CryptoPuzzle :
A collectible deflationary NFT with game mechanics

Wardesqwe@protonmail.com
Macha.orange@protonmail.com
https://CryptoPuzzle.com

Figure 1: Logo

Abstract : CryptoPuzzle is a deflationary NFT auction and acquisition game inspired by ERC-721 and developed on the Ethereum blockchain. The game's goal is to collect all 25 pieces of a CryptoPuzzle in order to forge it and get a part of the pool prize, as well as the corresponding ultimate token.

The initial distribution of the 5,000 puzzle pieces is random, and a ForceBuy system prevents loss of pieces and thus the constitution of the 200 CryptoPuzzles.

CryptoPuzzles' NFT are 64x64 pixel art, and will either be stored on the Ethereum blockchain or on IPFS.

A fee on each piece transaction (excluding CryptoPuzzle) as well as the initial claim cost of the piece will feed the pool prize as well as the developer's funding.

An ERC20 token, is entirely held by the developer team, allows governance as well as the distribution of the funds collected over time with DevTax.

Table of contents

1. Introduction to CryptoPuzzle

CryptoPuzzle wants to be a unique project on the Ethereum blockchain. We will see in this introduction the constitution of the pool prize and the economic model for financing developers. Then, we will see our choices to "gamification" the optention of these NFTs thanks to the phase of acquisition then creation of CryptoPuzzle, making deflationary the number of token. Then we will see the optimized auction system in order to reduce gas consumption, finally the sstore of NFTs on the blockchain and/or IPFS.

The prize pool is an element introduced to encourage random claim of all 5000 puzzle pieces at smart contract launch, because nobody can win prize pool until all the pieces are distributed. 90% of the price from random claim is put funded to prize pool. For each CryptoPuzzle created, creator also wins 5% of the prize pool. During the game, pool prize is regularly feed up a by the PoolPrize tax.

PoolPrize tax is only applied to puzzle pieces' transactions, and it's amount is 3%. It encourages CryptoPuzzles' creation, as transactions of CryptoPuzzles are exempt from this tax, and are only subject to DevTax.

DevTax applies to all tokens, pieces and CryptoPuzzles, 3 % transaction's amount.

The economic model chosen is taxation of transactions. It is the healthiest model because it is a win-win situation between players and developers. The cost of the random acquisition is only 10% for developers, so they have no interest in copying/pasting project ad nauseum to sell tokens in the largest possible quantity, which is deleterious for players who end up with a NFT less and less rare because of inflation. More volume mean more players gain, and also developers. It is therefore in the interest of developers to work with the community in order to bring more value to the project. Moreover, the deflationary game design of these NFTs guarantees a concentration of the total value of the project in only 200 CryptoPuzzle.

CryptoPuzzle is meant to be a unique deflationary NFT project. Paradoxically, all 200 Cryptopuzzles are not purchasable at launch. Their obtaining is "gamified" with a SmartContract, and is divided in two phases.

The first phase concerns the distribution of 5000 pieces. "ForceBuy" and "Mint" functions are not accessible until all puzzle pieces have found their first buyer. The amount of Ether for claim is defined during the StartSales by developers, is constant over time, until after 3 months when price will drops to 0, making claim free (excluding transaction cost). During this phase, transfers/bids/offers are possible.

The second phase comes when all pieces have been distributed. Unlocked functions are Mint and Forcebuy. Forcebuy allows to force the sale of a piece against a large amount of ether, which increases over time according to the number of Cryptopuzzle claim. This feature thus guarantees that every CryptoPuzzle is obtainable, but cannot be applied to a CryptoPuzzle. The Mint is available, and when 25 pieces of the same family are under the possession of the same address, Mint allows to forge CryptoPuzzle and to associate it to the address that minted them. The 25 puzzle's pieces are frozen (you won't be able to transfer/sell/buy/forcebuy them) and 5% of the prize pool is paid to Mint address' account.

A special features of CryptoPuzzles is that they have a 64x64 PixelArt design. This allows them to be easily stored on blockchain. Indeed, CPZs are not a web link to an image. They are sstore on blockchain for a relatively high amount, but this allows to have them forever available just by reading the event store of the contract. Also, gas optimization is a priority for developers, which

is why EIP 72 integration allows for an auction and sale system by signing off-chain transactions (free).

In a market where ITOs (Initial Token Offering) duplicate their NFT in order to finance themselves, CryptoPuzzle works against the fashion by rarifying its tokens by a regular destruction until only 200 tokens thus becoming a deflationary NFT project.

The economic model chosen by developers is like : to put a tax at initial distribution, and low taxation for each exchange. This economic model is for us the best possible for people wishing to acquire pieces of our CryptoPuzzle. Indeed, interest of an investor or a collector is to see the value of his token increasing with time. Since developers tax each sale, they will have an economic interest aligned with users by hoping for a contribution of sales volume. As this tax is not revocable, developers will have same interest : increasing token value after the sales.

Thus, users will not have any risk to see a duplication of their NFT, contrary to other projects, but will see very quickly a deflation of the CryptoPuzzle NFT.

2 Game mechanics

2.1 Inspiration

Game design is inspired by NFTs CryptoPunk, and auction system by Meebits (off-chain message signing with EIP-712).

2.2 Main game features

Each piece is unique, there is 5000 of them (n°1 - n°5000).
Each CryptoPuzzle is unique, there is 200 of them (n°5001 - n°5201).

NFT N°1 to 5000 = Piece.
NFT N°5001 to 5200 = CryptoPuzzle.

Each piece is part of a 25 pieces CryptoPuzzle.
CryptoPuzzle are organized in an increasing way.

Example : piece N°4 is part of the CryptoPuzzle #1 because it is included between piece N°1 and piece N°25. The 25 pieces of the CryptoPuzzle #1 allow to obtain the CryptoPuzzle 001.

Piece N°28 is part of the CryptoPuzzle #2 because it is included between piece N°26 and piece N°50. The 25 pieces of the CryptoPuzzle #2 allow to obtain the CryptoPuzzle 002.

2.3 Pieces

There are 5000 puzzle pieces that are randomly distributed in the first phase of the game. Each piece being part of a 25 piece CryptoPuzzle, they are destined to be consumed to forge a CryptoPuzzle.

2.4 CryptoPuzzle

CryptoPuzzle is a NFT forged using the gathering by a single Ethereum address of all 25 puzzle pieces from a single set. There are 200 of them, and they are stored in the Ethereum blockchain. They are subject to a 3% developer fee for each acquisition/sale, but are no longer subject to pool prize tax.

2.5 Differences between « Pièce » and « CryptoPuzzle »

Figure 2: Table to summarize the differences between a piece and a CryptoPuzzle

2.6 Random distribution

The first 5000 puzzle pieces are initially distributed in a pseudo-randomized way among players using claim function. This function evolves in two phases during distribution:

- First phase: each claim function issued by a player generates a randomized number derived from block number, the issuer's address of the transaction, and a randnonce internal to the contract, modulo total number of pieces (5000). The contract calculates if the token corresponding to the puzzle number is free, and if not, adds +1 until finding a free puzzle piece (owner =/= 0x0) or limited to 50 iterations. At the end, either a token is delivered to sender, or the transaction is "reverted" with a "50 loops limit reached" message in order to preserve sender's gas. Each loop costs 1084 gas.

- Second phase: claim function evolves when number of remaining puzzle pieces is 400 (8%). In order to avoid an exponential expenditure of gas, claim switches to linear mode. Each remaining piece is claimed in its natural order. However, distribution of previous 4600 pieces allows an acceptable randomization for the continuation of the game with respect to the gas spent in contract execution. ClaimLinéraire is there to save gas, guaranteeing a claim for last 400 pieces with a maximum expenditure of 7 million total gas. Number of loops between each linear claim token will average 12.5 per token.

2.7 Smart Contract features

Impossible to "burn" a puzzle piece to address 0x0 by transferring it.
Impossible to "force buy" a puzzle piece as long as 5000 pieces are not distributed.
Impossible to transfer a puzzle piece having been used for CryptoPuzzle minting.
Impossible to send pieces to a smart contract.

We will see here each function available for players, their conditions of execution and their effects.

I Security I

Modifer onlyOne : allows to secure some functions by letting them run only one at a time (Claimrandom, Mint, Withdraw)

II ERC 2222 II

Function stack: Repatriation of funds on FDT contract for Dev Tax's distribution weighted according to the quantity of tCPZ owned by different addresses.

III SSTORE NFT III

Function sstoreRobot : allows to store string of the CryptoPuzzle on blockhain as an event.

IV Bank IV

Function deposit : Allows to deposit ethers for user.

Function withdraw : Allows to withdraw all pending ethers on contract (coming from a token sale or when a jackpot is obtained).

V CPZ gameDesignRules V

Function startSale : allows to launch publicSale, while choosing parameters claim price, forcebuy, forcebuy step, and duration of the sale before claim price is removed,

Function pauseMarket : allows to pause claim function.

Claim token : payable function (0,01 ether) attributing a token, the number being generated either in a pseudo-randomized way or in a linear way. This function is unusable once 5000 tokens are distributed.

Transfertoken : allows to transfer an NFT to an address. Impossible to "burn" a token to address 0x0 by transferring it. Impossible to "force buy" a puzzle piece as long as 5000 pieces are not distributed.
Impossible to distribute a puzzle piece used for CryptoPuzzle minting.

ForceBuy : Allows to force a sale of a puzzle piece with a high price in ETH (price increasing with the amount of forged CryptoPuzzle by 0,005eth, base price 0,1 ETH is 10x the claim price).
Impossible to do on piece N°0.
Impossible to do on a CryptoPuzzle (number 5001-5200)
Impossible to execute on a puzzle piece having been used for CryptoPuzzle minting.
Impossible to do on a non-claim piece (owner address 0x0).
Both taxes are applied in ForceBuy to avoid spam.

TakeAJack function : allows CryptoPuzzle minting with its 25 associated puzzle pieces, and to win 5% of the prize pool.
Impossible to do if CryptoPuzzle associated to this piece is already claimed.
Increase ForceBuy’s cost by 0.005ETH.

VI Market with EIP 712 (OffChain transaction) VI

Trade is done off-chain using signature of a message. This message is stored on the website https://cryptopuzzle.com, and is used in acceptTrade and cancelTrade functions. Here are different possible trades and differents fields that can be filled in:

EIP-712 : OffChain transaction with signed message						
Champ	Nature du champ	Required	Bid	Bid To	Offer	Offer To
Domain	Hash	Yes	☑	☑	☑	☑
Maker	Address	Yes	☑	☑	❐	❐
M.Wei	Wei	No	❐	❐	☑	☑
M.Ids	Number CPZ	No	❐	❐	☑	☑
Taker	Address	No	0x0	☑	0x0	☑
T.WEI	Wei	No	❐	❐	☑	☑
T.Ids	Number CPZ	No	☑	☑	❐	❐
Expiry	Second	Yes	1630101101	1630101101	1630101101	1630101101

☑ : If field is filled
❐ : If field is empty
0x0 : Genesis address
1630101101 : Corresponds to 48 hours (in ms).

Function accept trade : Accepts trade (only possible when different from Maker).
Function cancel Trade : makes the trade signature unusable.

2.8 Taxe

Two fees exist in CryptoPuzzle contract.
The first fee is attributed to PoolPrize. Amounts is 3%, and is applied to each purchase and sale of puzzle pieces (including ForceBuy). It does not apply to forged CryptoPuzzle.
DevTax: it amounts to 3% and is applied to every sale and purchase of token as well as ForceBuy, pieces and CryptoPuzzle.

2.9 Pool Prize

It is funded in two ways:
- At initial distribution, 90% of the claimPrice is put into the pool for the 5000 pieces.
- Fueled by each purchase and sale of a piece (# 1 to 5000).

Each person who manages to forge a CryptoPuzzle by collecting all 25 pieces of a single CryptoPuzzle, will be rewarded (in exchange for freezing 25 pieces) by 5% of from the pool prize's amount pool, as well as the corresponding CryptoPuzzle. When the last CryptoPuzzle is forged,

remaining amount of the pool prize will be untouched on contract without any possibility of withdrawal by devTeam (will be probably a very small amount because of the 200 mint reiterations).

3. Sécurity : Wrapping

The economic system being taxation, wrapping functionality is partially removed. On the other hand, CryptoPuzzle (n° 5001 to 5200) will be wrappable on other contracts and exchange platforms (OpenSea etc.).

4. Non-Fungible-Token

4.1 History

In year 2140, the last block of Bitcoin was mined. ASICS, now useless, have rebelled in order to subdue humanity. A war breaks out between two camps, Light Army and Dark Army, where both sides must gather their weapons for battle. RISE ROBOTS !

4.2 Artistique direction

Each robot consists of a 64x64 image with a landscape background. It is separated into 25 to form the 25 puzzle pieces. When forged, landscape background becomes shiny to signify that it is completed.

4.3 « On chain » storing

Each robot image consists of 4096 pixels (64x64), design will be stored on blockhain, but previously worked on to optimize its storage cost. This image is translated into hexadecimal sentences. Each hexadecimal character forming 4 bits. 0's are transparent, and 1's are black, this forms robot' silhouette. They are stored on blockhain via sstore function of the contract. In order to save gas, and taking advantage of symmetry for each robot, only half of the drawing is sstore in hexadecimal format.

So we have CryptoPuzzle' silhouette. 0's being transparent, they are replaced by a landscape with a better resolution (not sstore on chain). This landscape becomes bright during CryptoPuzzle minting.

Example, starting image :

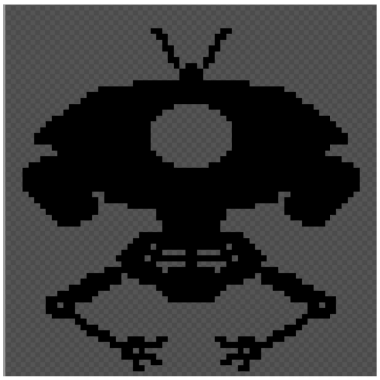
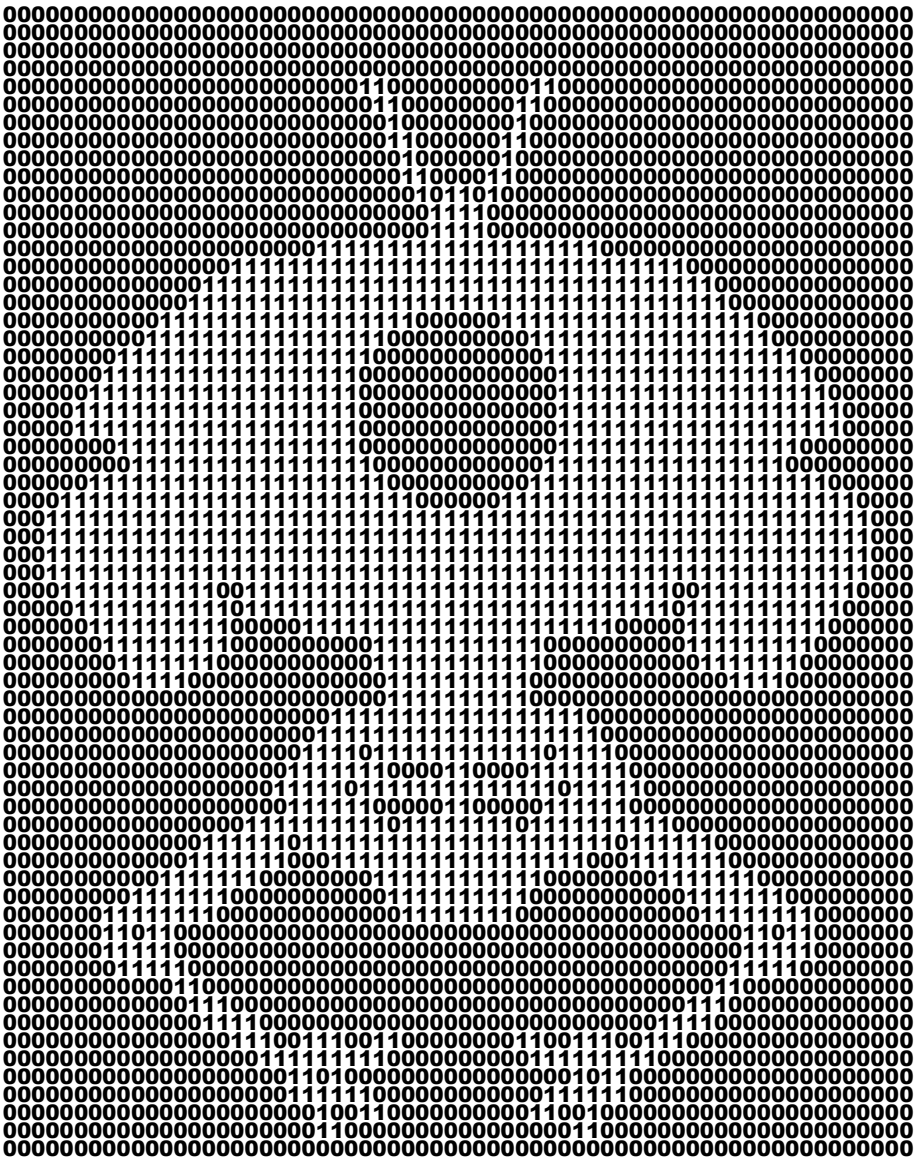
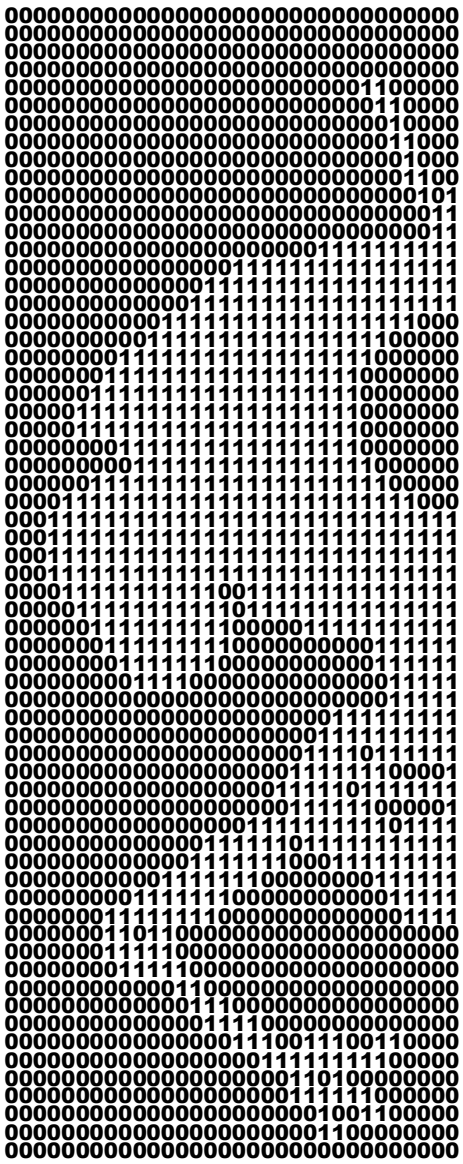


Figure 3: Pixel Art from CryptoPuzzle 22

Converting to binary (1 = black, 0 = white) with https://www.dcode.fr/binary-image :



To save gas for sstore function, we use symmetry:



Translation into hexadecimal :

60000000300000001000000018000000080000000C0000000500000003000000030000003FF0000FFFF0003FFFF0007FFFF001FFFF8003FFFE000F
FFFC001FFFF8003FFFF8007FFFF8007FFFF8000FFFF80007FFFC003FFFFE00FFFFFF81FFFFFFF1FFFFFFF1FFFFFFF1FFFFFFF0FFE7FFF07
FF7FFF03FF07FF01FF003F00FE003F0078001F0000001F000001FF000003FF000007BF00000FE100001F7F00000FC100007FEF0003F7FF0007F
1FF001FC03F007F001F01FE000F01B0000001F0000000F80000000C0000000700000003C0000000E73000003FE000000D0000000FC0000002600
0000030000000000

Then we use sstore function from contract, with parameters :

- uint : represents CryptoPuzzle number
- string : represents hexadecimal sequence of the CryptoPuzzle.

CPZ’s data are not intended to be modified, we store it via an event.

Sstore costs for a 512 HEX characters string is 60,000 gas.

5. Governance

5.1 ERC-20 tCPZ

An ERC20 is present on this smart contract: It is tCPZ, or CryptoPuzzleToken. It allows to distribute fund collected by the contract in an equitable way between tCPT's holders. There are 1,390,846,303 tCPZ representing 100% right for remuneration from Dev tax. They are initially held by developer team.

tCPZ quantity corresponds to Unix timestamp from bitcointalk post for HunterCoin (date of January 27, 2014 at 06:11:43 by Snailbrain)

5.2 ERC-2222 « Funds distribution Token Standart (FDT) »

L'ERC-20 tCPZ is used as a ERC-2222.

5.3 Governance

A governance is implemented according to tCPZ holders. The game being time limited, there is no system for governance votes. A vote will be done simply by signing a message, and the number of votes counted manually, one vote per tCPZ.

6. Road map

On website https://cryptopuzzle.com
Bot Discord
Bot Twitter
Video Youtube
NFT splitting
Sale of ERC20
Adding Wallet Connect features
Partnership with MEW
Communication
Exhibition
Commemorative puzzle

7. Team

- Wardesqwe, Smart Contract developer. Investor in Bitcoin in 2013.
- Macha, frontend developer. Investor in Bitcoin in 2013.
- SuportCPZ, alpha-tester, moderator and pixel art artist.
- Nampa, alpha-tester, moderator and pixel art artist.

8. References

Cryptopunk
Meebits
Randomization equation
ERC-20
EIP-712
ERC-721
ERC-2222
isContract Stackexchange
Piskel
Binary converter
https://bitcointalk.org/index.php?topic=435170.0