hodlCoin: A Staking Protocol

Zahnentferner
The Stable Order

Luca D'Angelo
zenGate Global
The Stable Order

Abstract

Staking is a common mechanism used for incentivizing people to continue holding their cryptocurrency, in order to reduce sell pressure. However, this traditionally relies on an inflationary supply of the cryptocurrency to reward stakers. Here, we introduce hodlCoin, a zero-sum multiplayer staking protocol that does not rely on an inflationary supply, wherein users stake a common base asset, thereby purchasing a tokenized representation of their stake. If users sell their hodlCoins, the price of a hodlCoin increases, but purchasing hodlCoins does not increase the price. We prove two theorems: the first that the price is guaranteed to always increase, and the second showing a theoretical maximal return. We have also implemented this protocol for Ergo and EVM-compatible blockchains.

2012 ACM Subject Classification Applied computing → Economics

Keywords and phrases Cryptocurrency, tokenomics, staking, smart-contracts

Related Version *Previous Version*: `https://eprint.iacr.org/2023/1029`

Acknowledgements We are thankful to Alexander Chepurnoy, for discussions about the hodlCoin protocol. We are grateful to Pulsarz, for the first implementation of this protocol on the Ergo blockchain, to Krasavice Blasen for finding a vulnerability in that first implementation and to Shishir Pai and Luca D'Angelo for fixing that vulnerability. We are also grateful to Zahnentferner, Luiz, Bryan and Sarthak Dengre for the first implementation of this protocol for EVM-compatible blockchains. Zahnentferner was responsible for the conception of this protocol and for the proof of Theorem 1 whereas Luca D'Angelo was responsible for the proof of Theorem 2.

1 Introduction

The hodlCoin game is a competitive zero-sum massively multiplayer staking protocol where the goal is to *hodl* (stake) an asset for long periods of time. By hodling, a user deposits *coins* of a given asset in a common reserve and receives a proportional amount of *hodlCoins*. Users who *un-hodl* (unstake) pay a fee that is accumulated in the common reserve. Thus, the longer a user hodls, in comparison with other users, the more the user will benefit from fees paid by the users who are un-hodling earlier. Surprisingly, we prove here that, thanks to the accumulation of fees, the price of hodlCoins in comparison with the underlying asset never decreases.

2 The hodlCoin Protocol

▶ **Definition.** *The system's state is a pair* (R, S) *where:*

- R *is the number of coins in the reserve,*
- S *is the supply of hodlCoins.*

▶ **Definition.** *The* price *of a hodlCoin is:*

$$P(R, S) = \frac{R}{S} \tag{1}$$

▶ **Definition.** *The user can perform 2 actions:*

1. ***hodl:*** *The user deposits n coins into the reserve, and the system mints and gives the user $\frac{n}{P(R,S)}$ hodlCoins.*
2. ***un-hodl:*** *The user gives back n hodlCoins to the system, and the system burns them and gives the user $n(1-\Phi)P(R,S)$ coins, where Φ is a* fee *such that $0 < \Phi < 1$.*

▶ Note. The system is assumed to be initialized with $R = 1$ and $S = 1$ and the *un-hodl* action is disallowed if it would result in $S = 0$. This guarantees that $P(R,S)$ is initially equal to 1 and is always well-defined.

3 Related Work

hodlCoins are like reserveCoins in Djed/SigmaUSD [1, 2] without stablecoins. The *hodl* action resembles *buy reserveCoin* and the *un-hodl* action resembles *sell reserveCoin*, except that:

1. The fees are different. Whereas in Djed/SigmaUSD, the user has to pay a fee when executing any of the two actions. In hodlCoin, the user only has to pay a fee when executing the *un-hodl* action.
2. Whereas in Djed/SigmaUSD the *buy reserveCoin* action is disallowed when the reserve ratio is above the maximum reserve ratio threshold, there is no restricton for the *hodl* action in hodlCoin.

4 Theorems

▶ **Theorem 1** (Never-Decreasing Price). *The price of hodlCoins never decreases: for any sequence of actions $a_1, \ldots, a_k$, $P_k \geq P_0$, where P_0 and P_k are the prices, respectively, before and after the sequence of actions.*

Proof. Proof by induction:

- Base case (to prove $P_k \geq P_0$ when $k = 0$): In this case, $P_k = P_0$, trivially.
- Induction case (to prove that $P_{k+1} \geq P_0$, assuming, by induction hypothesis, that $P_k \geq P_0$): Let R_k and S_k be R and S after action a_k. Proof by case analysis:
  - Case a_{k+1} is a *hodl* action: Let n be the amount of coins deposited by the user. Then $R_{k+1} = R_k + n = R_k(1 + \frac{n}{R_k})$ and $S_{k+1} = S_k + \frac{n}{P_k} = S_k + \frac{nS_k}{R_k} = S_k(1 + \frac{n}{R_k})$. Therefore, $P_{k+1} = \frac{R_{k+1}}{S_{k+1}} = P_k$.
  - Case a_{k+1} is a *un-hodl* action: Let n be the amount of hodlCoins given back by the user. Then $R_{k+1} = R_k - n(1-\Phi)P_k = R_k - nP_k + n\Phi P_k$ and $S_{k+1} = S_k - n$. Hence, $P_{k+1} = \frac{R_{k+1}}{S_{k+1}} = \frac{R_k - nP_k + n\Phi P_k}{S_k - n} = \frac{R_k}{S_k}\frac{1 - \frac{n}{S_k} + \frac{n\Phi}{S_k}}{1 - \frac{n}{S_k}} = P_k\frac{1 - \frac{n}{S_k} + \frac{n\Phi}{S_k}}{1 - \frac{n}{S_k}}$. Since $n \leq S_k$ and $\Phi > 0$, $\frac{1 - \frac{n}{S_k} + \frac{n\Phi}{S_k}}{1 - \frac{n}{S_k}} > 1$. Therefore, $P_{k+1} > P_k$.

◀

▶ **Theorem 2** (Return On Hodling). *Let b be the amount of coins a user u hodls to obtain h hodlCoins. Let R_0, S_0 be, respectively, the reserve of coins and the circulating supply of hodlCoins at the moment before the user u unhodles their h hodlCoins. Assuming every other user before u unhodles first, then the user u will obtain, by unhodling, a total return of:*

$$\rho = \frac{\frac{R_0}{S_0^{(1-\Phi)}}\left[(1+h)^{(1-\Phi)} - 1\right] - b}{b} \tag{2}$$

Proof. Let $P(t)$ be the price per t-th hodlCoin, indicating how many *coins* will be returned if the user u unhodles their t-th hodlCoin. Considering the amount of h *hodlCoins* the user u has as a continuum, then the total amount of *coins* returned to u is given by the following definite integral:

$$C(h) = \int_0^h P(t)\,dt \tag{3}$$

Let $R(t)$ be the amount of reserve leftover when the t-th hodlCoin is unhodled, then $R(t)$ and $P(t)$ are related in the following way:

$$\frac{dR(t)}{dt} = -P(t) \tag{4}$$

Thus, equation 3 is:

$$\begin{aligned} C(h) &= \int_0^h P(t)\,dt && (5)\\ &= -\int_0^h dR(t) && (6)\\ &= \int_h^0 dR(t) && (7)\\ &= R(0) - R(h) = R_0 - R(h) && (8) \end{aligned}$$

Expressing equation 4 as:

$$\frac{dR(t)}{dt} = -P(t) = -\frac{R(t)(1-\Phi)}{S(t)} \tag{9}$$

Where integration over R(t) and t is done as:

$$\int_{R(0)}^{R(h)} \frac{dR(t)}{R(t)(1-\Phi)} = -\int_0^h \frac{dt}{S(t)} = -\int_0^h \frac{dt}{S(0)-t} \tag{10}$$

Using standard integration techniques the following is obtained:

$$\frac{1}{(1-\Phi)} \ln\left(\frac{R(h)}{R(0)}\right) = \ln\left(\frac{S(0)-h}{S(0)}\right) \tag{11}$$

Thus, isolating for $R(h)$ obtains its equation:

$$R(h) = \left(\frac{S_0 - h}{S_0}\right)^{(1-\Phi)} \tag{12}$$

Which means that $C(h)$ is:

$$C(h) = R_0 - R_0\left(\frac{S_0 - h}{S_0}\right)^{(1-\Phi)} \tag{13}$$

Since it is assumed that the system is initialized with $R, S = 1$, then, by definition, the leftover amount to be claimed is:

$$\mathrm{L}(h) = C(S_0 - 1) - C(S_0 - 1 - h) \tag{14}$$

Where the first term represents removing all hodlCoins in circulation except the initial amount, while the second term represents removing the circulating supply of all users before user u. Therefore, the return on the user u's initially hodled amount b is:

$$\rho = \frac{\mathrm{L}(h) - b}{b} \tag{15}$$

$$= \frac{\frac{R_0}{S_0^{(1-\Phi)}}\left[(1+h)^{(1-\Phi)} - 1\right] - b}{b} \tag{16}$$

◀

5 Implementations

The hodlCoin protocol has been implemented in ErgoScript and deployed on the Ergo blockchain. Interacting directly with the smart contract can be done at `https://hodlcoin.co.in`, while interacting with the same smart contract but via a proxy contract can be done at `https://www.phoenixfi.app`. The Ergo smart contracts can be found at `https://github.com/StabilityNexus/hodlcoin-Ergo-Phoenix`. The source-code for the Ergo website interface, where interaction occurs directly with the smart contract, can be seen at `https://github.com/StabilityNexus/hodlcoin-Ergo-Frontend`.

There is also a Solidity implementation for Ethereum and other EVM-compatible blockchains that can be used at `https://evm.hodlcoin.co.in`. This version can create hodlCoin vaults with any ERC20 token. The solidity smart contracts can be found at `https://github.com/StabilityNexus/hodlCoin-Solidity`. The source code for the EVM website interface is available at `https://github.com/StabilityNexus/hodlCoin-Solidity-WebUI`.

6 Discussion

The hodlCoin protocol can be seen as a **dual** of a Ponzi scheme. Whereas in a Ponzi scheme investors who enter earlier are paid with money from investors who enter later, in the hodlCoin protocol users who exit later are paid with money from users who exit earlier. Furthermore, whereas a ponzi scheme fools investors who are unaware of the scheme's operations, the hodlCoin protocol is **fully transparent**, its rules are clear and users are aware of them. Finally, whereas a Ponzi scheme is unstable and invariably leads to collapse, hodlCoin is conjectured to enjoy a self-stabilizing effect: if the price of the underlying asset is falling and users start to un-hodl to sell the underlying asset, this may encourage other users to hodl to benefit from the fees paid by those who are un-hodling; this may reduce the selling pressure on the underlying asset.

References

1 Joachim Zahnentferner, Dmytro Kaidalov, Jean-Frédéric Etienne, and Javier Díaz. Djed: A formally verified crypto-backed pegged algorithmic stablecoin. Cryptology ePrint Archive, Report 2021/1069, 2021. `https://eprint.iacr.org/2021/1069`.

2 Joachim Zahnentferner, Dmytro Kaidalov, Jean-Frédéric Etienne, and Javier Díaz. Djed: A formally verified crypto-backed pegged autonomous stablecoin. In *IEEE International Conference on Blockchain and Cryptocurrency*, 2023. `https://icbc2023.ieee-icbc.org/program/icbc-2023-final-program`.

A License

B Official hodlCoin Channels

- `https://x.com/hodlCoinStaking`
- `https://discord.gg/7jS9qJNjJv`
- `https://t.me/hodlCoinGame`

[1] `https://creativecommons.org/licenses/by-nc-nd/4.0/`