HodlTree:

The second-generation decentralized lending protocol

Version 1.0

March 2020 /Updated August 2020/

Author

Azamat Malaev
https://hodltree.io/

<u>**Abstract**</u>

The final goal of the HodlTree team is to develop a second-generation decentralized lending protocol where lenders will be able to loan at a higher interest-rate than on the current decentralized lending protocols while borrowers can borrow at zero interest. HoldTree will be fair and trustful creating truly open markets that are not governed by a central authority. The protocol will be based on Ethereum.

Contents

Introduction

The principle of intellectual contracts was described by American cryptographer and programmer Nik Sabo in 1996 long before blockchain appeared. According to Sabo's concept, intellectual contracts are digital protocols for data transmission using mathematical algorithms to perform transactions automatically after accomplishing several conditions and full process control. This definition, which outpaced its time by more than 10 years then, is also accurate nowadays. However, in 1996 the concept couldn't be implemented because of the lack of necessary technologies.

In 2008 the Bitcoin appeared being the first cryptocurrency developed on revolutionary blockchain technology. The blockchain of Bitcoin doesn't enable to specify conditions for transaction performing due to containing only information about the transaction itself. Nonetheless, the advent of technology has become a milestone for smart-contracts development. Five years later, an Ethereum blockchain has enabled to utilize smart-contracts practically.

The volume of funds locked in smart-contracts based on Ethereum amounts to more than 8 billion dollars. More than 50% of locked funds are placed on decentralized lending protocols.

Decentralized lending & borrowing

Decentralized lending

Crypto holders can lend on decentralized lending platforms to earn passive income on their holdings through interest fees paid by borrowers. This is an attractive option for lenders as they can earn relatively low risk interest on their existing holdings without entrusting their private keys to a 3rd party centralized service.

Borrowing

Borrowing allows traders to get leverage which multiplies gains and losses while trading, as well as short selling, a trading strategy which makes money when the price of an asset goes down.

What Is Short Selling?

https://www.investopedia.com/terms/s/shortselling.asp

Advantages of decentralized lending protocols.

- Accessibility to any user all over the word, only a blockchain wallet is needed.
- Absolutely transparent system.
- All transactions are visible in the blockchain.
- No middlemen needed
- Lower commissions due to the absence of middlemen
- Nobody has access to your funds

Disadvantages of decentralized lending protocols.

- During periods of high volatility, transaction fees may rise.
- A risk of hacking in case the contract is deployed with mistakes.

Price oracle failure

The price oracle plays a crucial role in maintaining collateral ratio for each loan as it needs to constantly update the contract with the right price of each asset at all times. Failure to do so might result in the liquidation mechanism not working as intended, which could lead to loss on the lenders' funds.

Existing Work

Compound

Compound is an algorithmic money market protocol on Ethereum that lets users earn interest or borrow assets against collateral. Anyone can supply assets to Compound's liquidity pool and immediately begin earning continuously-compounding interest. Rates adjust automatically based on supply and demand.

Supplied asset balances are represented by cTokens: representations of the underlying asset that earn interest and serve as collateral. Users can borrow up to 50-75% of their cTokens' value, depending on the quality of the underlying asset. Users can add or remove funds at any time, but if their debt becomes undercollateralized, anyone can liquidate; a 5% discount on liquidated assets serves as incentive for liquidators.

The Compound protocol sets aside 10% of interest paid as reserves; the rest goes to suppliers. Compound initially launched on mainnet in September 2018 and upgraded to v2 in May 2019. The protocol now supports BAT, DAI, SAI, ETH, REP, USDC, WBTC, and ZRX. Compound has been audited and formally verified. As of May 2020, Compound has transitioned to community governance; COMP token-holders and their delegates debate, propose, and vote on all changes to Compound.

AAVE

Aave (from the Finnish word for "ghost") is an open source non-custodial protocol on Ethereum for decentralized lending and borrowing. For lenders, the protocol mints ERC20-compliant aTokens at a 1:1 ratio to supplied assets. Interest immediately starts compounding continuously, represented by steady increase in the amount of aTokens held by the lender. This interest stream may be redirected to any address, separately from aTokens that represent the underlying principal.

Users can borrow against most supplied assets; the collateralization ratio and liquidation threshold depend on the asset as does the liquidation penalty, which anyone can get as a bonus for liquidating an unhealthy loan. Interest rates adjust algorithmically based on supply and demand, but Aave lets borrowers opt into and out of (at any time) a stable rate that changes less often. The protocol keeps a liquidity reserve to ensure withdrawal at any time.

Launched in Nov. 2017 as P2P lending project ETHLend and rebranded to Aave in Sept. 2018, the protocol went live on mainnet in Jan. 2020 with 16 supported assets (13 can be used as collateral). Aave's code has undergone two external security audits, and Aave maintains a bug bounty program.
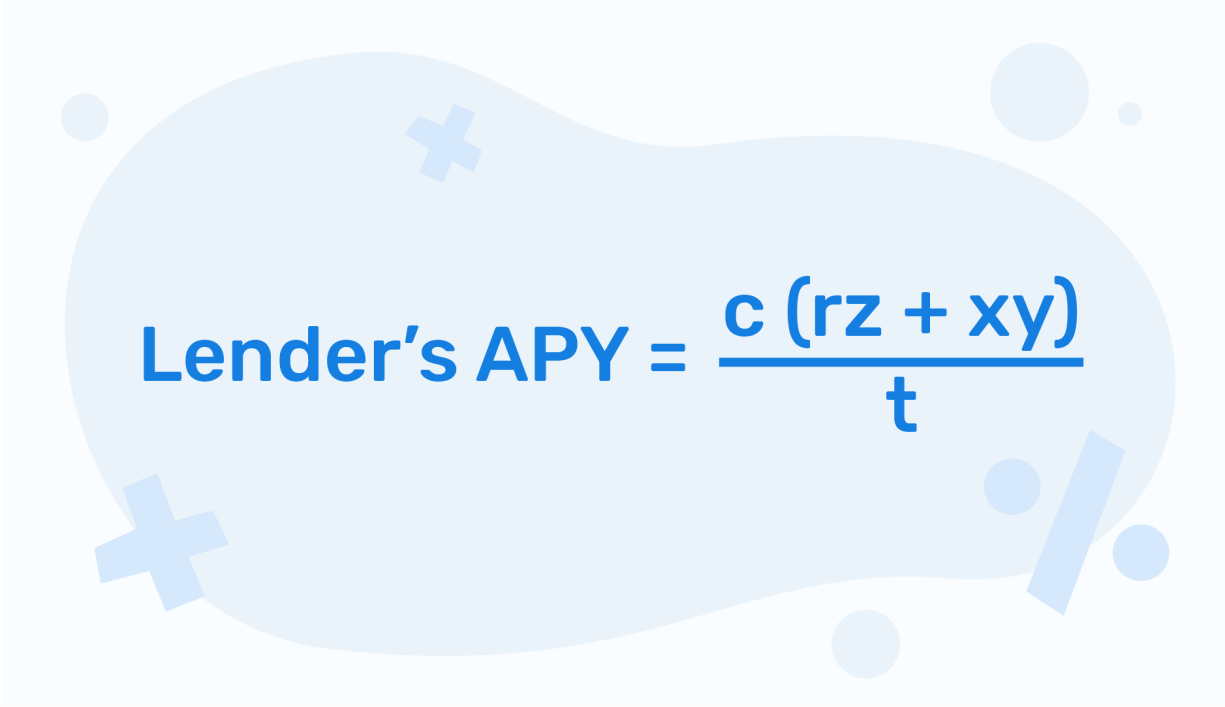
Overall architecture
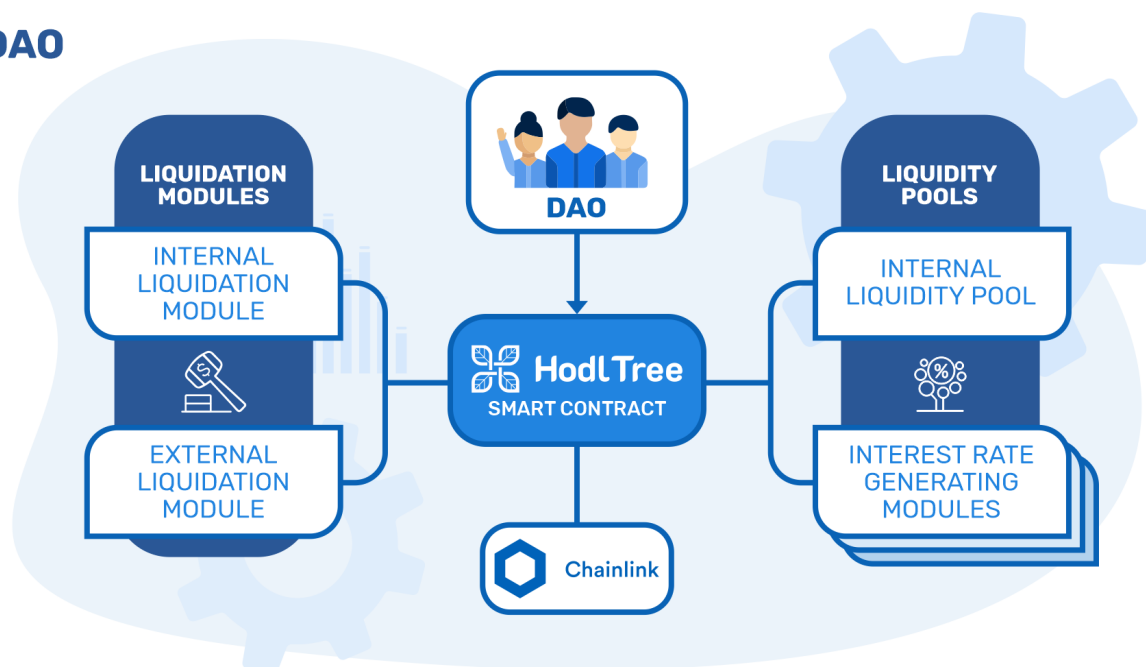
Existing decentralized lending protocols offer low rates for lenders of the cryptocurrency basing on not-so-optimal collateral management scheme. The HodlTree protocol will improve the current architecture and let lenders get much more attractive interest-rates while borrowers will borrow at zero interest.

For this goal the HodlTree will use the following scheme of collaterals placement. 80% of borrowers' collaterals will be placed in interest rates generating modules while the other 20% will be saved as a backup pool for immediate usage. Also, 80% of lenders' placed funds will be set in Interest rates generating modules, the other 20% will be saved as a backup pool for immediate lending.

The calculation of rates is listed as follows:

$$\text{Lender's APY} = \frac{c\,(rz + xy)}{t}$$

For lenders

X = a total number of funds in borrowers' collateral (of the certain coin)
C = collateral ratio placed in interest generating modules
Y = the rate in the interest rates generating module (of the certain coin)
Z = a total number of unused funds in lenders' collateral (of the certain coin)
R = the rate in the interest rates generating module (of the certain coin)
T = total lenders capital

A simplified example of the rate calculation:

Price of 1 ETH - 100
Alice placed 1 ETH for the lending
Bob borrowed 1 ETH on collateral of 200 DAI
The rate in the module of interest-earning (DAI) - 10% annually
The rate in the module of interest-earning (ETH) - 1% annually
Total number of funds in borrowers' collateral - 200
Total number of funds in lenders' collateral - 0
Collateral ratio - 0.8

(200*0.8*0.1+0*0.8*0.01)/100=0.16
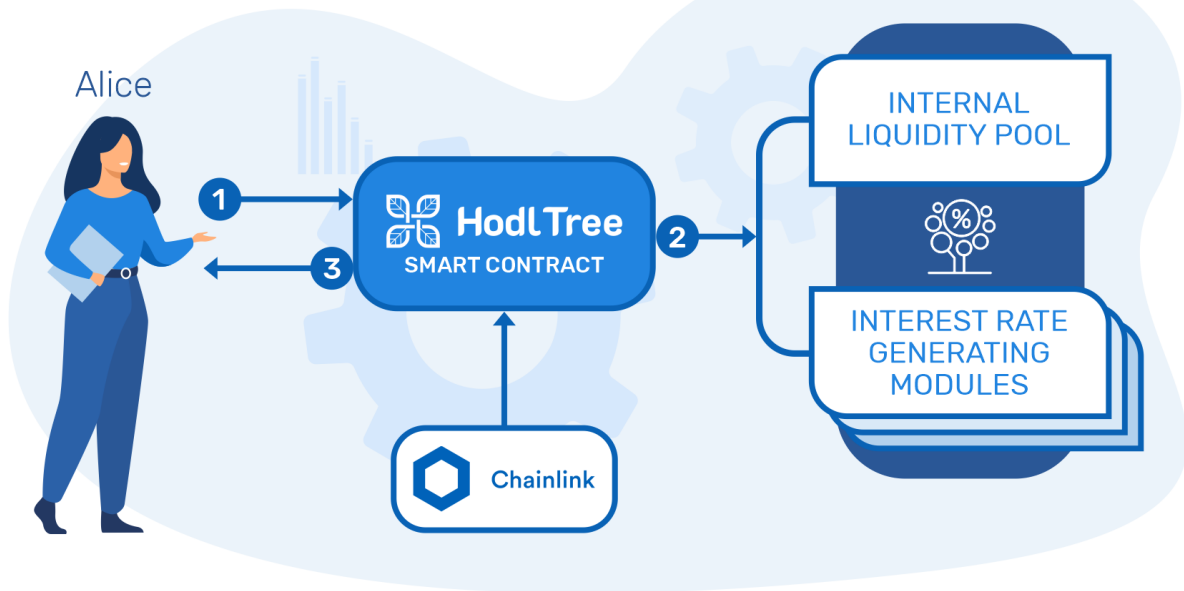
For Alice APY will account 16% APY
For Bob the borrowing cost will be 0.

Funds set on the HodlTree protocol will be presented as ERC20 tokens hTokens.
With interests accrued price of hTokens will increase.
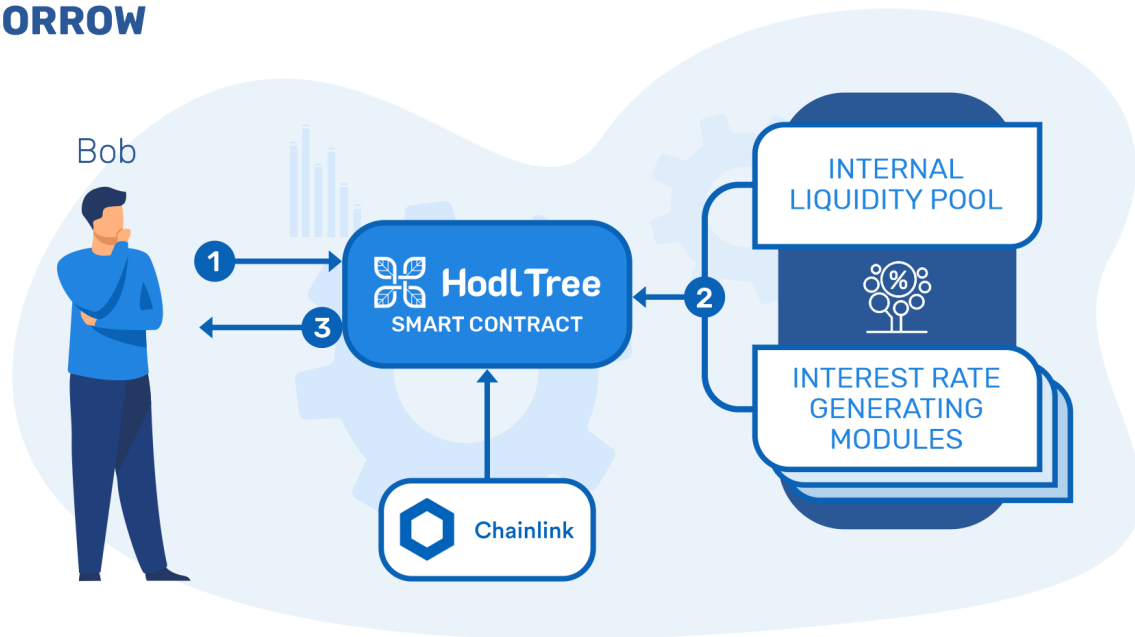hTokens can be exchanged at any moment on their collateral.

LENDING

SIMPLIFIED LENDING SCHEME

Lending

1. Alice places ETH on a smart contract to earn interest.
2. Smart-contract divides funds into 2 parts, 20% of funds set in the internal liquidity pool, other 80% - in the interest rates generating modules.
3. Smart-contract mints and sends hTokens to Alice.

BORROW

SIMPLIFIED BORROW SCHEME

Borrowing

1. Bob sends collateral (DAI) onto the smart-contract to borrow ETH.
2. Smart-contract mints hDai and locks it on the protocol, afterward 20% of Bob's collateral setting in the internal liquidity pool (DAI) and the other 80% in the Interest rates generating module (DAI).
3. Smart-contract sends ETH to Bob from the internal liquidity pool (ETH) or from the Interest rates generating module (ETH), in case there is a lack of ETH in the first one.

LIQUIDATION
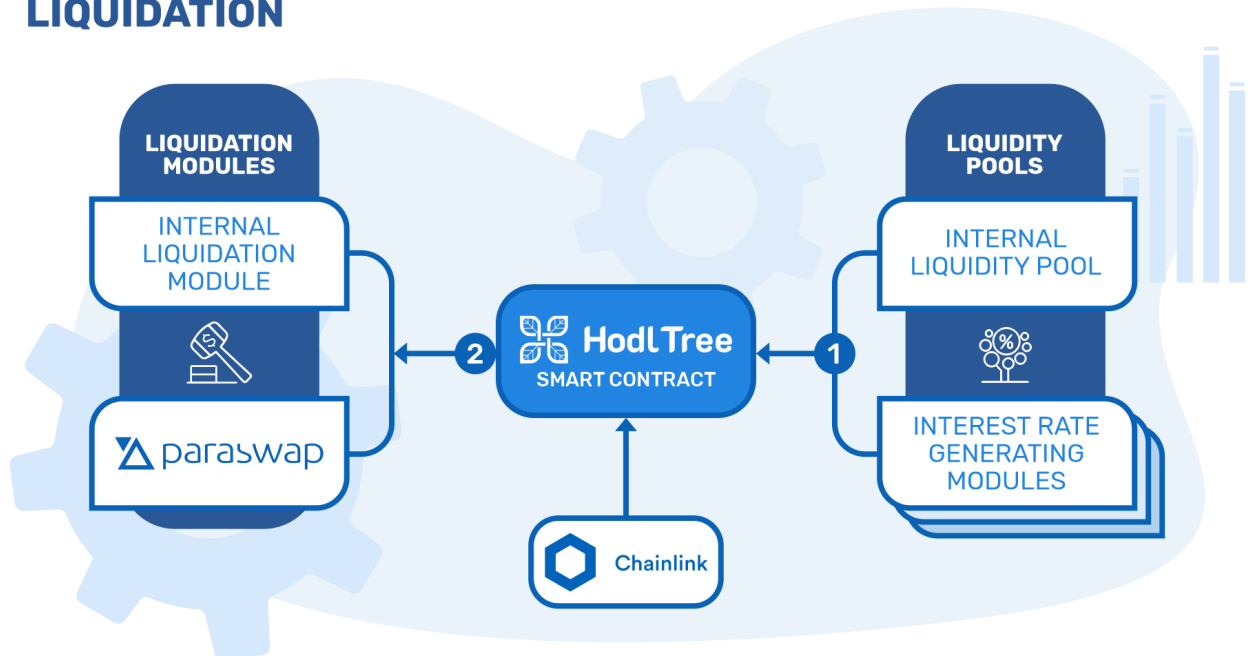
SIMPLIFIED LIQUIDATION SCHEME

Liquidation

hTokens will be utilized as collateral to borrow from the protocol. Every market will have a collateral factor from 0 to 0.8 which will represent a portion of the underlying asset value that can be borrowed. Total sum of an account's underlying token balances, multiplied by the collateral factor will be equal to user's borrowing capacity.

If number of borrowed funds exceeds user's borrowing capacity, the protocol will initialize liquidation procedure. The loan will be liquidated with a discount from the current price to attract arbitrageurs. If it's not enough, the protocol will start liquidation procedure by itself with the use of the decentralized aggregator Paraswap.

Any user that possesses the borrowed asset can take part in liquidation. All funds left after liquidation will be available to Borrower for withdrawal.

Interest rates generating modules

To earn on unused funds the HoldTree protocol will place free funds on interest rates generating modules.

Both existing decentralized protocols such as Compound, AABE, dYdX, Uniswap, Balancer Pools and independently developed decentralized structured products enabling to earn interests can act as interest rates generating modules.

Individual Interest rates generating modules will be developed for each asset

To add new Interest rates generating modules voting will be carried out. In case of positive decision and after a security audit, a new module will be integrated into the protocol. In the protocol there will also be an option to switch Interest rates generating modules off.

What is a structured product

A structured product, also known as a market-linked investment, is a pre-packaged structured finance investment strategy based on a single security, a basket of securities, options, indices, commodities, debt issuance or foreign currencies, and to a lesser extent, derivatives.

https://www.investopedia.com/articles/optioninvestor/07/structured_products.asp

Oracle

The reliable source of prices is crucial to ensure stability of the collateral and liquidation modules. It is broken down into two important tasks: calculating the value of collateral when issuing loans and monitoring off-chain prices for timely execution of liquidations in case of insufficient collateral.

Given that price action for cryptocurrency markets takes place across many different centralized and decentralized exchanges, an oracle is required to connect off-chain and retrieve aggregated price data that takes into account marketwide price discovery. We have selected Chainlink's Price Reference Data as the oracle mechanism to power HodlTree. It provides us with several guarantees:

- Accurate price data that reflects volume adjusted market coverage across all trading environments
- High availability and tamper-resistance delivery of data via its decentralized network architecture made up of secure node operators
- Time-tested reliability that currently secures around billion dollars in value for many leading DeFi applications.

Importantly, Chainlink's Price Reference Data includes numerous price oracles already on mainnet and an established framework for building new ones that we can use to launch additional collateral types on HodlTree quickly. This will allow us to scale up rapidly to support a large selection of assets for lending & borrowing, as the backend oracle development work is already done and proven to be reliable.

DAO

Governance management

HodlTree token holders will be able to vote for parameters change.
To put a proposal for voting 3% of total tokens are needed.

What parameters token holders can change:

- What share of lenders' funds to place on the Interest rates generating modules (separately for each token)
- What share of borrowers' funds to place on the Interest rates generating modules (separately for each token)
- Adding new features.
- New tokens adding to the protocol.
- Change of the collateral factor (separately for each coin).
- Adding and deleting interest rates generating modules.
- The distribution between interest rates generating modules.

At least 20% of all holders have to vote for proposal acceptance
Each HodlTree token is equal to one vote.

There will be a temporary lag between decision making and a new version running.

Summary

HoldTree will develop the second-generation decentralized lending protocol with significantly improved interest rates.

HoldTree will be formed as a DAO where users can manage the protocol.

- Lenders will be able to get much more attractive interest-rates for their tokens
- Borrowers will be able to borrow tokens at 0 interest using stable coins as the collateral.

References:

[1] Investopedia.com
[2] Compound.finance
[3] Defipulse.com
[4] Chain.link
[5] Paraswap.io