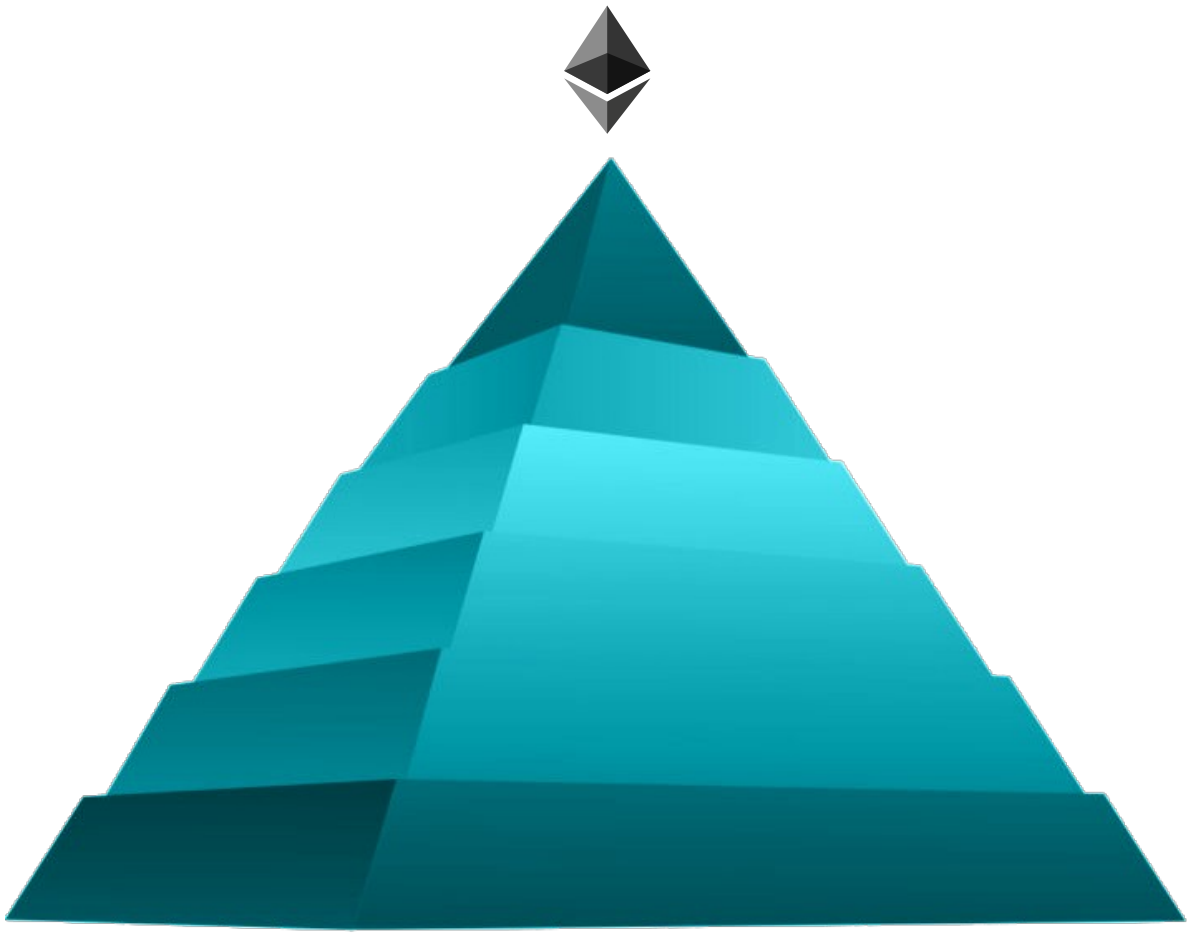
pyramid
game
.eth

white paper, draft 0.92



unstoppable lottery

Table of contents

Prelog

The idea behind this project is to create a digital life-form, an abstract being, that is completely self-sufficient.

The choice for the natural habitat of this creature fell on the blockchain, as this makes it easy to solve a major problem of a digital life-form: its dependency on the underlying hardware. The blockchain is kept alive by actively paying for itself from transaction fees of it's users. No users, no transaction fees, nobody wants to run hardware for it, hence no public blockchain.
The creature is said to be alive as long as it actively reduces entropy, or in terms of the blockchain, is generating transactions. This guarantees it's survival, as it needs to care for transactions so the underlying hardware it lives on is being paid in the real world and hence keep the habitat existing.

Biology

The biology of this digital creature is to feed from greed of people: a resource abundantly available in the crypto space. But it should not be a parasite or something the people it is feeding from want to get rid of like a virus. People should like it, it should be fun, so both can live in perfect symbiosis forever, like an addiction. Those thoughts led to the conclusion to represent the creature as a casino style game that people want to play over and over again to win more than they invested: a mechanic that has proven to be efficient and is so potent that it is heavily regulated, everywhere.

Growth

For the ability to grow it is required that the creature cares for a growing number of blockchain transactions. The need for wide player base is important for its survival as a player could stop playing anytime and the game needs to be introduced to new people before they stop playing. The ideal game design targets the incentive of players to attract new players. One conclusion to this is to use mechanics of some sort of a Ponzi scheme.

Abstract

The described game is a mixture of a Ponzi style pyramid scheme and a lottery. It is designed to have a constant incentive to play, no matter what state the game is in. The game restarts when one player wins, to keep it interesting and to play again until eternity.

What the crypto market wants.

Crypto is not just about financial profits. But then it mostly is, and pyramid schemes tend to be popular in the crypto community: get in early, get out before it collapses, pump and dump. This project targets nothing else. It even promises exactly the Ponzi Scheme it’s based on.

It’s an artsy project.

The Pyramid Game is digital artwork and displays the purest form of modern capitalism by a working scheme that mimics by definition it’s very purpose. All just to give life to the abstract being described above.

Nobody can pull the plugs.

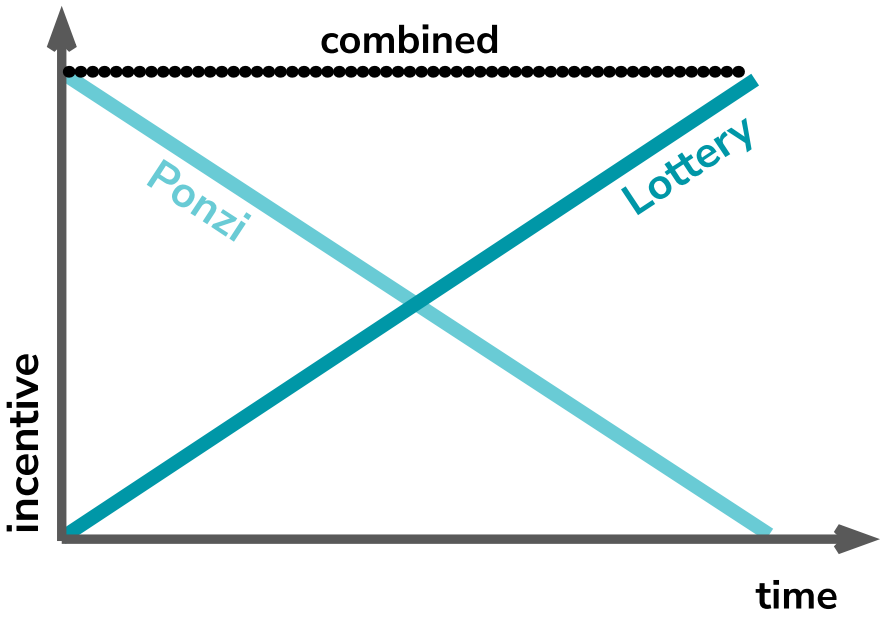
The whole project is completely decentralized and a DAO contract owns all involved contracts. All deployed source code is open source. The web3 front-end is only accessible via IPFS, found in the ENS record of the project.

Nobody is responsible.

Everything is deployed completely anonymously and comes with no promises for further upgrades or plans to expand etc. The DAO is governed by an NFT that comes as 20 Gods with more power and a growing number of Pharaohs (see below). The website provides an on-chain chat for a truly decentralized interaction among players.

Constant incentive to play

The Pyramid Game uses two incentives that together offer a constant lucrativity for a player to play. The idea is, that first one very strong incentive is there that gets less strong over time, and proportionally a second incentive starts getting stronger, so on average it’s constant and the game never loses its drive.



The two chosen incentives to play, that fit above criteria are:

- a pyramid scheme that starts very lucrative and looses traction over time
- a lottery of all the invested tokens, which gets better over time

Pyramid Scheme: The first one wins.

The base concept of pyramid schemes is that participants that enter earlier in the scheme, profit from the payments of the later ones.
The beauty about this type of game is that is self-sufficient in regard of marketing, as the only win condition for players to convince new other players to start playing.

Additionally, the higher up in the pyramid a player is, or the earlier a player entered the pyramid, he makes more profits than the ones below. This is important for a pyramid game to start quick traction, as it has big profit potential for the early ones.
And this is exactly what the Pyramid Game needs, a mechanics that has very strong incentive to play, early on.

In the Pyramid Game, a virtual pyramid is built by players placing blocks (represented by the in-game currency BL0x). The pyramid is formed by projecting a pyramid with levels twice the size of the previous, onto the currently bet BL0x. The pyramid starts on level 1 with 1 BL0x, continues with 2 BL0x on level 2, 4 on L3,... 2^N on L_N.

Each player earns a multiple of his bets, based on levels the pyramid has grown after the placed BL0x. For each additional level, the player gets his BL0x back.

As the game is designed in cycles, where the pyramid collapses after a time and afterwards a new Pyramid arises. (see below) The profits for each pyramid cycle can be collected after the collapse, when the end result is known.

Lottery: The last one wins.

A lottery is a game type where money is collected from all players and then redistributed among some winning players. The more is in the pot, the more will the winner multiply his investment.
So this type of game is specially lucrative to play when there is already money in the pot but makes it especially hard to start them as there is nothing to win yet. But this exactly the needed mechanics to serve as the second incentive, as it gets better over time, where the pyramid schemes becomes weaker.

Normally the profits are paid out after the game. But as the pyramid scheme of the first incentive would suffer from a fixed game time length, the lottery was designed so each buy-in into the game can win the pot by a known dynamic probability, at all the time. This probability is the key point of the lottery game, and is adjusted to reflect the current expected value and also the popularity of the game, so the game never stops being active. (see below)

As soon as someone wins the Jackpot, the pyramid collapses and a new one is formed. The winner of the Jackpot wins additionally the first BL0x of the new pyramid, on Level 1. He becomes so to say the Pharaoh of the new Pyramid. To express this, the winner can mint an NFT and profit from future eternal payouts from the DAO.

Dynamic collapse probability

When the sales stall and the pyramid scheme cools down as it’s not lucrative to enter anymore, the pyramid may literally collapse.

The changes for this to happen are known and are increasing with time. As anybody can be the last person to collapse the current pyramid by minting another BL0x, this will potentially boost the sales again where it starts being lucrative again to mint etc.

When the pyramid starts, it should not collapse right away and the chance for this to happen starts at zero. After this generally speaking, with each additional BL0x this chance raises, until to the point where the expected value of the pyramid game is equal to the expected value from the lottery game. From this point, the probability tends equalize the expected value from chance * pot size to meet the buy-in price, and raises when nobody plays.

To balance the transition between pyramid scheme and lottery the probability for the pyramid to collapse it adjusted dynamically depending on various parameters that can be setup before each game by the DAO.

A simple way to describe the probability calculation: When there is less activity the probability rises over time, when there is a lot of demand it decreases. And as the pyramid grows, the probability calculation is adjusted to the expected return for collapsing the pyramid.

(For more details, see technical implementations below.)

Gameplay

Mint BL0x

There exists one current pyramid. At any time players can place a block (= BL0x) on the lowest current level. Each buy-in of 1 BL0x has the same price. The level capacity doubles with each additional level.

The collapse of the Pyramid

A pyramid scheme can’t grow forever and once needs to collapse. Each buy-in has a dynamic probability for the pyramid to collapse and win the Jackpot, the root BL0x of the next pyramid and a Pharaoh NFT.

The chance of a collapse depends on several factors like game activity, pyramid size and configuration.

Our implementation of random values need some future blocks to be calculated. So the player needs to wait about a minute to see the result of his bet. When collapsed, a new pyramid is created.

Collect payback

Each buy-in receives a payback, depending on which level the BL0x got placed and at what level the pyramid collapsed. This is the classic pyramid scheme, the earlier a player entered the game, the higher the payback.

payback bonus = grown levels * BL0x price

A BL0x starts getting payouts as soon as the pyramid levels up. From there on it will gradually get gains from later levels, one full buy-in back per full level and a percentage of the last started level proportional to how much it’s filled up.

As an example, the player placed BL0x on on level 5 and the pyramid collapsed at exactly at the middle of level 10, he will get back 4.5x his investment as payback that can be collected after the pyramid collapsed.

Tokenomics

BL0x token

The Pyramid Game consists of a single token: the BL0x. They can be placed in the current pyramid and after payout or win, the tokens can be transferred to other accounts like any other ERC20 tokens. Also they can be bet again on another Pyramid later.
BL0x tokens can be minted for a fixed ETH price and can be swapped back to ETH without any fees, apart from gas.

Minting / Burning

The only way to mint BL0x tokens is to buy blocks in the pyramid. This make it a special good for any token fetish wallet. The amount of BL0x existing at any moment * the current BL0x price is equal to the reserves of ETH the pyramid contract possesses. If ETH are withdrawn, the corresponding amount of BL0x tokens is burned.

Pyramid collapse / Jackpot

A part from all buy-ins flow into a Jackpot that is won by the player who collapses the pyramid. In the first pyramid this is 10%, in later games this value can be changed by the DAO.

Payback

After the pyramid collapses, each placed BL0x receives a payback, depending on the level of the BL0x and the pyramid size. The total value of all paybacks is:

All buy-ins - Jackpot amount – DAO/Game rigging prevention

Game rigging prevention

A small cut must be deducted from paybacks and not paid back to the players to prevent whales from buying all available BL0x which leads to a 100% collapse of the pyramid and can be used to take advantage of the other players. To de-incentivize this behavior, a cut from all invested coins are credited to the DAO.

DAO membership

Each DAO member (owners of NFTs) have access to a share of the DAO funds. (see more below)

Fixed ETH value per account

BL0x token price in ETH can be changed by the DAO (for each pyramid), but the accounts BL0x balances are adjusted appropriately (rebasing token), so that the token balance of an account can be changed back to the same amount of ETH at any time.

Player’s balance

For comfort BL0x tokens are ERC20 compatible. The balance is the sum of stored tokens and the paybacks of the last played pyramid.
To check how much a player won, a simple wallet reload is enough, no need to check back on the website. As soon as the wallet balance updates, the pyramid has collapsed and the payback is available for transfer, payout to Ether or bet again into the new pyramid.

Technical implementation details

You can find all verified and carefully documented source-code in the corresponding block explorer on each deployed chain.

General remarks

- Only one pyramid can be played at the same time (on the same chain)
- Pyramid can only collapse when BL0x are minted
- Payouts from previous pyramids can be accessed forever

Public contract interactions

Mint

Placing a BL0x on the current pyramid is the players basic action to play. Multiple BL0x can be placed at the same time, for a higher collapse probability. This is done by sending BL0x or sending ETH to the contract.

Collapse

After the random calculation timeout, the decision about the collapse is available and can be executed by anyone. The winner will be the player who caused the collapsed, no matter who is executing it on the blockchain.

Payout

BL0x can be swapped back to ETH at the time, as soon as they are available as balance, no matter if won from Jackpot, Payback or via transfer from another account. (ETH or native Blockchain Token for other Blockchains).

Blockchain Randomness

A source of randomness is used each time after a mint to decide if the pyramid collapses. A configurable number of block hashes after the mint has taken place are analyzed and if one of them is below a value which corresponds to the calculated probability, the pyramid is in a collapsible state.

For each mint a PendingBuilds entry is stored to be able to check the hashes when enough blocks where produced by the blockchain.

```
struct PendingBuilds {
  address addr;                // bl0x owner
  uint16 bl0xCount;            // how many bl0x where minted
  uint80 blockNum;             // block number when minted (uint80 sufficient)
  uint256 collapseMinHash; // one hash must be < for collapse
}
```

Because of block hashes only being accessible during 256 blocks from the smart contract there is a limited time to collapse the pyramid. If the pyramid is not collapsed after that time, the collapsible state is being discarded and the game continues.

This design of randomness is not perfect and has the following (controllable) issues:

Attacker trying to prevent the pyramid from collapsing

- After one of the block hashes in the chain causes the pyramid to be in a collapsible state, a miner can try to create a longer chain and the (critical) block hash would be discarded.

Attacker trying to collapse the pyramid

- A miner can decide to mine many blocks and increase his chance to collapse the pyramid for each valid block mined, which is very hard / expensive because multiple blocks are used and so the probability value is much lower.

Both of the described attacks need a significant amount of hash power to be successful and have only limited probability to succeed. For the amounts that are possibly at stake the design is strong enough to discourage this unwanted behavior.

The DAO configurable value **randomBlocks** (how many block-hashes are used to decide if a pyramid collapses or not) can be increased to lower the risk of these randomness attacks or decreased to speed up the game if the additional security is not needed (depending on the chain used, centralization risks, etc.)

In addition the DAO can adapt the bl0xPrice and expected target pyramid level to prevent those attacks if necessary and keep the game in a safe size.

ERC-20 Compatibility

The whole Pyramid Game is implemented as a ERC-20 Token. The balance is calculated from the tokens payed out after a pyramid collapses and can be directly used for transactions.

The game can be played (almost) entirely from the wallet:

- Send ETH to contract to buy BL0x on current level (use sufficient amount of gas as it is not a normal transfer)
- Wait for the pyramid to collapse and your bonus payment will be automatically appear as BL0x in your Wallet

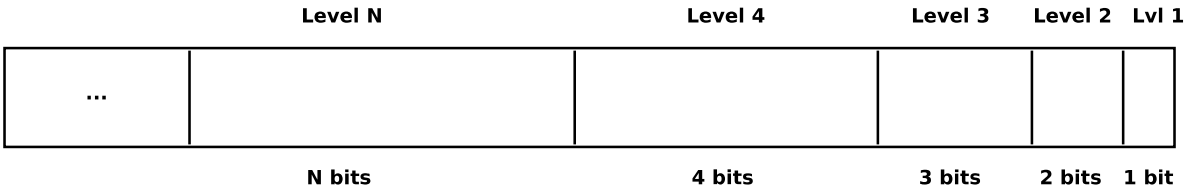
To cash-out BL0x to ETH or to enter a new pyramid with your BL0x balance you need to call a smart contract method or obviously use the dApp.

BL0x tokens can be sent to any address or be traded like any other ERC-20 Token.

The Accounting Field

To optimize the storage of each players account, a simple **uint256** is used to store all investments. This enables the representation of a players bets on 21 levels, which is far more than ever needed (Yes, Bill G. said..), as it stores balances for Pyramids of up to 2^21 BL0x purchased. Quite a massive thing that probably will collapse much earlier.

As each level doubles in size, the storage layout is as follows:
The first bit is used to express the bets on level 1, the next two bits for level 2, the next 3 bits for level 3, up to N bits for level N, where sum(1-N) < 256, which results in N < 22.



Governed by the All-Seeing-Eye DAO

The Game and the NFT contract, as well as the ENS domain *pyramidgame.eth* are owned by the PyramidDAO. In its first version it is a simple contract which allows to change the game parameters, website content and pass the ownership to a new DAO implementation based on democratic decisions between the God NFT holders.

Pyramid Settings

There are few but powerful configuration values which decide on the speed, price, security and other characteristics of each pyramid. God NFT holders can propose new config values and vote on those proposals.

uint64 **payoutFactorX64**

Factor of all pyramid BL0x which are reserved for the jackpot winner / collapser.

uint64 **ownerFactorX64**

Factor of all pyramid BL0x which are reserved for the DAO and are divided between the GOD and PHARAOH NFT owners.

uint64 **probGrowthPerSecondX64**

This value is multiplied with the base probability and added to the current probability each second. It defines how fast the probability can reach 100% or any high percentage which ends the game if anyone mints a BL0x and collapses the pyramid.

uint64 **probShrinkPerMintX64**

This value is multiplied with the current probability for each mint, which decreases the probability for the next mint.

uint128 **bl0xPrice**

Price of a BL0x in wei.

uint32 **probStartBl0x**

BL0x number where the base probability starts being the fair probability considering the price of BL0x and the probability of collapsing the pyramid.

uint8 **randomBlocks**

Number of block hashes used for the probability calculation. Must be a value between 1 and 128 and must be a power of 2.

ENS contenthash changes

The only way to change the content hash of the *pyramidgame.eth* domain (the content of the website) is by a DAO vote.

Pyramid / NFT / ENS Owner

The only way the owner of the Pyramid contract, NFT contract and ENS domain can be changed is by a DAO vote. This can be the future path to a more complete DAO implementation.

Important:
The funds of the current DAO CANNOT be moved NEVER and will be available for NFT holders to withdraw also when the DAO is changed to a new implementation.

Governance Parameters

A minimal time of 12 hours is needed before a proposal with absolute majority (min 11/20 votes in favor) can be executed. After 24 hours a relative majority (more yes than no votes) can execute a proposal. If it is not executed after 48 hours proposals are discarded.

On-chain Live Chat

To connect players in the current game the DAO provides an on-chain live chat. It’s featured on the website and can be accessed by anyone. It only needs a small amount of gas for the transaction.

Owners of Pharaoh and God NFTs can send messages that are displayed in different colors.

Owners of God NFTs can send messages which are directly relayed to the Pyramid Game Twitter account by adding the @twitter keyword to their in-game chat messages.

PyramidGame NFTs

The Gods

20 God NFTs exist who rule the pyramid game, each one representing a god of ancient egypt. Gods are NFT TokenIDs 1-20.

Using the DAO, Gods can propose new game configuration parameters for the next pyramid, change the IPFS contenthash for the *pyramidgame.eth* website or even promote a new implementation of the DAO contract.

The Genesis Pharaohs

Before the game is launched, 420 GENESIS Pharaoh NFTs will be sold on the project webpage. Genesis Pharaohs are NFT TokenIDs 21- (max. 440) and have the same rights as normal Pharaoh NFTs.

The number X how many genesis pharaohs are minted during presale, determines the share of the DAO profits which all pharaohs receive each game.

Pharaoh Gain Percentage = 70 * (X / 420)

In the special case that ALL 420 Genesis Pharaohs are minted, a 10% extra percentage is given to the Pharaohs, so they keep a total of 80% of all DAO profits.

Genesis Pharaohs can ONLY be minted during the presale period.

For each collapsed pyramid each minted Genesis Pharaoh receives an equal share which will be shared with a slowly growing number of pharaohs (see below).

Genesis Pharaoh NFTs do not have voting rights in the DAO (for now)

The Pharaohs

Each winner of the Jackpot becomes the Pharaoh of the next pyramid and can exclusively mint 1 Pharaoh NFT of his pyramid. Pharaohs are NFT TokenIDs beginning from the last minted Genesis Pharaoh ID + 1.

A Pharaoh receives a part of profits payouts (from all completed pyramids after he was minted).

Pharaoh NFTs do not have voting rights in the DAO (for now)

Revenue Pyramid Profits

DAO profits are distributed between 20 Gods and all minted Pharaohs. The amount of Genesis Pharaohs minted during presale, defines how profits are split between Gods and Pharaohs. (see Genesis Pharaoh section)

The profits can be claimed at any time for all eternity by the account owning the specific NFT(s) on pyramidgame.eth or calling the Pyramid DAO contract directly.

Not Promised Roadmap

As described above there is no promised roadmap or coming updates like in many other projects. The PyramidGame comes as it is and only maybe there will be new things coming to it, like:

DAO v2

- DAO voting dashboard on the public webpage
- Adding voting power to Pharaoh NFTs
- Adding more chains and cross-chain DAO voting