

# **EthFair project**



**Autor: Milliano Conti**

**[millianoconti@gmail.com](mailto:millianoconti@gmail.com)**

**[www.ethfair.org](http://www.ethfair.org)**

**version 0.9b**

## **Abstract**

EthFair - is a DeFi lottery project built on the Ethereum blockchain with a use of solidity smart-contracts and ERC20 standard tokens.

The project is a draw that will feature a total of 3 Lamborghini Huracans, 3 other elite supercars, several new iPads, MacBooks, iPhones and other prizes.

The distinction of this draw is its use of blockchain technology, so the winner selection process is transparent and verifiable without any possibility of fraud.

## **1. Introduction**

Every day, hundreds of different lotteries are held in the world. A huge number of people participate in them. But often it is not known exactly how the winner is chosen, how the money raised for the lottery is distributed.

After studying the lottery market, we decided to make our own fair drawing of prizes. Where each participant will see how much money is collected, how is it distributed. And the main thing is that the winner will not be chosen by a person or a pre-programmed randomizer, but by a smart contract. After all, the crypto industry was created to solve the issue of trust.

## **2. Overview**

The goal of the project is to conduct a prize drawing among ICO participants, held by the organizers of the EthFair project and governed by the smart-contract in a transparent and verifiable manner.

To participate in the EthFair lottery, the user needs to buy EthFair tokens.

The chance of winning a prize is proportional to the number of tokens deposited to the drawing contract by the user.

Detailed information about the rules of the drawing can be found at section **4 Draw rules**. A total of 3 ico`s will be held, each of which will feature 3 billion tokens. Prior to the ICO, the EthFair smart-contracts will pass a security audit.

### 3. ICO

Date of the first Ico: December 18 to January 30.

The goal for the first ICO: \$1,000,000

Users can buy tokens on ICO at a fixed rate of 900,000 EthFair tokens for 1 ETH (Ethereum cryptocurrency).

The funds collected at ICO will be spent on the prize draw.

#### **First ICO goals and prizes:**

If during Ico the project collects:	Prize:
3.000 \$	iPhone 12
10.000 \$	iPad air
25.000 \$	Macbook air
30.000 \$	Listings on exchanges.
50.000 \$	Apple Mac + iPhone 12
100.000 \$	Listings on exchanges.
200.000 \$	Toyota Camry or 30.000 \$
250.000 \$	iPhone 12.
350.000 \$	Mercedes e-class or 50.000 \$
420.000 \$	Macbook air.
500.000 \$	Porsche Panamera or 100.000 \$
600.000 \$	Additional listings on exchanges.
1.000.000 \$	Lamborghini huracan evo or 300.000\$

At the stage of the ICO, the organizers retain the right to withdraw funds from the ICO contract to cover the expenses of the project development.

All the tokens that are not sold during the ICO will be subsequently sold at exchanges. After the expiration of the main prize draw, an additional prize will be drawn with the use of these funds.

## 4. Draw rules

Users participating in the ICO purchase EthFair project tokens in exchange for ETH (Ethereum crypto currency) at a fixed price of 900,000 per 1 ETH.

### **Example:**

For example, that four users bought tokens on Ico: the first one bought 2 million tokens, the second bought 4 million tokens, the third bought 6 million tokens and the fourth bought 100 million tokens.

The organizers announce a Macbook Air draw.

The first three users decided to participate: the first sent his 2 million, the second sent his 4 million and the third sent his 6 million tokens.

The total number of tokens participating in the drawing is 12 million tokens.

Total: Chances of the first to win are 16.7%

The second has a 33.3% chance of winning

And the third 50% chances of winning.

The fourth user decided not to participate in this drawing.

**Important: Do not send ETH to the contract from exchange wallets!**

### **Time allotted for the drawing:**

After the Ico, the organizers need 2-3 weeks to prepare and test contracts for the draw. Then, the organizers announce the prize draw and give users time to decide to participate.

iPhone 12 (7 days to decide on participation and entropy submission)

iPad pro (7 days after the previous draw for the decision on participation and entropy submission)

Macbook air (7 days after the previous draw for the decision on participation and entropy submission)

Apple mac + iPhone 12(7 days after the previous draw for the decision on participation and entropy submission)

Toyota camry or 30.000 \$ (10 days after the previous draw for the decision on participation and entropy submission)

iPhone 12 (7 days after the previous draw for the decision on participation and entropy submission)

Mercedes e-class or 50.000 \$ (10 days after the previous draw for the decision on participation and entropy submission)

Macbook air (7 days after the previous draw for the decision on participation and entropy submission)

Porsche panamera or \$ 100.000 (10 days after the previous draw for the decision on participation and entropy submission)

Lamborghini huracan evo or 300.000\$(20 days after the previous draw for the decision on participation and entropy submission)

In confirmation of the awarding of prizes, the organizers of the project will post transaction hash or check in the social media resources of the project.

Because the organizer does not know what the winner will choose (prize or cash), then the organizer may need an additional month to order and send a

prize to the winner, plus a month in case of force majeure beyond the control of the organizer.

The organizers are allowed to participate in the prize draw under the same conditions as other users.

During the ICO, users can transfer or sell tokens to other users.

The chances of winning will be higher for those users who have bought more tokens and have previously sent tokens to the contract for the drawing.

Prizes will be drawn through a contract that will randomly select a winner.

## 5. Technical Details

### 5.1 General technical details

The total supply: 9.9 billion tokens

9 billion tokens would be sold through ICO.

900 million tokens would be allocated for the project developers to fund the development of the project (reward for users, salaries and other expenses).

The winner will be selected at random through the open source smart-contract.

### 5.2 Randomness of the winner selection and entropy

To eliminate the fact of fraud and determine the winner in a transparent way, our project will use an on-chain random number generation with on-chain source of entropy. Random number generator will be implemented in an open-source smart-contract which will accept entropy inputs from users and reward them for supplying entropy to the contract.

The generation of a random number is a two phase process. At the first phase users must provide hashed entropy to the contract. After the first phase is over these users must disclose the original values of their entropy to the contract. EthFair project organizers will provide an additional entropy number at the beginning of the first phase and disclose it at the end of the second phase of each drawing. Entropy providers are rewarded for providing the entropy to the RNG smart-contract. In order to become an entropy provider and get rewarded a user must:

- Prepare an entropy number that will serve as a source of entropy for the contract. The entropy number can be any value ranging from 0 to 340282366920938463463374607431768211455 (uint128 maximum value).
- Prepare a “salt” number. Salt can be any value ranging from 0 to 340282366920938463463374607431768211455 similarly to the entropy number.



- The entropy provider must securely save both the entropy number and salt number.
- Using the RNG smart-contract the entropy provider must calculate a hash of entropy and salt numbers.
- The entropy provider must then call a *provide\_entropy* function in the RNG smart-contract and input the generated hash. The function will require the entropy provider to deposit a collateral of 1 ETH to the contract. The collateral will be refunded at the moment of the entropy disclosure.
- At the specified point of time the entropy provider must disclose the entropy by calling a *disclose\_entropy* function in the RNG smart-contract. It is important that the entropy provider must provide the original entropy and salt numbers at this step. Upon disclosing the entropy the entropy provider will receive 1 ETH collateral + additional entropy providers reward from the smart-contract.

For users to participate in providing entropy, they must have at least 1 million EthFair tokens at their wallet balance.

For prize drawings ranging from 0 to \$200,000 the entropy collateral is 1 ETH and the reward is 0.05 ETH so that every entropy provider will receive 1.05 ETH if he will disclose his numbers to the contract. There will be a maximum number of 10 entropy providers for these prize drawings.

For prize drawings ranging above \$200,000 the entropy collateral is 2 ETH and the reward is 0.1 ETH. There will be a maximum number of 100 entropy providers at this stage.

**Important! If the user does not disclose entropy within 180 days, then his funds that he sent to the contract may not be returned to him.**

### 5.3 Verification

For each prize drawing, a winner has the option to choose whether to collect the prize or receive its cash value.

If the user will choose the cash option then he will receive the equivalent amount of ETH to the winning address (the price will be calculated by the coinmarketcap data at the moment of transaction generation). If the users chooses the prize option then he needs to contact the organizers to provide the further information required for the delivery of the prize.

In both cases the user needs to confirm the ownership of the winning address.

After the drawing, the user who won within three days after the announcement of the winner must contact the organizers of the drawing. The user can contact Telegram(<https://t.me/EthFairDeFi>) or E-Mail ([EthFair.DeFi@gmail.com](mailto:EthFair.DeFi@gmail.com)).

To verify the ownership of the wallet, the user can use the Civic Wallet. With this wallet, users can verify their identity. In case of using the Civic Wallet the organizers will compare the information from the wallet and social networks of the winner and then discuss the details of the prize delivery.

Countries are restricted from using Civic Wallet:

Nationals and residents of the following countries are restricted from using Civic Wallet: Afghanistan, Algeria, Bangladesh, Belarus, Bolivia, Burundi, Cambodia, Central African Republic, China, Colombia, Congo, Côte d'Ivoire, Cuba, Cyprus, Ecuador, Egypt, Eritrea, Haiti, Indonesia, Iran, Iraq, Jordan, Lebanon, Liberia, Libya, Morocco, Myanmar, Nepal, North Korea, Pakistan, Russia, Saudi Arabia, Somalia, South Sudan, Sri Lanka, Sudan, Syria, Taiwan, Ukraine, United Arab Emirates, Venezuela, Vietnam, Yemen, and Zimbabwe.

You can also use <https://mycrypto.com/> to confirm ownership of the wallet.

In order to confirm the ownership of the address using MyCrypto wallet a user must go to the message signing page at MyCrypto. Access your wallet; Enter the message that you wish to use to prove your ownership of the address. Click the

big blue "Sign Message" button. You can use this message as proof that you own an address, and share it with organizers via email ([EthFair.DeFi@gmail.com](mailto:EthFair.DeFi@gmail.com)).

## **5.2 Smart-contracts**

## **6. Project finance distribution**

Funds raised up to \$ 200,000 will be used for prizes and project development only.

Of all additional funds raised over \$200,000 (up to the goal of \$1,000,000) the following distribution method must be applied:

Prize fund - 60,5%;

Project development - 27%;

Organizers' reward -12,5%

Upon raising the first goal of \$30,000 the project development team will pursue exchange listing of the token.

## **7. References**

[www.ethfair.org](http://www.ethfair.org) -website

[EthFair.DeFi@gmail.com](mailto:EthFair.DeFi@gmail.com) -Email

[www.twitter.com/Eth\\_Fair](https://twitter.com/Eth_Fair) -Twitter

[www.reddit.com/user/EthFair](https://www.reddit.com/user/EthFair) - Reddit

<https://t.me/EthFairDeFi> - Telegram