Ethereum

smart Contracts

Study and analyze report

By Morteza Shahabi

25 Dec 2021

At this document, this blue-colored texts are authors notes.

1- Ethereum smart contract with ERC-20 standard:

All the following information is about the smart contract itself and has nothing with the client-side.

Definition:

From: https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/

What Is ERC-20?

One of the most significant Ethereum tokens is known as ERC-20. ERC-20 has emerged as the technical standard; it is used for all smart contracts on the Ethereum blockchain for token implementation and provides a list of rules that all Ethereum-based tokens must follow.

ERC-20 is similar, in some respects, to bitcoin, Litecoin, and any other cryptocurrency; ERC-20 tokens are blockchain-based assets that have value and can be sent and received. The primary difference is that instead of running on their own blockchain, ERC-20 tokens are issued on the Ethereum network.

ERC-20 Defines a Common List of Rules

As of August 2021, around 442,647 ERC-20-compatible tokens exist on Ethereum's main network. The ERC-20 commands vital importance; it defines a common list of rules that all Ethereum tokens must adhere to. Some of these rules include how the tokens can be transferred, how transactions are approved, how users can access data about a token, and the total supply of tokens.

From: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

What is ERC-20?

The ERC-20 introduces a standard for Fungible Tokens, in other words, they have a property that makes each Token be exactly the same (in type and value) of another Token. For example, an ERC-20 Token acts just like the ETH, meaning that 1 Token is and will always be equal to all the other Tokens.

As the conclusion, The ERC-20 is a standard to deploy token smart contracts on Ethereum blockchain and the token can be crypto currency,

game chip or etc. Although it's not mandatory to follow this standard to start a new token, following this standard has some benefits like:

- Easier process for applying the coin for major crypto currency exchange markets.
- Being more reliable.
- Being easier to make it popular.

Deployment operation:

The ERC-20 standard smart contract must be able to do all these operations:

- `name` returns the name of the token (e.g., Binance Coin)
- `symbol` returns the symbol of the token (e.g., BNB)
- `decimals` returns the number of decimals the token uses
- `totalSupply` returns the total number initially supplied to the token
- `balanceOf` returns the balance of an account
- `transfer` transfers a certain amount of tokens to an address
- `transferFrom` transfers a certain amount of tokens from a beneficiary address to a recipient address
- `approve` withdraws tokens from the owner's address up to a certain amount of tokens
- `allowance` returns the number of tokens withdrawable from the owner's account
- `event Transfer`, which must be triggered when tokens are transferred
- `event Approval`, which must be triggered when an account is approved to collect a certain amount of tokens

Since every blockchain operation does cost gas, in order to deploy the contract, we need to have some ether in the wallet address which will be used to deploy the contract.

Deployment of the JTC (Jafari Test Token) with below specifications costed 0.00166752 Ether.

Technical Information:

The Solidity version of the smart contract is 0.4.24. There are newer versions of solidity and each of which has its own pros and cons which will be discussed in further reports.

Contract address: 0x83398BD07Dd481E2743f1A0D76deD8F5C38Feb34

Host blockchain: Ropsten Test Network.

In JTC all the tokens have been generated the moment the smart contract has been deployed on the blockchain. however, tokens can be generated on certain events such as a mining result or game winning or .... (I’m not sure if it's against ERC-20 standard principles or not).

2- Ethereum smart contract with ERC-721 standard:

All the following information is about the smart contract itself and has nothing with the client-side.

Definition:

From: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/

What is ERC-721?

The ERC-721 introduces a standard for NFT, in other words, this type of Token is unique and can have different value than another Token from the same Smart Contract, maybe due to its age, rarity or even something else like its visual.

From: https://decrypt.co/resources/erc721-what-is-it-guide-ehtereum-token

What is ERC-721?

ERC721 is a token standard on Ethereum for Non-Fungible Tokens (NFT). Fungible means interchangeable and replaceable so something like Bitcoin is fungible because any Bitcoin can replace another Bitcoin. Each NFT, on the other hand, is completely unique. One NFT cannot replace another.

As the conclusion, The ERC-721 is a standard to deploy NFT smart contracts on Ethereum blockchain and the token can be almost everything like any collectibles, trophies, art works or etc.

Deployment operation:

In addition to ERC-20 smart contract standard methods, these events and functionalities must be available in an ERC721 smart contract:

- `event` Transfer - This emits when ownership of any NFT changes by any mechanism.
- `event` Approval - This emits when the approved address for an NFT is changed or reaffirmed.
- `event` ApprovalForAll - This emits when an operator is enabled or disabled for an owner. The operator can manage all NFTs of the owner.
- `function` balanceOf - Count all NFTs assigned to an owner
- `function` ownerOf - Find the owner of an NFT.
- `function` safeTransferFrom - Transfers the ownership of an NFT from one address to another address including some additional data.
- `function` safeTransferFrom - Transfers the ownership of an NFT from one address to another address.
- `function` transferFrom - Transfer ownership of an NFT -- THE CALLER IS RESPONSIBLE TO CONFIRM THAT `_to` IS CAPABLE OF RECEIVING NFTS OR ELSE THEY MAY BE PERMANENTLY LOST.
- `function` approve - Change or reaffirm the approved address for an NFT.
- `function` setApprovalForAll - Enable or disable approval for a third party ("operator") to manage.

- `function` getApproved - Get the approved address for a single NFT.
- `function` isApprovedForAll - Check if an address is an authorized operator for another address

Some of these functions may need to have overloads that would have the same name and same functionality but with different inputs.

Technical Information:

Deployment of the contract:

The Solidity version of the smart contract is 0.8.0

Contract address: 0x31A61A2ba07705c59032790547FF7100a27BAB0D

Contract Name: NewNTF

NFT Name: Synth NFT

NFT Symbol: SYN

Paid fee to deploy the contract: 0.00166752 ETH.

Host blockchain: Ropsten Test Network.

Minting the first NFT on the contract:

Minting transaction hash:
0x31A61A2ba07705c59032790547FF7100a27BAB0D

Paid fee to approve the mint: 0.00040813 ETH

Approve the first NFT:

Minting transaction hash:
0x31A61A2ba07705c59032790547FF7100a27BAB0D

Paid fee to approve the mint: 0.00012359 ETH

NFT json file address:

https://ipfs.io/ipfs/Qme89zQQzmKbcr9fKboUrcWMzgiGtxZ1pYbhBPS92XaHsB

NFT Image link:

https://ipfs.io/ipfs/QmdDWqZFBXmfmzHmPaNMz88W9LChZHSn9JkuVHWmPcWysy

3- Study of Sushi swap and Pancake swap:

Introduction of pancake swap:

Pancake Swap is a decentralized platform which provides useful services like:

- **Exchange**: (Actually the action of swapping) A marketplace where user can trade various tokens in exchange to each other.
- **Liquidity**: Providing liquidity to the liquidity pool. (Needs detailed research. Seems client can provide liquidity to the platform and as the reward takes a small percent of all trades on the pair).

- **Farms**: Earning CAKE token for providing liquidity.
- **Pools**: Earning tokens by Steaking Cake in desired pool.
- **Competitions**: (Actually, this part is a little complicated and I prefer to do more research on it and provide the info later).
- **Predictions**: (Something like binary option) User predicts the BNBUSDT price and if the price hits the target user rewarded and vice versa.
- **Lottery**: User buys a ticket for 5$ in Cake and takes a ticket and receives a huge amount of CAKE if the ticket wins. It also may have sub winners like when half of the ticket's digits match the jackpot.

Introduction of sushi swap:

Pancake Swap is a decentralized finance community driven platform which provides useful services like:

- **Swap**: A marketplace where user can trade various tokens in exchange to each other.
- **Pool**: Liquidity providers earn a 0.25% fee on all trades proportional to their share of the pool. Fees are added to the pool, accrue in real time and can be claimed by withdrawing your liquidity

- **Farms**: Earning CAKE token for providing liquidity.
- **Lend**: Isolated lending markets mitigate your risks as an asset lender. Know exactly what collateral is available to you in the event of counter party insolvency.
- **Borrow**: Borrowing allows you to obtain liquidity without selling. Your borrow limit depends on the amount of deposited collateral. You will be able to borrow up to 75% of your collateral and repay at any time with accrued interest.
- **Create**: If you want to supply to a market that is not listed yet, you can use this tool to create a new pair.

The Technical key difference between Sushi swap and Pancake swap is the Sushi swap has been implemented on Ethereum blockchain using ERC-20 standard and the Pancake swap has been implemented on Binance Smart Chain using BEP-20 standard.

4- The new principle of calculation of gas:

Definition:

From: https://ethereum.org/en/developers/docs/gas/#post-london

Since each Ethereum transaction requires computational resources to execute, each transaction requires a fee. Gas refers to the fee required to conduct a transaction on Ethereum successfully.

The London Upgrade was implemented on August 5th, 2021, to make transacting on Ethereum more predictable for users by overhauling Ethereum's transaction-fee-mechanism.

Starting with the London network upgrade, every block has a base fee, the minimum price per unit of gas for inclusion in this block, calculated by the network based on demand for block space. As the base fee of the transaction fee is burnt, users are also expected to set a tip (priority fee) in their transactions. The tip compensates miners for executing and propagating user transactions in blocks and is expected to be set automatically by most wallets.

Calculating the total transaction fee works as follows:

Transaction fee = Gas units (limit) * (Base fee + Tip)

5- Ethereum smart contract with ERC-1155 standard:

All the following information is only about the standard, its use cases and features.

Definition:

From: https://phemex.com/academy/what-are-erc-721-and-erc-1155

What is the ERC-1155 Standard?

ERC-1155, an improved standard beyond ERC-721, is another token standard on the Ethereum blockchain that facilitates the creation of both kinds of tokens, fungible and non-fungible. The goal is to create a smart contract interface that can represent both types.

From: https://eips.ethereum.org/EIPS/eip-1155

Simple Summary

A standard interface for contracts that manage multiple token types. A single deployed contract may include any combination of fungible tokens, non-fungible tokens or other configurations (e.g. semi-fungible tokens).

Abstract

This standard outlines a smart contract interface that can represent any number of fungible and non-fungible token types. Existing standards such as ERC-20 require deployment of separate contracts per token type. The ERC-721 standard's token ID is a single non-fungible index and the group of these non-fungibles is deployed as a single contract with settings for the entire collection. In contrast, the ERC-1155 Multi Token Standard allows for each token ID to represent a new configurable token type, which may have its own metadata, supply and other attributes.

Use cases and features:

From: https://phemex.com/academy/what-are-erc-721-and-erc-1155

Benefits of ERC-1155 Tokens

- Effective Transfer: The ERC-1155 standard allows users to make massive transfers natively of the tokens within a smart contract. For example, in a smart contract with a series of fungible or non-fungible tokens, a developer can choose to transfer multiple tokens in the same operation. It not only reduces the transaction cost but also minimizes the impact on the network.
- Multiple Tokens in A Single Contract: Each ERC-1155 token describes the existence and operation of both the fungible and non-fungible token types. For example, while an ERC-1155 can create one or more NFTs, it can also describe fungible tokens – all within the same contract.
- Secure Transfer of Tokens: ERC-1155 token standard includes a function that checks whether a transaction is valid or not. If a transaction doesn't go through, this function returns the token to the issuer. It helps when users accidentally make a mistake in the transcription or send out tokens to the wrong address. The code can automatically revert the transaction.

From: https://eips.ethereum.org/EIPS/eip-1155

Motivation:

Tokens standards like ERC-20 and ERC-721 require a separate contract to be deployed for each token type or collection. This places a lot of redundant bytecode on the Ethereum blockchain and limits certain functionality by the nature of separating each token contract into its own permissioned address. With the rise of blockchain games and platforms like Enjin Coin, game developers may be creating thousands of token types, and a new type of token standard is needed to support them.

However, ERC-1155 is not specific to games and many other applications can benefit from this flexibility.

New functionality is possible with this design such as transferring multiple token types at once, saving on transaction costs. Trading (escrow / atomic swaps) of multiple tokens can be built on top of this standard and it removes the need to “approve” individual token contracts separately. It is also easy to describe and mix multiple fungible or non-fungible token types in a single contract.

Also, there is more about ERC-1155 that seems beneficial which will be discussed in further reports.

All the content of this report is a drop of a vast ocean. Of course, there are lots of technical and financial areas which this report doesn't cover. I hope some of them be in the next report's subjects.

Happy holidays.