HOdlcoin –
A Cryptocurrency With A Nominal Interest Rate

FreeTrade
freetrade@hodlcoin.com
hodlcoin.com

Abstract. HOdlcoin extends Satoshi Nakamoto's Bitcoin with a number of improvements, most notably the introduction of an automatic 5% nominal interest rate on recent transaction outputs and a sliding range of nominal interest rates up to 9.9% on transaction outputs that are time locked for durations of between 2 and 365 days. Other improvements include a proof-of-work function designed to be friendly to consumer grade hardware, a minimum transaction fee as a spam control measure, destruction of 50% of transaction fees as an inflation control and expiring small transaction outputs to reduce the memory requirements for network nodes.

1. Introduction.

HOdlcoin is Bitcoin[1] type cryptocurrency with an added nominal interest rate. While capital increase measured in another currency cannot be guaranteed, the interest payments of HOdlcoin come from monetary supply and thus are guaranteed by the blockchain. The interest rate is set at 5% to model a historically average rate of interest.[2]

2. Interest calculation

Casual balances attract interest for a 30 day period, but the APR can be calculated as follows. With a target of 204,765 blocks per year, with an interest rate of (1/2^22)% per block, it gives an overall Annual Percentage Rate (APR) of 5%.

$$APR=\left(\left(1+\frac{1}{2^{22}}\right)^{204765}-1\right)\times 100\approx 5.00311$$

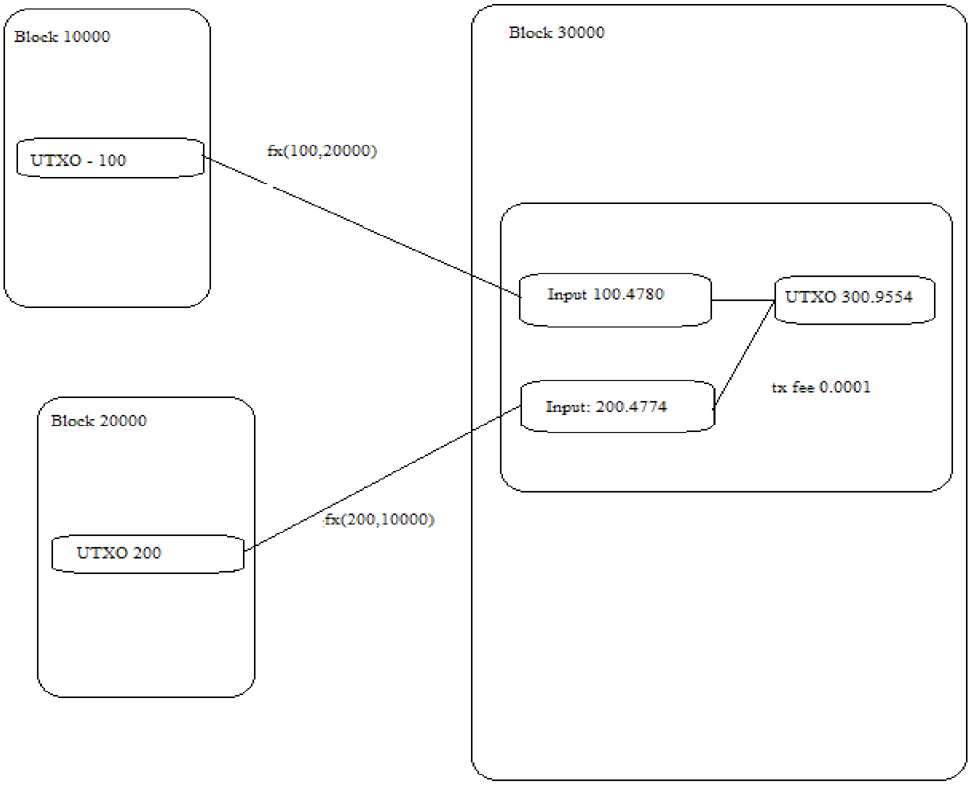
3. Transactions

Interest is calculated when a UTXO is spent as an input to a new transaction. The value of the input is calculated as compound interest on every block between the unspent output and the new input with a function

$$duration = CHAINHEIGHT_{OUTPUT} - CHAINHEIGHT_{INPUT}$$

$$interest = f(Amount, duration)$$

Contrary to the 'staking' approach, HOdlcoin funds do not need to be in a 'hot' wallet and interest calculations only take place once, minimizing resources needed to keep track of interest payments. Consider this example transaction.



4. Interest Rate Lookup Table

Compounding interest is usually handled with a Math.pow floating point style function. However this creates difficulties in the context of blockchain verification across different platforms. Exponential functions can create different results on different platforms. These differences are tiny but even a tiny difference can cause some nodes to validate a transaction, and others to reject it, causing a catastophic chain fork. To avoid this only integer mathematics can be used. These calculations can be time consuming over many transactions but a lookup table can be created at the outset so that a large volume of transactions can be handled.

5. Time deposit bonus

Savers can further be incentivized by offering incentives to tranactions using the Check Lock Time Verification (CLTV)[3] operation code. This code prevents an output from being used until a specific point in the future. By encouraging savers, or even the sender, to attach this code, funds become time locked and this prevents large amounts of the currency from flooding the market in a panic. The bonus amount is designed to encourage longer locking times over shorter locking times

$$duration = CHAINHEIGHT_{OUTPUT} - CHAINHEIGHT_{INPUT}$$

$$Bonus\ Multiplier = (1 - ((409530 - duration)/409530)^{6})$$

6. Bonus Interest

Risky currencies attract deposits by raising interest rates. Similarly, bonus rates can be paid in the initial stages of the currency to attract depositers willing to hold and time deposit their coins. Again the calculations can be handled in a similar way to regular interest rates using integer mathematics and a precomputed table.

7. Proof Of Work

While Bitcoin's Proof of Work function can be optimally run on specialized hardware known as ASICs, HOdlcoin's Proof of Work is a Pattern Search function designed to be amenable to commodity hardware. This is to encourage participation and adoption by a widespread user base.

Pattern Search involves filling up RAM with pseudo-random data, and then conducting a search for the start location of an AES encrypted data pattern in that data. Pattern Search is an evolution of the ProtoShares Momentum PoW[4], first used in MemoryCoin[5] and later modified for use in CryptoNight(Monero,Bytecoin), Ethash(Ethereum). The POW Algorithm is considered a technical detail and is subject to change to favor CPU and consumer grade hardware with the intention of keeping mining participatory and distributed.

8. Minimum Transaction Fee

A number of types of attack can be targetted on a blockchain with large blocks and low transactions fees. An attacker can make it costly to run nodes by creating millions of junk transactions all requiring indefinite storage. Also users may see the network as a near-free data storage service, filling it up with data of no use to most network participants with much the same results for nodes.

To prevent this, a minimum transaction fee of $0.01 will be applied to an average sized transaction. It will therefore be costly for an attacker who wishes to create large blocks that need to be stored by network nodes. As miners can avoid transaction fees by creating blocks and thereby keeping all transactions fees, 50% of transaction fees will be required to be destroyed so that an attacker cannot spam simply by becoming a miner.

Destroying 50% of transaction fees has the added beneficial effect of introducing a deflationary pressure. This will counter the inflationary pressure of the interest payments and block subsidies.

The amount of HOdl required to cover a cost of $0.01 is approximated by using the current network difficulty. Only transactions including a fee of at least this approximation will be valid. A maximum minimum of 0.05 HDL will apply to avoid prohibitively large transaction fees if the coin has a low market value.

Operating at full capacity, with 561 32MB blocks each day with minimum fees on all transactions will create $250 million in transaction fees each year. Half of this is destroyed. This deflation of the money supply is sufficient to offset an inflation rate of 7.5% on a $1.7 billion dollar capital value.[6]

9. Expiring transactions

Currently over 50% of Unspent Transaction Outputs (UTXOs) on the Bitcoin blockchain have balances of less than .001 BTC, and represent only .01% of the total coins[7]. Many of these balances are abandoned, and a disproportionate use of resources is required to support them. By expiring these kind of outputs after a reasonable amount of time, we can avoid a similar situation arising with HOdlcoin. UTXOs will thus be considered expired with the following schedule.

After 2 years outputs of .00000099 HODL and below are expired
After 3 years outputs of .00000999 HODL and below are expired
After 4 years outputs of .00009999 HODL and below are expired
After 5 years outputs of .00099999 HODL and below are expired

The expiry test will not take interest earned into account, so a .00009999 balance that has earned .00000005 will still be treated as a .00009999 balance and expired after 4 years. Blocks containing transactions referencing UTXOs that are expired will not be considered valid by nodes.[8]

By expiring small UTXOs, we significantly reduce the memory and database resources to run a node.

References

[1] Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.com/bitcoin.pdf

[2] Tejvan Pettinger, Historical Interest Rates UK, https://www.economicshelp.org/blog/1485/interest-rates/historical-real-interest-rate/

[3] Peter Todd, BIP 65, https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki

[4] Daniel Larimer, MOMENTUM - A MEMORY-HARD PROOF-OF-WORK VIA FINDING BIRTHDAY COLLISIONS, https://bitshares.org/media/archive/pts/whitepaper/MomentumProofOfWork.pdf

[5] FreeTrade, Memorycoin 2.0 Proof of Work, https://bitcointalk.org/index.php?topic=355532.0

[6] FreeTrade, HIP001, https://medium.com/@freetrade68/hodlcoin-improvement-proposal-001-a802f9948d68

[7] Bitinfocharts, https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

[8] FreeTrade, HIP002, https://medium.com/@freetrade68/hodlcoin-improvement-proposal-002-adf802d2ccb7