Kibo©

LOTTO

Whitepaper version 1.06, under review

KIBO IS A DECENTRALIZED LOTTERY BASED ON ETHEREUM SMART CONTRACTS

This document describes the technical implementation of a system based on smart contracts and important aspects regarding the promotion and market launch of the system

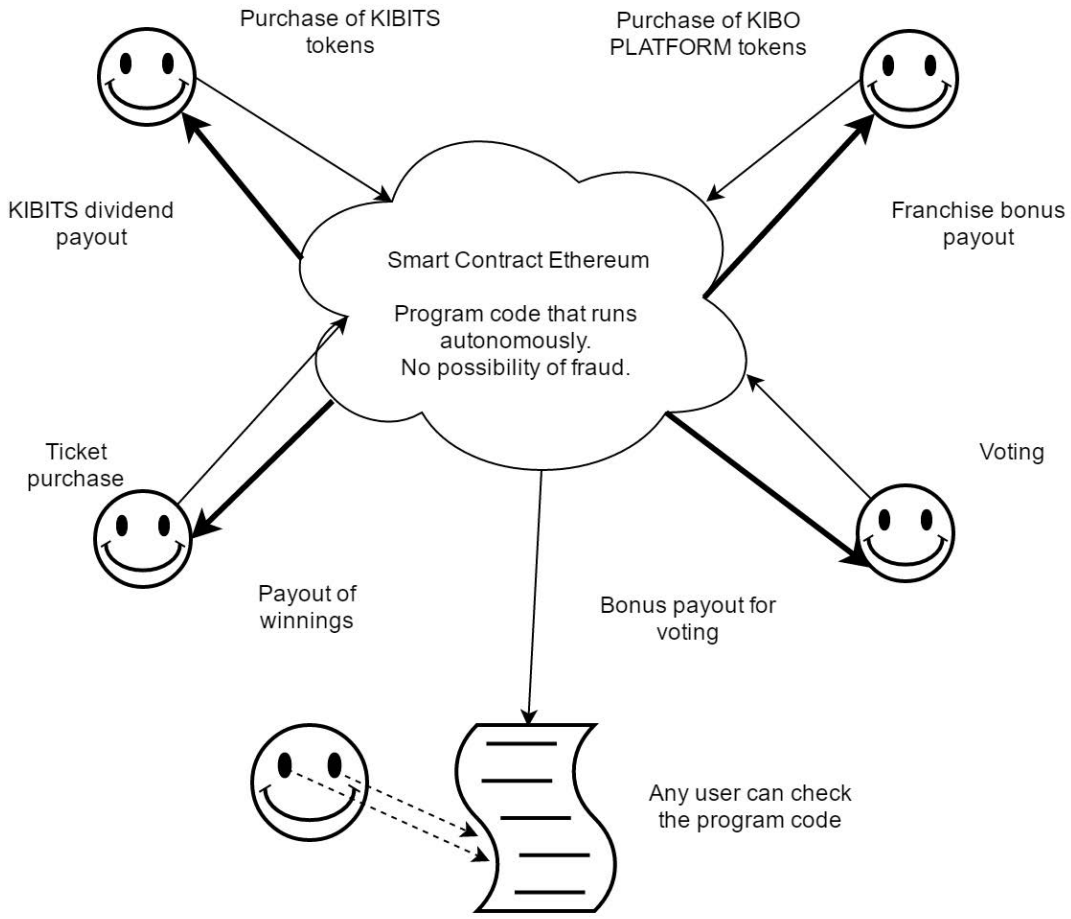
1. INTRODUCTION

Today, lottery is the largest social and entertainment game in the world. The share of lotteries on the world's gambling market is over 30 %. The annual turnover of this market today is $284 billion. Along with the penetration of the Internet and the growing number of devices connected to a network, the number of users who prefer playing this game online is growing. Consequently, the online lottery market today is promising area.

But despite such popularity, the lotteries currently present on the market cannot provide the user with a 100 % guarantee of an honest lottery or offer full transparency with regard to the formation and distribution of the prize fund. It is not surprising that this issue is a hot topic for discussion on forums and in private conversations among amateurs who like try their fortune in this game. Unfortunately, at present one can see licensed operators periodically caught in various sorts of violations regarding prize fund distribution and the honesty of the lottery. Just as important are the conditions for receiving awards, which also have a number of shortcomings in the form of delayed payments and various kinds of commissions.

Now, thanks to smart contracts, we have the ability to address these critical issues. KIBO is a decentralized lottery, the main advantage of which is the complete transparency of all processes taking place on the platform and the fundamental absence of opportunities for fraud. Unlike "fair play checks", which allow one to check game results in existing cryptocurrency lotteries, KIBO itself eliminates the potential for fraud. This is made possible by Ethereum and the concept of smart contracts. The marketing component of the lottery is also implemented based on smart contracts, allowing franchise partners and owners of KIBIT tokens to be sure of receiving their earnings and the correctness of its calculation.

KIBO is a platform where all processes are implemented and managed by smart contracts. Ticket purchase, random number generation, and prize payouts, as well as accruals in the distributed partner network, are performed by a smart contract without the possibility of intervention by third parties. Changes in the platform are made by a vote of control token holders



ETHEREUM AS THE BASIS FOR IMPLEMENTATION

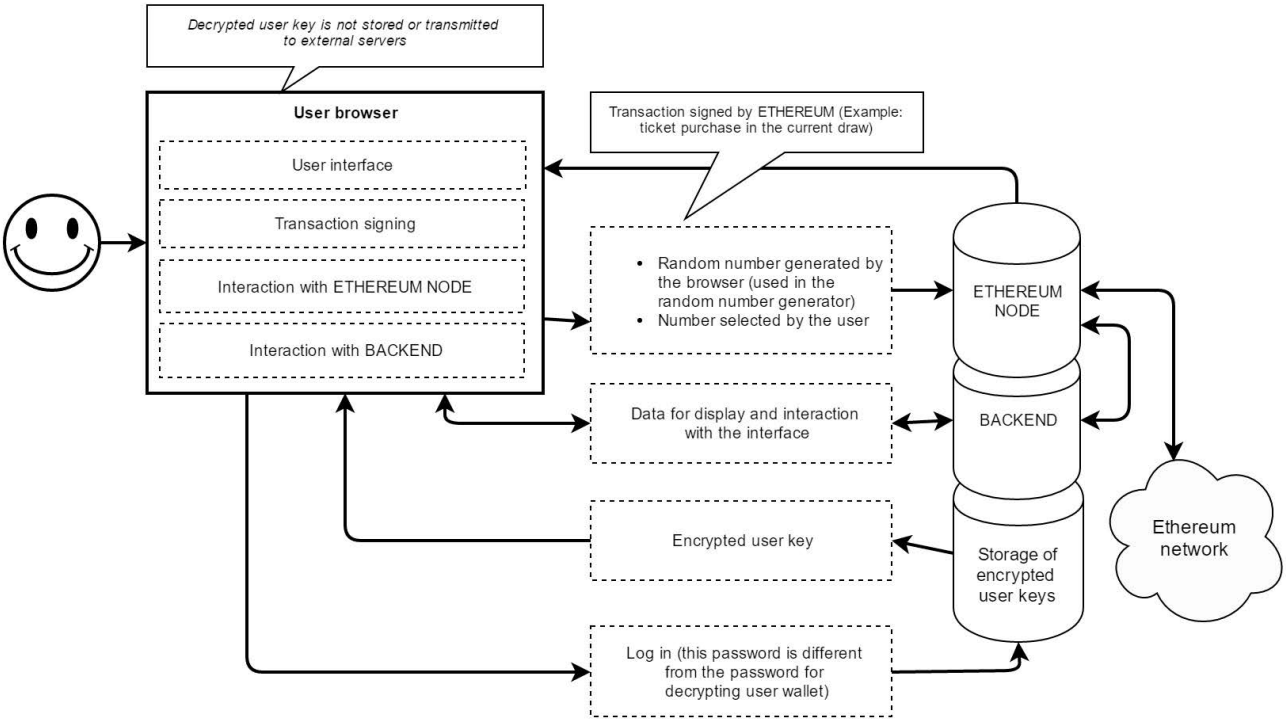
For implementation of the project, the Ethereum [2] decentralized network, which uses the concept of “smart contracts”, was chosen. Ethereum has great potential for scaling [3] and the broad support of the cryptocommunity and investors. Currently, the network is theoretically capable of handling about 10 transactions per second; this is enough to start project implementation.

Methods for network scaling presented in the above-mentioned report [3] will make it possible to accept more than 50 million users in the near future.

2. The KIBO framework

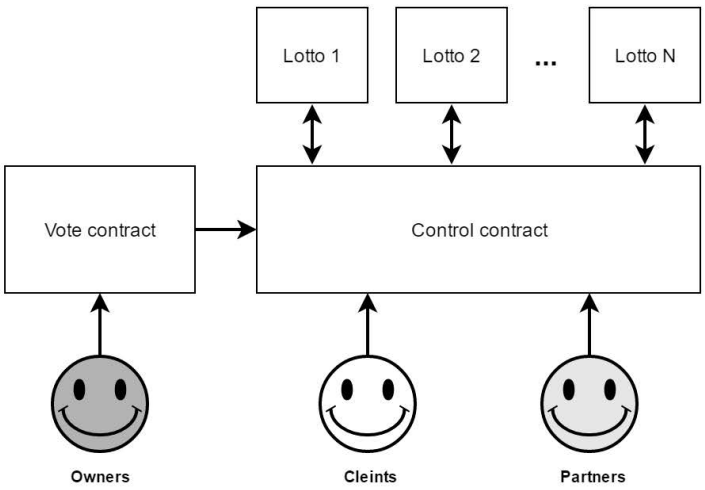
Currently, Ethereum infrastructure cannot yet offer a complete solution which includes the decentralized part of the interface (the required functionality will appear at the Metropolis stage. An excerpt from Ethereum's official blog [5]:

As it is not yet possible to decentralize the application interface itself at the moment, the KIBO project is implemented partially in a server infrastructure which contains standard solutions for such cases, as well as a specialized application based on smart contracts. In parallel with the work on the server solution, we are working on various options for decentralizing the interface part, including our own solution.



3. The contract scheme.

The KIBO Ethereum infrastructure is a set of contracts which interact with each other according to the scheme below:



At the initial stages of the platform's work, contracts in the system can be replaced (by the voting of control tokens, which at this stage are in the team of KIBO developers). Upon completion of the test and development stages, the relations between contracts will be recorded and subsequent changes in contracts and their relationships will not be possible.

A. Managing contract

The contract which coordinates the interaction of all other KIBO contracts, such as lotteries or voting contracts. New user registration, lottery ticket purchases and implementation of decisions adopted in a voting contract are performed by means of referencing the managing contract.

B. Repository

repository contract is used to store data about users, franchisee partners and their relationships. It should be noted that the contract only stores anonymous data that are not linked to the user's identity (the user is defined by his/her alias and wallet), so any system user can be completely anonymous.

Modification of certain data in the repository is only possible from the managing contract; the central contract address is determined by voting of control token holders.

```
struct K_Users_User {
        uint shareholder;                   // if user is shareholder
        uint big;                           // amount of kibits 2 user
        uint small;                         // if user is partner
        uint partner_type;                  // 0 - new, 1 - registered before platform start
        string username;                    // login
        uint[8] partner_parents;            // parents-partners structure for 7 levels
        uint[8] partner_parents_level;      // user have %q% partners at level of 7
        uint[8] player_parents;             // parents-players structure for 7 levels
        uint[8] player_parents_level;       // user have %q% players at level of 7
        }
```

C. Voting contract

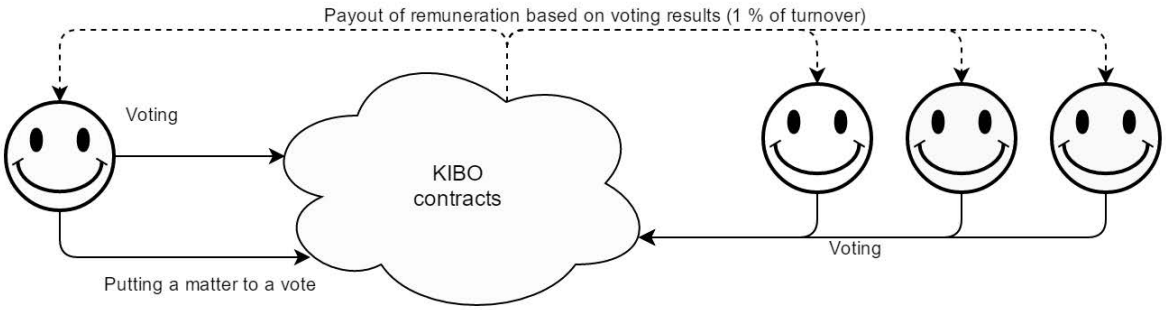
A contract that stores a list of issues for the management of all contracts, as well as the conditions for making decisions on these issues. The voting and decision-making system is implemented such as to allow the development of the platform and the addition of new games to KIBO's functionality without the possibility of intervention in the algorithms for accrual and work with the customer base of the separate branch of each partner. Only control token holders have the right to vote in this contract.

```
struct K_Ballot_Type {
        string theme;                   // issue text
        uint quorum;                    // quorum for decision-making as a %
        uint need;                      // % for decision-making
        uint length;                    // voting duration (seconds)
        }
```

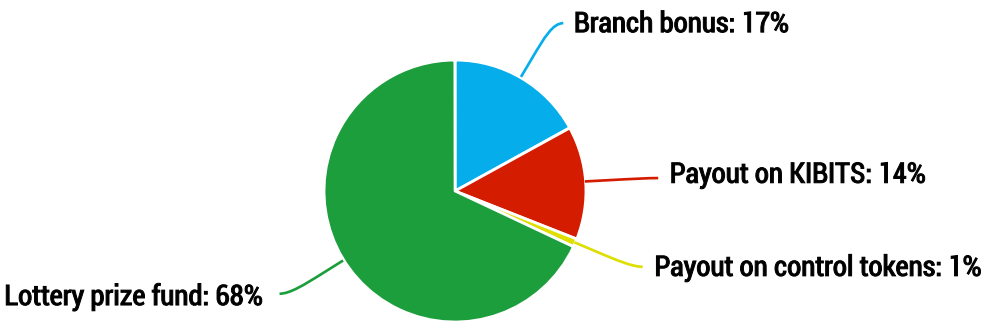
4. Contract management

Contract management is carried out by voting of control token holders. The list of issues and the decision-making conditions for each of them is initially set in the contract. Any control token holder can initiate voting on any issue in the list and vote. Voting results are accepted in the case of a positive vote of 30 % to 51 % of control token holders, depending on the importance and impact on the subsequent development and operation of the KIBO platform of the issue put to vote.

To further stimulate voting activity, the following mechanism has been implemented: accrual of remuneration per token upon voting is carried out immediately after a control token holder votes. The amount of remuneration for all 10,000 tokens is 1 % of turnover from all platform lotteries.



When tickets are purchased, funds are distributed as follows



Payout for the KIBO PLATFORM franchisee branch network 10 %	For payout of bonuses for the line-by-line branch network. 7 % distributed upwards, 1 % per level.	Payout on KIBIT tokens 14 %	Deferred payout on control tokens 1 %
Prize fund formation 68 %			

5. Tokens

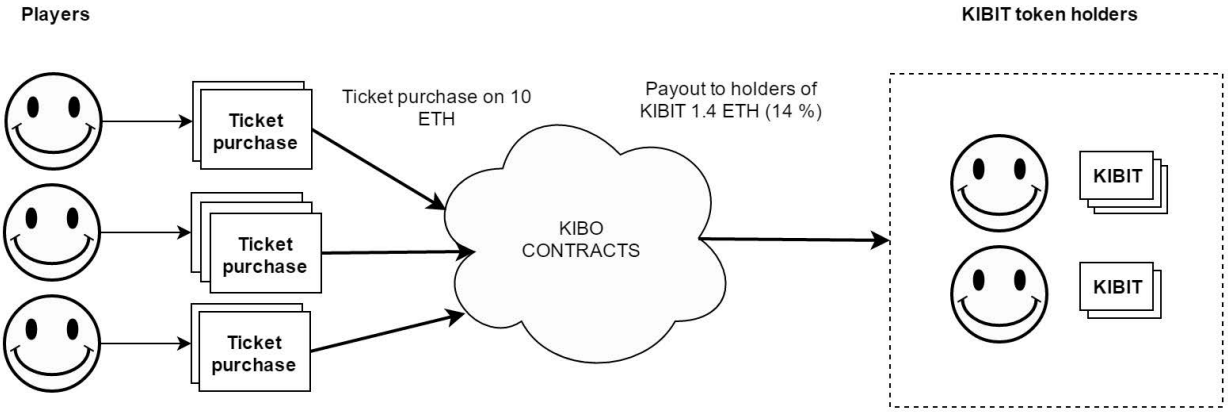
The KIBO platform has several different types of tokens, each of which has its own set of features and an expanded incentive system. All Payouts and accruals of remuneration in the branch network and all types of tokens are triggered when tickets are purchased (this is the most frequent action in the system). Payouts of prizes to players are also triggered by this and in one more way described below in the "Payout" section. All platform tokens are not KIBO internal currency and are not intended for internal settlements in the system. All payouts and remunerations are made directly to the user's wallet in ETH cryptocurrency.

KIBO control token 10,000 units are intended for contract management. It allows one to put issues to a vote (voting contract) or vote on an issue. To further stimulate voting activity, 1 % (in ETH cryptocurrency) from the total turnover of all lotteries connected to the KIBO system is accrued to all 10,000 tokens. Accrual of remuneration takes place at all times; however, the actual payout to the user's wallet is carried out only at the moment a control token holder votes. Thus, we strengthen the motivation to vote, even for minority holders of control tokens.

At the initial stage, control tokens will be distributed among the managing partners. In the future, all or part of the control tokens may be distributed among a large number of partners interested in the project's development and growth. These are major holders of KIBIT tokens or owners of platforms with large client bases.

This mechanism is incorporated in the smart contract algorithm in order to transfer contract management to a decentralized basis in the future.

KIBIT token: The KIBO platform's main investment asset. There are a total of 350 million tokens, to which 14 % of total turnover from all platform lotteries is accrued.

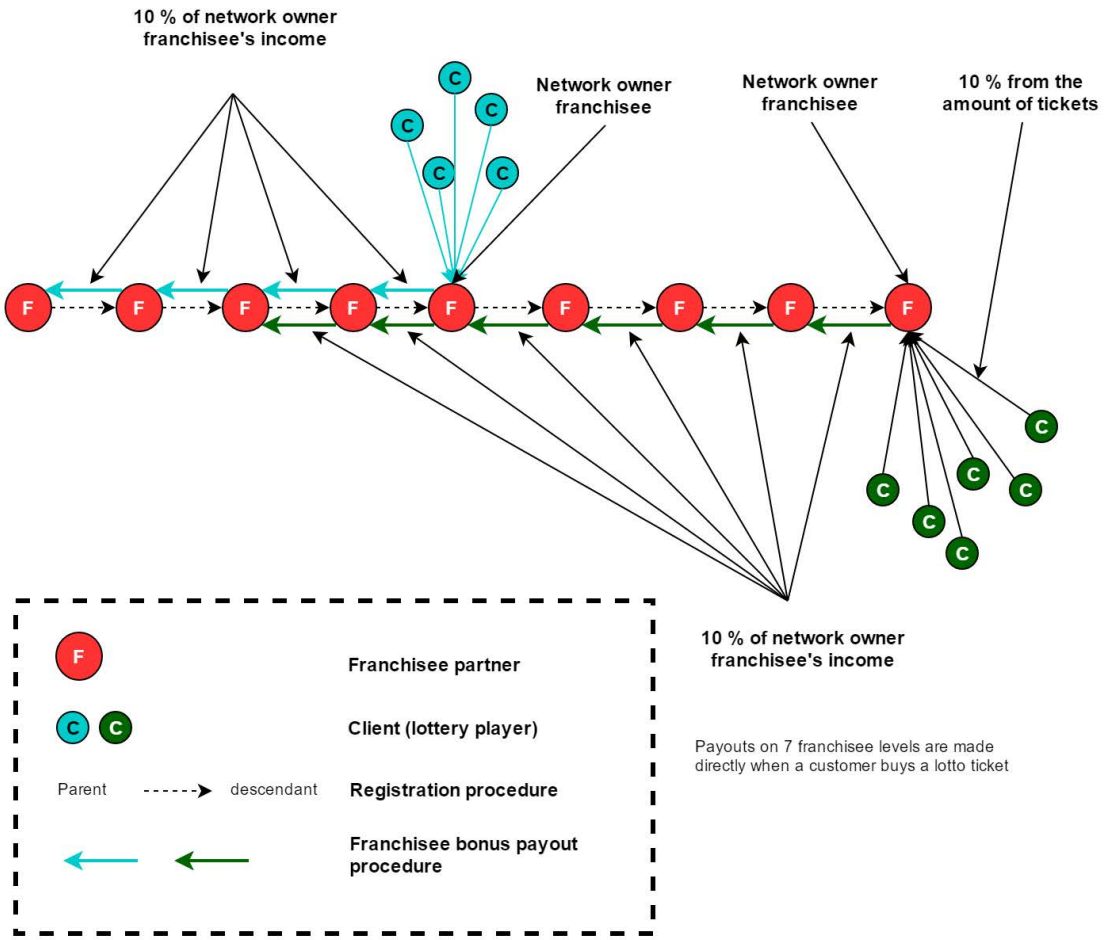


As part of the marketing strategy, at the crowd-sale stage 100 million KIBIT tokens will be distributed, to which 4 % of turnover will be allocated. The remaining 250 million are owned by the development team and will form the company's income and will be used at the team's discretion, including for further platform development, options within the team, and other strategic decisions.

Tokens not sold during the sale remain under the control of the managing partners. Income generated by these tokens may be
sent to a specific address by voting.

KIBO PLATFORM token: Allows one to become a KIBO branch owner and receive the respective bonus for the expansion of the client network and building of a branch network. All operations and payouts of remuneration in the operation of KIBO branches are guaranteed by a smart contract. There a total of 20,000 base (Kibo Platform) tokens

The branch owner receives 10 % from all tickets purchased by clients invited by him 5 levels deep



Also, the KIBO platform's functionality incorporates the possibility of expanding one's own branch network by sending registration links and platform recommendations at the time of the crowdsale. When there are such networks, additional accruals from each of these platforms will be 10 % from the income of all partner branches up to the 7th level.

Thus, 17 % will be paid out from the purchase of each ticket to stimulate the development of the client network and branch network. 10 % from ticket sales is paid out to the client base owner, and 7 % is allocated among 7 levels upwards, 1 % each, for payout to higher branches, which is equal to 10 % of the partner's income at each level.

6. Integrated marketing tool to promote continuous platform growth

The user can participate in promotions and draws which are present on the KIBO LOTTO platform. Any player can invite other players to the platform using his own link and receive 5 % of the invited players' winnings on a constant basis. This mechanism is also managed by a smart contract and is part of a marketing strategy called "game with friends". Receipt of winnings from a game with friends is governed by the following rules:

To receive 5 % of the winnings of invited players:

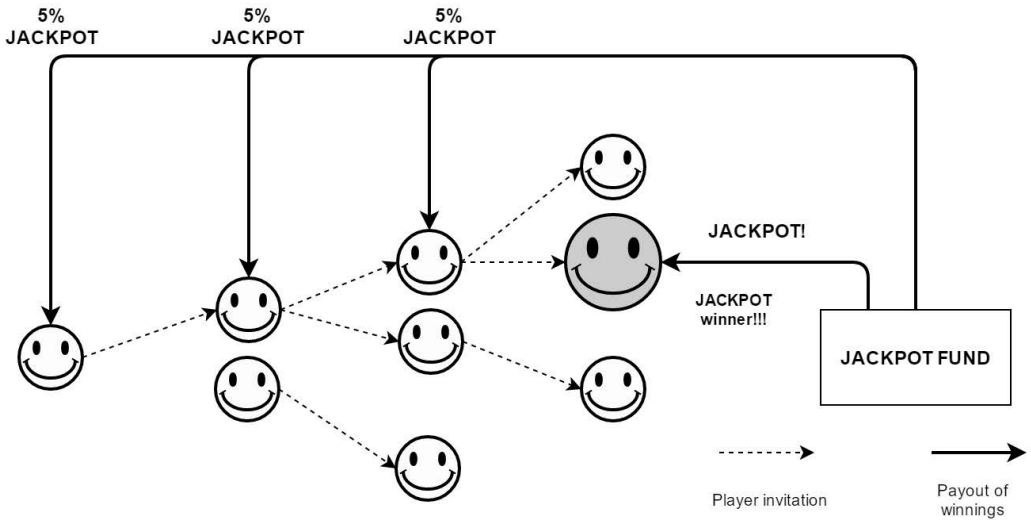
At level 1 you must have bought 1 ticket for this draw
At level 2 you must have bought 3 tickets for this draw
At level 3 you must have bought 7 tickets for this draw

Thus, the player is interested in inviting other players, because
every invited person will greatly increase the chances of winning in each draw.

Promotion

An important marketing component embedded in the KIBO platform smart contract is the proper motivation of each client at all levels of development, both for ordinary users and for the platform owners.

In the promotional draws, which will continue for three months after the platform launch, everyone can take part in a series of free draws with large cash prizes. This promotion is aimed at expanding the client base of each branch and KIBO LOTTO as a whole. Each player, as part of this promotion, will be able to give his friends the opportunity to participate in this series of draws. The free tickets received by a player as a gift win only if 6 numbers are matched. As in the "Game with friends" mechanism, if a player at one of the three levels below another player wins, the latter player receives 5 % of the amount won by the former player. To obtain this bonus, it is not necessary to buy tickets; the player needs only activate his free tickets for this draw.



Free ticket activation and protection against bots.

To reduce the risk of possible bot attacks during free draws, free ticket activation for a new player is carried out through balance refill in an amount of $1 or more. After that, a restriction on cash withdrawal is set and funds in the amount of $1 cannot be withdrawn, but are at the user's disposal. They are available for purchase of tickets for participation in any paid draws that are held on the platform along with the promotions. The user can withdraw any amount above $1 at any time. Once this account has purchased 3 tickets on the platform, the restriction is automatically removed, and from that point on the user can withdraw all the funds and zero out the balance. Thus, a bot attack becomes very costly and is comparable to simple participation in the lottery, but for larger amounts.

Prize fund formation and distribution.

68 % of a ticket purchase is allocated to prize fund formation.

Comments: Since we have tickets from which payouts for the partner and client bonus do not come entirely, as they fall within the area of non-distribution, there is always a remainder. This remainder is always used to replenish the current draw prize fund. This means that in fact the percentage used for prize fund formation is different each time and is always greater than 68 %. Let us take the initial 68 % as the basis for the description. These funds are intended for payouts related to the lottery and distributed according to the reserve funds system within the contract as follows

10% are deposited to the “reserve fund”, from which a guaranteed minimum jackpot is formed for the next draw, if a jackpot is to be awarded in the current draw.

13.5% are used for the formation of a fund from which 5 % are paid three levels upwards if a player with players above that invited him wins. Part of these funds will not be spent each time after draw completion. For example, if a player who has only one player above him wins. In this case, 10 % will not be paid to anyone. After each draw, the unclaimed remainder from this fund is automatically sent to the “reserve fund” of this lottery.

76.5% are used for the formation of the prize fund, from which the jackpot and other prizes are formed.

Next, 2 of the 4 lotteries presented on the platform at launch are described as an example.

Lottery 6/49

76.5 % of funds received for the formation of the prize payout fund in the lottery 6/49 are allocated as follows.

First of all, 48 % goes towards jackpot formation. By directing the funds from a purchased ticket to increase the jackpot first of all, we always know the jackpot size even before the draw and we can reflect its increase in proportion with ticket sales. Other prizes are formed after draw completion from the remaining 52 % as follows.

Fixed prizes are calculated first

- Tickets that guessed 2 main balls are first. These players receive a prize in an amount equal to the ticket price.
- Next, those who guessed 2 main balls + bonus ball receive their payout. The amount of the payout is 1.7 times the ticket price.
- Next, those who guessed 3 main balls receive their payout. The amount of the payout is 3 times the ticket price.

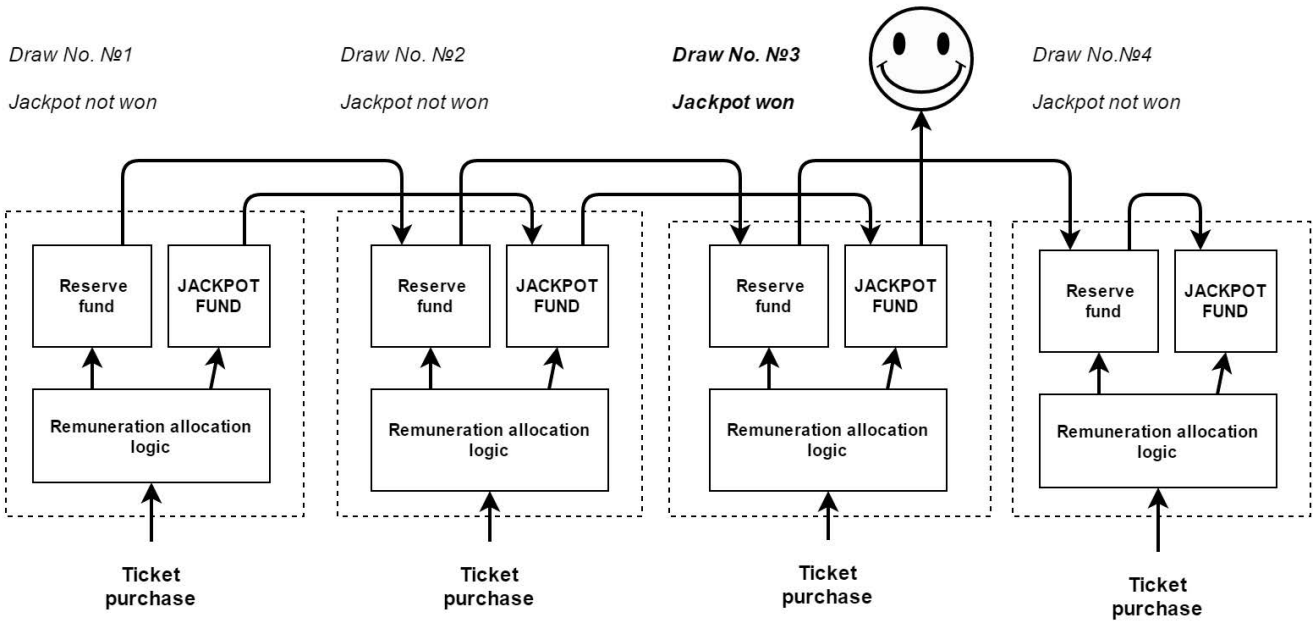
The remaining funds are allocated among those who guessed 4 numbers or more in the following order:

- 4 main balls 57 %
- 5 main balls + bonus ball 16 %
- 5 main balls 27 %

For example: 10 players guessed 5 balls; 27 % is allocated among them in equal shares.

Jackpot increase

If in the current draw the jackpot is not won, the jackpot funds (48 %) go to increase the next jackpot. That is, we take the 48 % and add them to the amount that is allocated for the jackpot from the ticket sales for the next draw. Thus, the jackpot continues to grow until it is won. Once the jackpot is won, the contract accesses the reserve fund and withdraws the amount for the minimum guaranteed jackpot, which increases from ticket sales according to the same scheme.



General points
A lottery contract is intended for conducting a lottery and storage of its draw results. Only the last 8 draws + the current draw are stored.

To generate random numbers, a combination of several factors is used:

- Every time a ticket is purchased, the user transmits a random set of data (automatically generated by frontend by default)

- After completion of the draw, the contract takes hashes of every other block out of the 14 blocks after draw completion and mixes them with the random data from users.

```
        // generate 7 numbers (6 + 1 bonus number)
        function generateResult() private {
                if (game - 1 > 0) {
                        uint counter = 1;
                        uint tmp_num = 0;
                        for (uint i = 0; i < 6; i++) {
                                tmp_num = generateResultNum(game - 1, i, counter);
                                while(!checkResult(tmp_num)) {
                                        tmp_num = generateResultNum(game - 1, i, counter);
                                        counter += 1;
                                }
                                result[game - 1][i] = tmp_num;
                        }
                        result[game - 1][6] = generateResultNum(game - 1, 7, counter);
                }
        }

        // ...

        // When drawing is ended, we remember the block.number
        // Then we wait 50 blocks;
        // Then using this remembered block we start to generate 7 numbers each second block back
        // starting from remembered block + 30
        // After all it is several blocks ahead from drawing end and several blocks behind current
        function generateResultNum(uint _game, uint _index, uint _counter) constant private returns
(uint) {
                uint num = 0;
                uint last_block = game_stats[_game].gameendblock + 30;
                num = ((uint160(sha3(block.blockhash(last_block - _index * 2), user_random[_game]
[uint160(sha3(block.blockhash(last_block - _index * 2))) % user_random[_game].length])) * _counter) %
49) + 1;
                return num;
        }
```

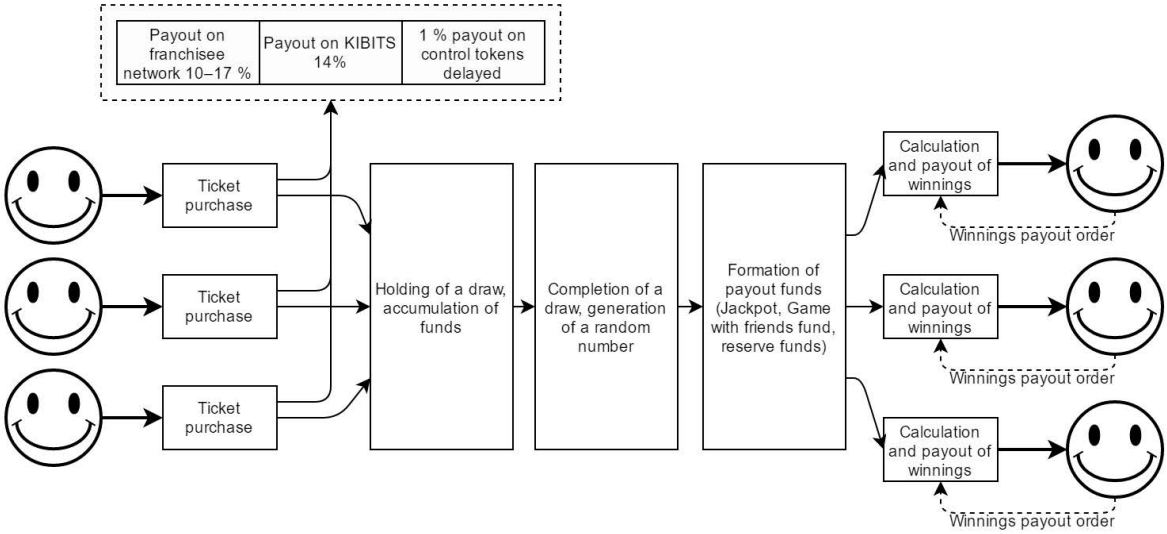
JokerBall lottery

In the JokerBall lottery, unlike in 6/49, the winning combination takes into account not only the digit, but also its position in the number. The JACKPOT is fixed and is allocated among the winners in the following way:

Coincidence	Prize
2	0.0003 % of the Jackpot per one ticket
3	0.0006 % of the Jackpot per one ticket
4	0.005 % of the Jackpot per one ticket
5	0.05% of the Jackpot per one ticket
6	2 % of the Jackpot per one ticket, but not more than 100 %
7	100 % of the Jackpot on all tickets

Random number generation is similar to that for lottery 6/49. The lottery scheme is also identical to that for lottery 6/49

7. Payout of winnings



Due to the technical limitations of the ETHEREUM network at the moment, payouts of winnings are made at the user's request (a click on the button in the user interface next to the corresponding draw).

Due to the fact that in order to make the payout, a large number of records in the contract must be sorted (since payouts on some matches are made as a percentage, that is, they depend on the number of people who guessed the given combination), the payout is not made immediately, but only after sorting all the necessary data.

For one user's payout request, 100 tickets are sorted; after all the tickets have been sorted, the actual payout to all users is launched by clicking the "payout" button (100 payouts per click). Payouts are made only to those users who have clicked the "payout" button.

Thus, in order to complete sorting and payouts on all the tickets, one out of fifty users who purchased a ticket needs to take his winnings. As the Ethereum network scales up, the number of tickets sorted in a single operation will increase.

8. Conclusion

This document presents a part of the technological and marketing solutions that are planned in the process of the KIBO platform's development. Also, as the Ethereum blockchain improves, we will actively use emerging network capabilities that will make KIBO the most reliable and extensive decentralized lottery in the world, and will provide an opportunity to all those who joined the platform at the starting period to share our success.

9. Roadmap

The launch of the KIBO platform will take place in the following stages:

1. BTC: Launch of the lottery on Bitcoin, Presale.
2. Start: Implementation of work on Ethereum franchisee account contracts, two lotteries. Start of token sales.
3. Go: Start of two additional lotteries
4. Work: System market launch, fixing of contracts.
5. GUI: Decentralization of lottery user interface (Mist)

10. List of references

1. https://github.com/alfredwoooden/kibo_contracts (Access will be open later)
2. https://ethereum.org
3. http://kiboplatform.com/ethereum_paper.pdf
4. http://kiboplatform.net/en/strategy.html
5. https://blog.ethereum.org/2015/03/03/ethereum-launch-process/