ethereum help blockchains develop in a good way.

However, a lot of cryptocurrencies have been created, it is adopted in specific purposed, and the majority of people still feel difficulty in using cryptocurrency in real life. Seem like the adoption would take more time to let people familiar with.

Herb Coin is a payment-focused cryptocurrency which will be used in herb ecosystem, It is run on Hybridge blockchain Proof-of-Work (PoW) and Proof-of-Stake (PoS) protocol using its custom developed PoS consensus engine with a native cryptocurrency.

2. The Purpose of Herb Coin

In general use, herbs are plants with savory or aromatic properties that are used for flavoring and garnishing food, for medicinal purposes, or for fragrances. Around the globe, the varieties' purpose of using herbs leads to increase demand in the market especially to the rare herbs. Moreover, there are many steps in supply chain before reaching to consumers which take times and impact in market price, Herb Coin is created based on Bitcoin, Novacoin, and Blackcoin technology, and to be used in specific eco-system aim to adopt in Herb market related and also allow producers and consumers around the globe can contact each other directly through the eco-system. The platform would be help eliminate the intermediaries, cut unnecessary cost which result in decreasing the price of the product for end consumer, and increase rare herbs more accessible to everyone. In additional, the users can earn more benefit from the ecosystem in DeFi part.

Our goal is to create a global marketplace with cryptocurrency payment option to remove currency conversion costs, reach farmers and customers beyond country borders and decrease the overall costs even more. We aim to engage key partnerships such as universities, medical institutions, farmer, marketplaces etc. to get involve in supply chain and ecosystem. This innovative to traditional Herb market would bring positive impact in the smart way. Herb Coin is created based on real business and back-up by value of the business itself. This means the value of the coin relates with business value directly. Herb Coin can be exchanged to products, medical & wellness services and earn more Herb Coin from DeFi functions.

3. Why Proof of Stake

With some similarity to PoW, PoS differs from it in fundamental ways. For instance, PoS protocol implies that the miner of a new block is chosen in a semi-random, two-part process, where the first element to be considered is a user's stake. The more you stake, the better your chances of being selected for block validation. If your transaction vote is aligned with other miners — you get a block reward. Because the most important theory of PoS is that those who stake are going to want to help keep the network secure by doing things correctly. If a forger attempted to hack the network or process malicious transactions, then they would lose their entire stake. This is why the model works so well. The more you stake, the more you earn. But at the same time, the more you lose if you go against the system.

There are many PoS implementations, most notably are Delegated PoS proposals, used by BitShares, EOS, and Steem. The PoS protocol is also utilized by such digital currencies like Blackcoin, Peercoin, and Nxt.

Key Advantages

Below is the list of reasons why PoS is widely regarded as one of the best consensus algorithms.

1. Energy Efficient: The technology of PoS algorithms assures energy efficiency, especially compared to PoW, by getting away from the energy-intensive mining process because PoS does not need highly complex sums to be solved, meaning that the electricity costs to verify transactions are substantially lower.

2. Affordable for Users: Being less energy consuming, PoS system allows more users to participate in the mining process. Nice mining hardware can cost a miner up to a thousand dollars. Besides, they need to calculate the costs for cooling, electricity and other expenses when they start to participate. With PoS, you do not need any special hardware and only have to buy more coins to take part in the process.

3. Decentralization: Large mining-pools can control a majority of PoW-based networks, which means a threat of centralization. It is a result of the exponential increase in reward per investment on PoW systems, contrary to the linear increase on PoS systems.

4. Security: To attempt a 51% of attacks on the PoS system, the attackers would have to put their assets (a stake) at least 51% of the total amount of cryptocurrency in circulation, which is a big deterrent. If they decided to buy an amount this substantial, then the real-world value of the coin would increase along the way. As a result, they would end up spending significantly more than they could gain from the attack. Not only this but once the rest of the network had realized what had happened, the attackers would lose all of their stakes! For comparison, in case of the PoW system, they won't lose their hardware when attempting the same attack. That mean it is less chance to get 51% attack.

Key Disadvantages

As every consensus algorithm, the PoS protocol also has its disadvantages which are:

1. Weakness against Malicious Intentions: Any participant who is staking coins may very probably have malicious intentions. For instance, a user may vote for both forks of the blockchain. It would then be an extremely undue advantage if a validation mechanism is not present.

2. The Likelihood of an Oligarchy: PoS system opens the ability to monopolize the entire network for its users. When a network node stakes large amounts of coins at once, it's revenue increases. Then the revenue can be spent to buy and stake more coins. This creates a positive feedback loop that brings the network to the same state as an endgame of a board game "Monopoly". Those who have the most money will always have the best chance of winning the reward, making the rich richer. To prevent this, users will have to rely on the majority of big coin holders to be altruistic, which might not work out perfectly.

3. Double-spend attack: PoS allows people to verify transactions on multiple chains, which PoW doesn't. The reason this could be an issue is that it might allow a hacker to perform a double-spend attack. This is when somebody transfers funds to somebody else, but before the transaction is confirmed, they manage to spend the funds again. Under normal circumstances, such an attempt would be prevented when all of the other miners on the network see it. Furthermore, because Proof of Work only allows devices to mine on one chain, the dishonest chain would simply be rejected. On the other hand, in a Proof of Stake model, it doesn't cost forgers any money to mine on multiple chains, possibly allowing

somebody to successfully perform a double-spend. Which is otherwise known as the "'nothing at stake' problem.
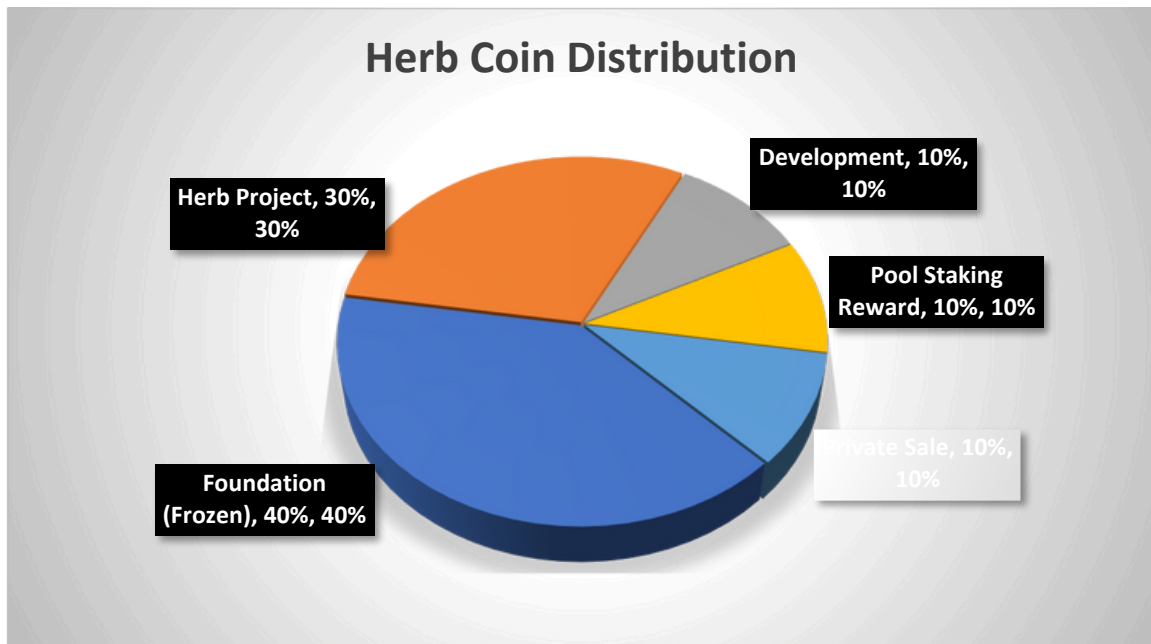
4. The Roadmap
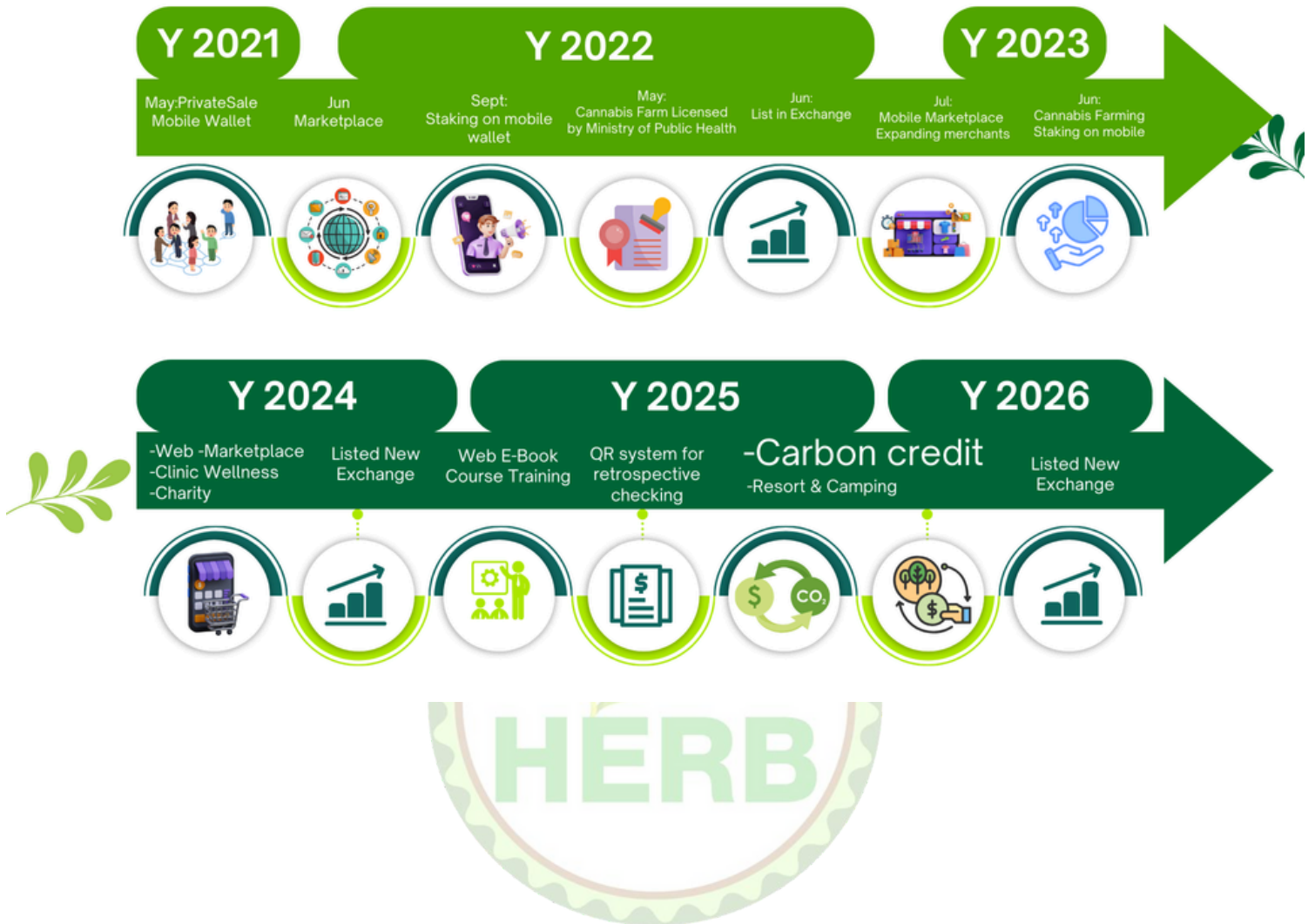
5. HERB Coin Distribution

Total supply is 100,000,000 Herb Coin
- 90,000,000 Herb Coin from PoW
- 10,000,000 Herb Coin from PoS as staking reward (3 Herb per 120 second)

Herb Coin Distribution

- Herb Project, 30%, 30%
- Development, 10%, 10%
- Pool Staking Reward, 10%, 10%
- Private Sale, 10%, 10%
- Foundation (Frozen), 40%, 40%

6. Legal Disclaimer

a) Token Sale Restrictions

If the laws of the country you reside in involve certain requirements for you, as a potential token holder, or for the process of tokens acquisition and exchange, we recommend you consult the lawyers with the relevant practice in your jurisdiction and make a decision about the tokens based on their recommendation. Besides, we would like to bring to your notice that due to technical organization of token issuing and exchange, we do not collect, store, or make use of the potential token holders' personal data, and, thus, we cannot control what jurisdiction they belong to and whether the laws of this jurisdiction are violated. As a result of such circumstances, the responsibility for exchanging tokens in your jurisdiction rests with you, as the token holder.

b) Risks

You acknowledge and agree that there are numerous risks associated with purchasing HERB, holding HERB, and using HERB for participation in Herb Coin Project.

(1) Uncertain Regulations and Enforcement Actions
The regulatory status of HERB and distributed ledger technology is unclear or unsettled in many jurisdictions. It is impossible to predict how, when or whether regulatory agencies may apply existing regulations or create new regulations with respect to such technology and its applications, including HERB Coin Project. Regulatory actions could negatively impact HERB Coin Project in various ways. The Project (or its affiliates) may cease operations in a jurisdiction in the event that regulatory actions, or changes to law or regulation, make it illegal to operate in such jurisdiction, or commercially undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. After consulting with a wide range of legal advisors and continuous analysis of the development and legal structure of virtual currencies, the Project will apply a cautious approach towards the sale of HERB. Therefore, for the crowdsale, the Project may constantly adjust the sale strategy in order to avoid relevant legal risks as much as possible.

(2) Competitors
It is possible that alternative networks could be established that utilize the same or similar code and protocol underlying HERB and attempt to recreate similar facilities. The project may be required to compete with these alternative networks, which could negatively impact Herb Coin Project.

(3) Failure to develop
There is the risk that the development of HERB will not be executed or implemented as planned, for a variety of reasons, including without limitation the event of a decline in the prices of any digital asset, virtual currency or HERB, unforeseen technical difficulties, and shortage of development funds for activities.

(4) Security weaknesses
Hackers or other malicious groups or organizations may attempt to interfere with Herbalist Token Project in a variety of ways, including, but not limited to, malware attacks, denial of service attacks, consensus-based attacks, Sybil attacks, smurfing and spoofing. Furthermore, there is a risk that a third party or

a member of the project or its affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of HERB which could negatively affect Herb Coin Project.

    (5) Other risks

In addition to the aforementioned risks, there are other risks associated with your purchase, holding and use of HERB, including those that the Project cannot anticipate. Such risks may further materialize as unanticipated variations or combinations of the aforementioned risks. You should conduct full due diligence on the Project, its affiliates and the Herb Coin Project team, as well as understand