Dao.Casino

Next Generation Gambling Platform

https://dao.casino

1. Introduction

We are bringing to your attention the first Decentralized Autonomous Organization in the gambling industry - Dao.Casino.

Dao.Casino will invest the funds in games' developers, making a profit as a percentage of earned games money. On the other hand, Dao.Casino provides the developers with a convenient platform for placing games with a large flow of users.

Key parties:

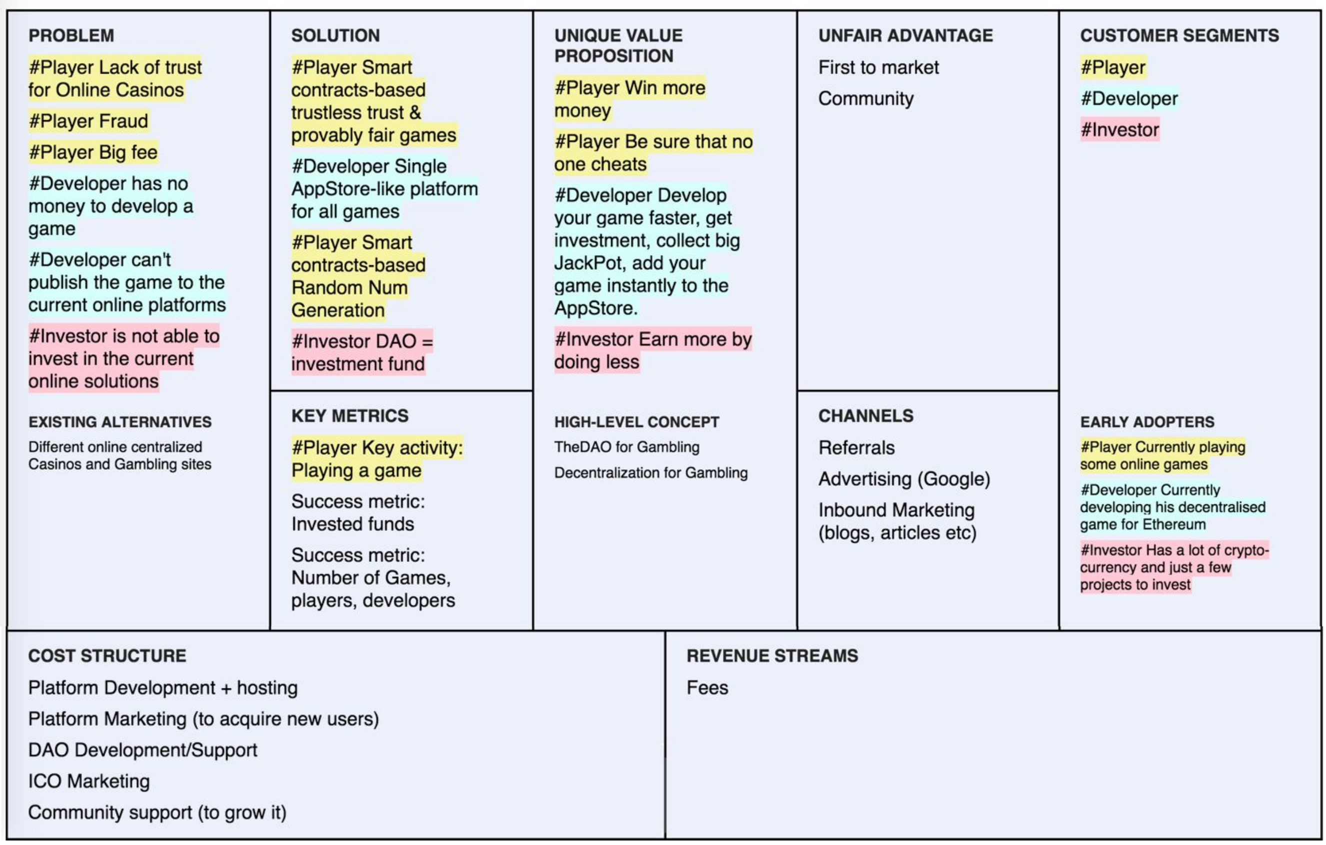
- Creators and developers of Dao.Casino;
- DaoTokenHolders (DTH) - Investors who have invested Eth funds in the Dao.Casino;
- Developers of gambling games;
- Referrers - those who bring the players to the platform / game;
- Players.

Existing problems in the market of online gambling:

- The player is afraid of fraud on the part of online casinos;
- The player cannot check the result of the draw;
- The player is forced to pay a big fee for the game;
- The developer cannot promote his product and embed it on a passable area;
- The developer does not have enough funds to develop the game;
- The investor cannot buy shares of online casino and invest therein.

Dao.Casino Objectives:

- Earn a profit for its investors;
- Provide developers with convenient tools for game development;
- Create AppStore-like platform with large flow of users;
- Raise honesty and provability of games to a new level;
- Reduce the costs for development and promotion of gambling games;
- Provide games with the big JackPot.



PROBLEM

#Player Lack of trust for Online Casinos

#Player Fraud

#Player Big fee

#Developer has no money to develop a game

#Developer can't publish the game to the current online platforms

#Investor is not able to invest in the current online solutions

EXISTING ALTERNATIVES

Different online centralized Casinos and Gambling sites

SOLUTION

#Player Smart contracts-based trustless trust & provably fair games

#Developer Single AppStore-like platform for all games

#Player Smart contracts-based Random Num Generation

#Investor DAO = investment fund

KEY METRICS

#Player Key activity: Playing a game

Success metric: Invested funds

Success metric: Number of Games, players, developers

UNIQUE VALUE PROPOSITION

#Player Win more money

#Player Be sure that no one cheats

#Developer Develop your game faster, get investment, collect big JackPot, add your game instantly to the AppStore.

#Investor Earn more by doing less

HIGH-LEVEL CONCEPT

TheDAO for Gambling

Decentralization for Gambling

UNFAIR ADVANTAGE

First to market

Community

CHANNELS

Referrals

Advertising (Google)

Inbound Marketing (blogs, articles etc)

CUSTOMER SEGMENTS

#Player

#Developer

#Investor

EARLY ADOPTERS

#Player Currently playing some online games

#Developer Currently developing his decentralised game for Ethereum

#Investor Has a lot of crypto-currency and just a few projects to invest

COST STRUCTURE

Platform Development + hosting

Platform Marketing (to acquire new users)

DAO Development/Support

ICO Marketing

Community support (to grow it)

REVENUE STREAMS

Fees

As a result, owing to the Dao.Casino, all the parties will get benefit.

1.1 Gambling games.

Online casino takes about 10% of total legal turnover of world gambling business. 60% of online casino belongs to 22 leading networks. Another 30% are subsidiaries of well-known offline casinos, and the remaining 10% is owned by private individuals. Taking into account these monopoly phenomena, the developer has little chances to attract alone the required number of audience to start its project in this market.

Internet gambling games cause distrust in most cases on the part of the players. The player is faced with the following real problems:

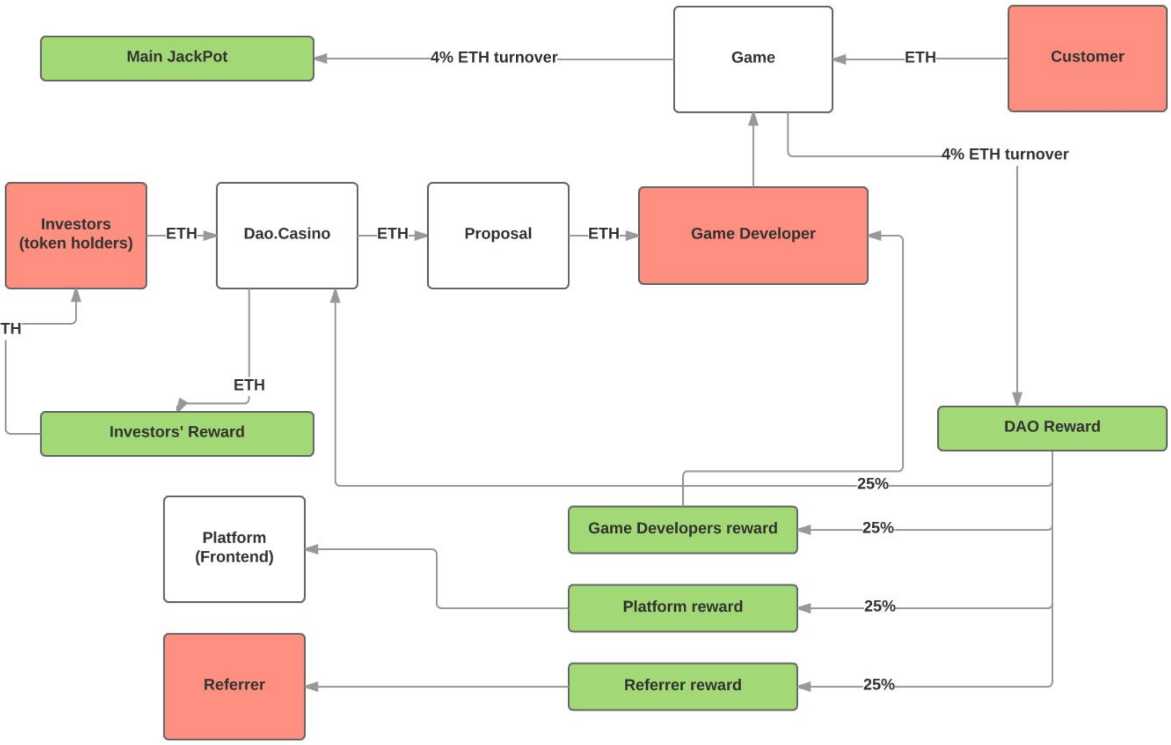
- After transferring the money to game account, it is not credited and is stolen;
- For unknown reasons, the money disappeared from the account;
- After withdrawal the money from the deposit, it has not been credited to the plastic card;
- The player has not received the promised bonuses;
- The player is not able to enter his game account;
- The casino charges a fee for the gain withdrawal;
- The player can withdraw funds only on a certain day.

Organization of gambling market based on an open code and smart contracts, using the blockchain technology is required to ensure safety. With the help of smart contracts it is possible to unite all participants of the gambling game market, and to establish commonly understood, honest rules of the game prescribed in the blockchain, in which there is no place for fraud.

2. Business Model

The objective of Dao.Casino is to create a balanced model, which would be beneficial to all the parties involved in the business process. It should be profitable for the developer to work with the Dao Casino, rather than on its own. Dao.Casino distributes the resulting sales revenue as follows:

- Developer - 25%
- Dao.Casino - 25%
- Referrer - 25%
- Platform - 25%



2.1. The developers

"Developers, developers and developers again!" - Steve Ballmer said. Placement of game in Dao.Casino will be more profitable than its independent release.

Firstly, the developers have access to a large audience. Secondly, each player will additionally participate in the drawing of MainJackPot. The developer gets 25% of the profit.

2.2. Affiliate program

The Referral is a participant of the affiliate program, signed up under recommendation of another participant.

The Referrer is a member of the affiliate program, who brought a referral.

The Referrers receive 25% of the profits for term of life. If the referrer is absent, and the player came to the platform on its own through the platform’s own channels, then the platform itself is considered as the referrer, which means that it receives the reward.

This commission will allow to compensate the costs for attraction of players, and can be also a good business model for many free applications.

2.3. Platforms

The platform is a frontend for Dao.Casino, with which the players work directly. The platform will be developed with an open initial source. Anyone will be able to launch its similar platform and connect it to Dao.Casino. See. P.5 "Platform"

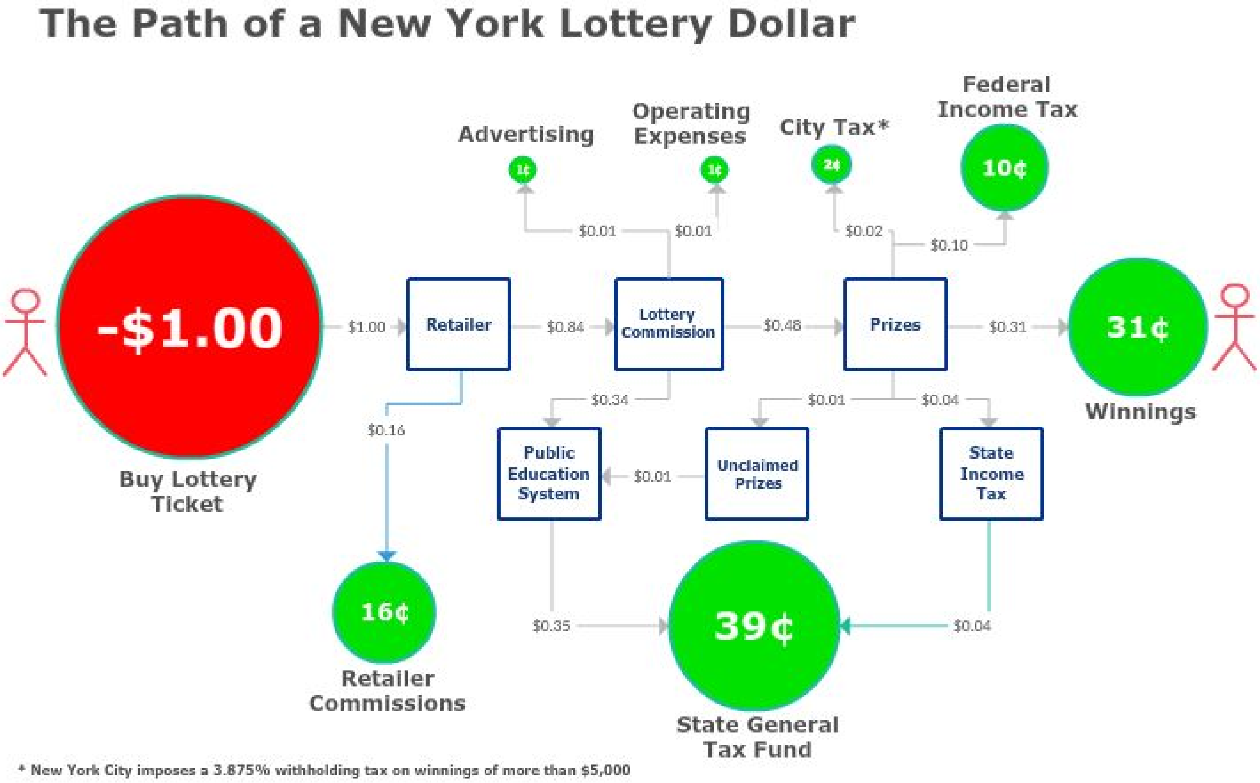
«Dao.Casino Platform» is the centralized commercial organization (Foundation), which goal is to create a platform for Dao.Casino and receive gain therefrom.

2.4. DAO

DAO Objectives:

- Provide the developers with the most reliable solution for generation of random numbers.
- Earn dividends for its contributors by investing in games / developers;
- Set game rules for all the participants;
- Ensure safety and transparency;
- Conduct an audit of contracts;
- Provide a big Jackpot for gambling games;

2.5. Lottery Example



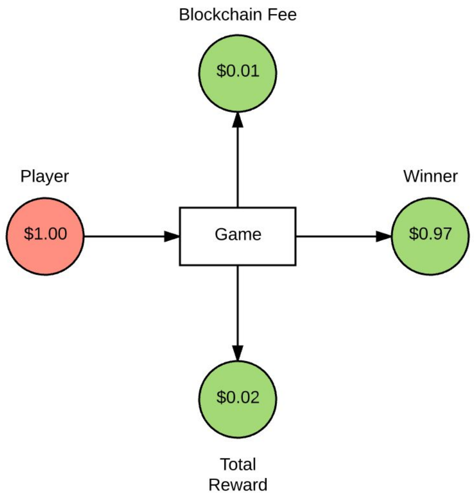
According to Visualcapitalist data, $1, received from the player in the most popular offline lottery is distributed as follows:

To sum up the math

- 51% of each dollar goes to tax revenue: federal, state, and municipal.
- 18% goes to covering expenses, such as advertising or retailer commissions. This is the part that makes the process inefficient.
- 31% of each dollar actually goes to the prize money, and that basically sums up the terrible odds behind winning in the first place.

In other words, for every $3 spent on the New York Lottery, less than $1 is paid out to winners, while the other $2 is going to expenses and tax revenues.[1]

Below is the lottery model when using smart contracts:



2.6 Advantages of smart contracts

- Due to elimination of mediators and possibility of direct interaction of the players with each other, the highest possible percentage of payments is achieved;
- Blokchain and smart contracts remove the issue of trust between the users, and eliminate the need to trust third parties. This is so-called Trustless Trust;
- Open initial code and transparent behavior;
- Payout is guaranteed;
- Players can participate from anywhere in the world (as compared to offline casinos);
- The necessity to pay taxes, as desired, in the jurisdiction of residence (compared to offline casinos).

2.7 Initial Coin Offering (ICO, CrowdSale)

Dao.Casino token distribution:

- 10% to Foundation DAO.Casino Platform.
- 10% founders reward
- 5% Future Dev.Reward

- 25% of the resulting Eth CrowdSale will be invested in creation of «DAO.Casino Platform».
- 75% of the resulting Eth CrowdSale goes to DAO fund.

2.8. Future Dev.Reward

5% of tokens is allocated for the formation of the core between the developers, who joined the platform:

1) 1% goes to the team that finds and implements the best solution for the calculation of random numbers;

2) 4% will be distributed by the founders in equal parts by 0.1% between the first 40 teams of developers, who will integrate their games in dao.casino.

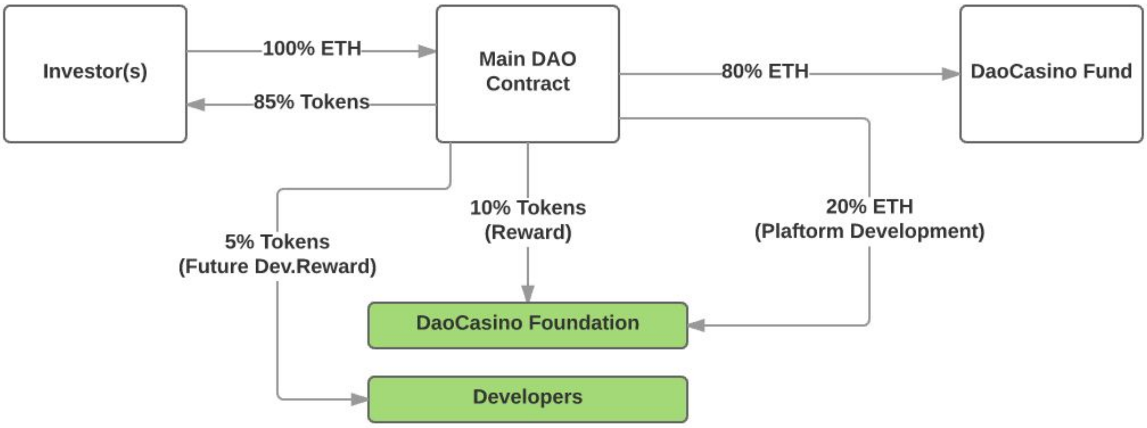
3. Obtaining random numbers

Complex technical problem in gambling games is obtaining random (RNG) or pseudo-random (PRNG) numbers. There are different approaches to obtaining such values. It is important that there exist formal mathematical proofs of the high quality of the selected generation method. Only in this case we can say that the players and the casino are protected, and the scheme of work is tested and reliable.

3.1. Definition

Pseudo random number generator (PRNG) is an algorithm that generates a sequence of numbers, the elements of which are almost independent of each other and are subject to a given distribution (generally uniform).

Random Number Generator (RNG) is an algorithm, which generates absolutely random numbers.



Such generators are mostly used for generating unique symmetric and asymmetric encryption keys. They are built mostly from a combination of cryptographically strong PRNG and external entropy source (and, namely, this combination is commonly understood as RNG).

3.2. Methods of generating random numbers in a centralized casino

In a centralized casino (online and offline) different hardware/software complexes are used that are certified for compliance with the certain standards.

Most poker rooms get special certificates to prove the viability of their RNG and software. Cigital, one of the largest companies in this field, is engaged, among other things, in certification of the poker software and RNG. The largest poker rooms Full Tilt Poker and PokerStars have the Certificate of this company. The basis of any RNG testing is a set of tests NIST (National Institute of Standards and Technology), based on US standard FIPS 140-2 (Federal Information Processing Standard). It includes various tests - from the test on ratio of 0 and 1 in the generated sequence, to the test on LZO algorithm compression (random sequence may not be significantly compressed, because it must not have many repetitive sequences).

The most common method of random numbers generating is called a linear congruential method, but there is another one - an additive congruential method. These methods generate a sequence of numbers satisfying the condition of randomness. The basis for the use of these and other methods of random number generation is the software, infinitely generating numbers, regardless of whether the participant is currently in the game or not. This eliminates the possibility for the player to independently determine the generation method, used at this moment, and "guess" the drawn numbers.

For example, the US law requires that the random number generator in the slot machines should operate all the time. In addition, the software vendors themselves deal with this issue directly.

FullTilt RNG is built on a similar principle with PokerStars, there are used 3 independent generators: hardware RNG with physical source of entropy and two independent PRNG (ISAAC and OpenSSL).

3.3. Methods of random numbers generation in a decentralized casino

Decentralization imposes high demands on the RNG.

Ideally:

1) Random numbers should be evenly distributed and unpredictable;

2) Mechanism of obtaining a random number should be maximally decentralized;

3) The possibility of intervention to fraud the lottery results should be very small.

3.4. Main methods of RNG decentralized obtaining

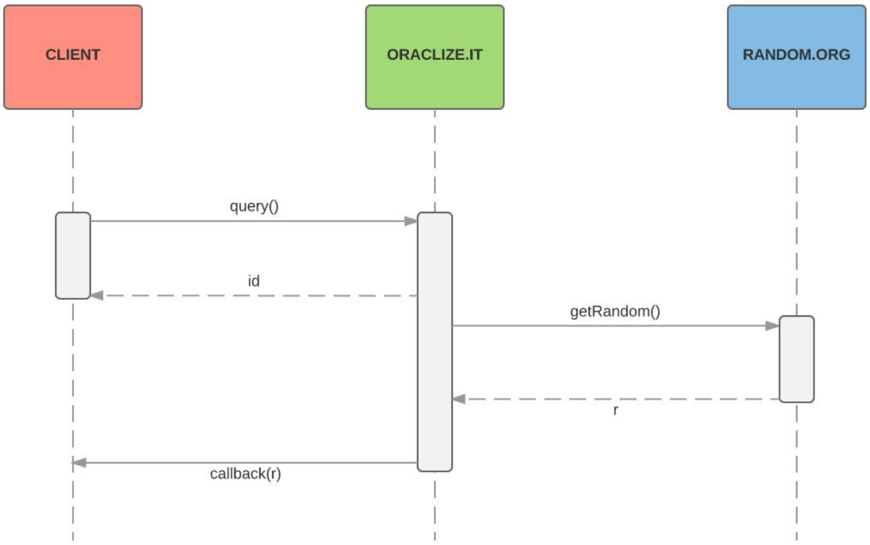
Internal method - this method involves the use of current block hash values or hash block. The main problem of this method is that there is a high likelihood of fraud. See, for example: http://martin.swende.se/blog/Breaking_the_house.html

External method - in this case, a random value is obtained from external sources. This hybrid scheme, which cannot be considered fully decentralized. One example of this approach is project EtherDice:

The only external dependency is a random number generator because the determinateness of blockchains prevents from reliable obtaining a random number in a simple manner. The idea is that the contract holds a certain amount of so-called "generations." The generation starts when one of the two sources of random numbers produces hashes of proposed values. Two sources increase the complexity of compromise, nevertheless they do not cancel that possibility completely. The hashes are saved, and the contract is waiting for some time in order the rates were obtained in the current generation. After the first bet, the generation takes next bets for some more blocks, and then closes. The contract is waiting for a few more blocks in order to put the generation in "value disclosure" regime. The sources of random numbers reveal random values (the hashes are verified), after which the players can receive the gains. Several generations work simultaneously and in parallel, so the system is able to accept bets at any time.

Oracles (external) - external generators of random numbers, they are translated into blackchain network. The weak spot of this approach - the oracles can be compromised. This approach is used, for example, by etheroll.com:

The source of random values is Random.org - which we get through Oraclize.it. The latter allows us to increase security with the help of "TLSNotary" technology, which can prove that the number was not changed after it was requested by Random.org. Unfortunately, there is no easy way to verify it directly from a smart contract. Such a verification can be made only after a certain time.

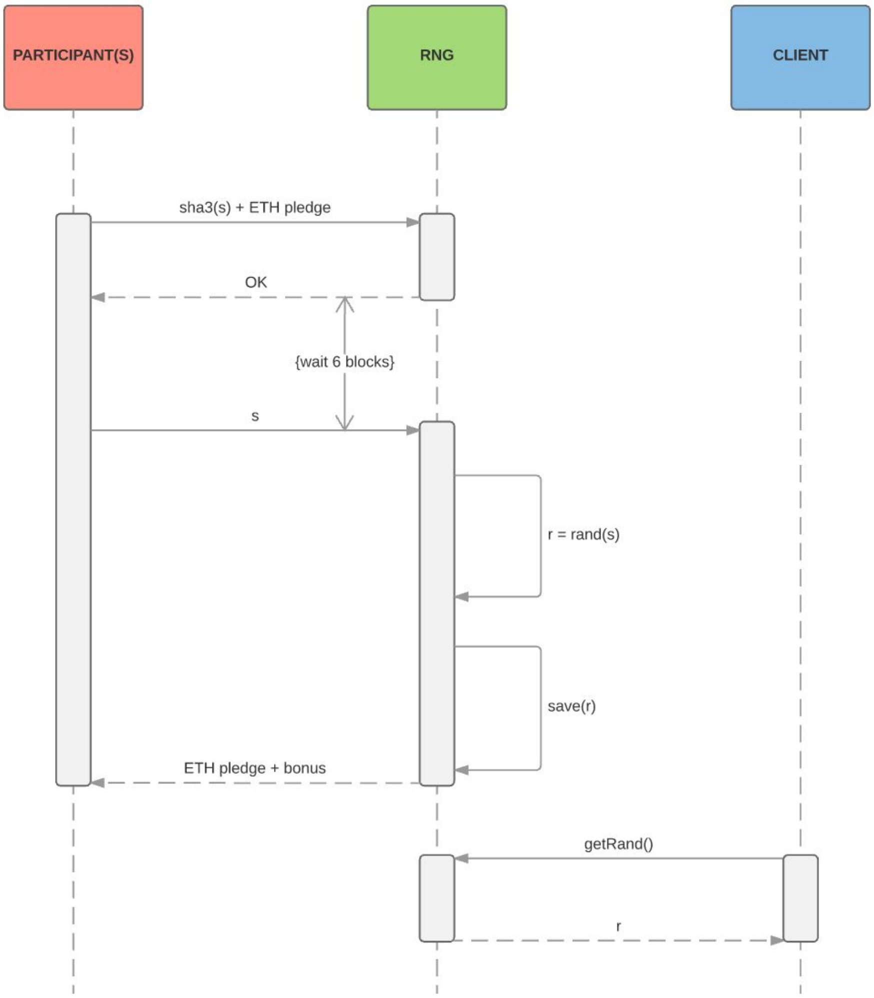


Commit / Reveal - quite an advanced distributed method for producing random values. This approach is actively used in RanDAO, Sleth, Maker-Darts.

The feature of this algorithm for finding the random values is a scheme of work in 2 steps. In the first step, the participants send hashes of random values, and deposit a pledge. In the second step, takes place the disclosure of the values, of which the resulting random number is drawn up.

If one of the participants cheats and does not disclose a proposed number, then his pledge is lost. This motivates all participants in generation to be honest.

This method is subject to DDOS attacks, resulting in the loss of pledge by fair participants.



3.5. The chosen approach

Gambling games have different requirements for the reliability of the algorithm for finding random numbers. For example, at huge jackpot drawing they are higher and at handing out cards in poker with small bets they are significantly lower.

Each of the above approaches has its own "value" of use. One of the most sophisticated, reliable, long and costly is the Commit / Reveal algorithm (RanDAO).

On the other hand, the simplest one is the internal method of finding random numbers. For example, Rouleth project uses this method, in particular. The studies have shown that cheating is possible, but it is insignificant, if the bet does not reach high values:

To fight the miners' fraud, one must choose such parameters that it would be simply unprofitable for them from a mathematical point of view. They conducted a simulation, the results of which are available on github. The analysis showed that the attacker must possess at least 3% of the capacity of the network. In this case, the attacker should spend about 23

ETH per block. This value, however, decreases as the possession of computation capacity by the attacker increases. If he possesses 10% of the network, then for the attack only 2 ETH per block is needed, and 25% of capacity decreases this amount up to 1.2 ETH. The attacker will be forced to spend 0.5 ETH, if he owns 51% of the network, but in this case, the entire network is subject to far greater danger than a simple roulette hack!

We intentionally keep the gain volume low so that for the attacker it would be economically unprofitable to practice deception. Please note, that the cheating miner can make a lot of bets per block to increase the probability of winning. Therefore, we have set the maximum number of bets per block equal to 2 (but this can be changed).

Currently in the world there are 7 pools which have a capacity of more than 3% each.

Game EthereumLottery uses a hybrid method of random numbers generation: through BTCRelay the smart contract receives a new block hash from Bitcoin network. The advantage of this approach is sufficiently high reliability, the disadvantage is the low performance of the algorithm, because the Bitcoin block is generated significantly longer than in Ethereum network.

Here is what the author of the project says:

Imagine that the JackPot is $ 5,000, and the attacker owns 5% capacity of the whole bitcoin network. Imagine that the attacker buys tickets for $ 5,000, and now owns 50% of all tickets, and the JackPot becomes $ 10,000.

At this moment, the attacker has the expectation of $ 10,000 * 50% * 99.5% (lottery takes a commission of 0.5%) = $ 4,975. In one of twenty cases (5% capacity belongs to the attacker), the attacker can replace the block, which will decide the fate of the draw.

If he finds a block, and learns that he has not won in the lottery, he drops it (which gives him another attempts), and if he wins - he sends it to the network. This increases the chances of success from 50% to 75% because only in 25% of cases 2 attempts lose.

But when the attacker drops a block - he loses the reward for mining. The losses amount to $ 4218.75, taking into account the current size of the reward equal to 12.5 BTC.

Increase of the chance to win gives the expectation equal to $ 10,000 * 75% * 99.5% = $ 7,462.50. The attacker spent $ 5000 for tickets, and lost $ 4218.75 at the unit dropping. This means that such fraud is not economically profitable. It becomes profitable only when the JackPot is more than $ 10,000.

Dao.Casino enables to generate random numbers in various ways. Afterwards, it is possible to develop the own solutions or modify the existing ones.

4. Dao.Casino Contracts

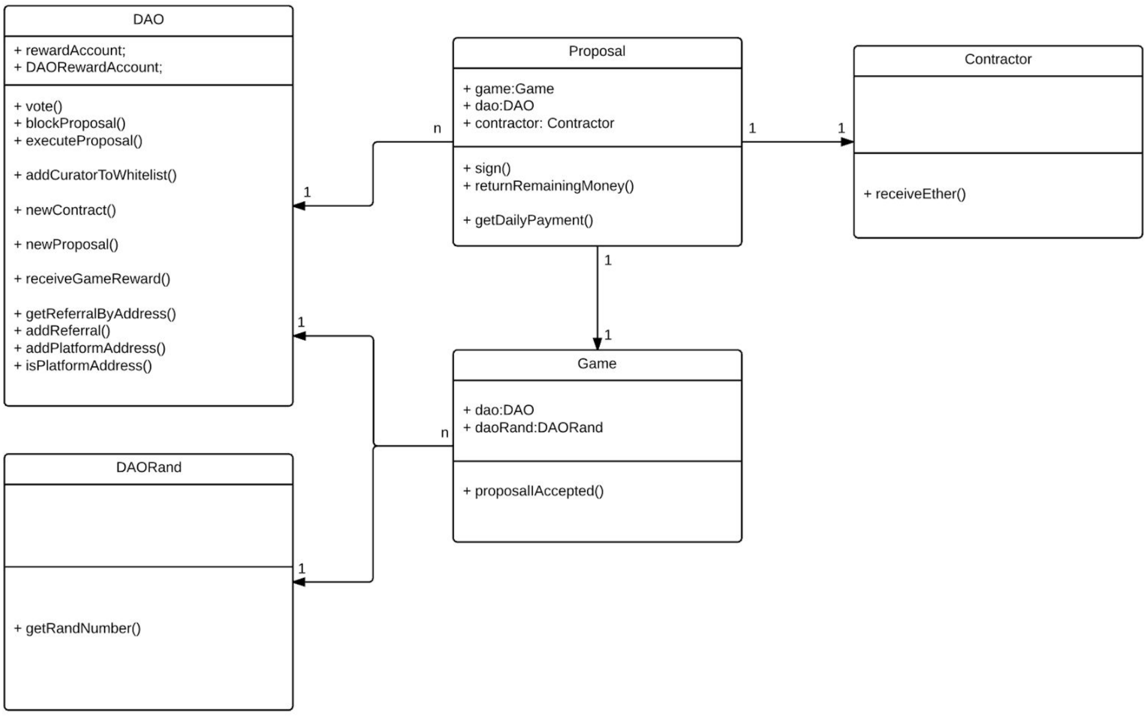
Platforms

The game can be played on many different platforms at once. Each platform will get its own fee.

Affiliate program (referral system)

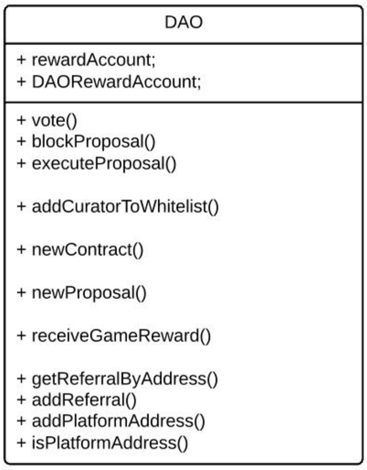
Referrers are managed by each platform separately.
Dao.Casino does not have a single “referrer <-> referal” registry.
Referrer info is passed to the game contract by the platform.

Deployment Scheme



DAO.sol

This is the main Dao.Casino contract that is used to collect funds, manage proposals, etc.



vote(uint proposalID, bool supportsProposal);

Called by the curator. Will increase pro/cons votes for the proposal.

blockProposal(uint proposalID);

Can be called by DaoTokenHolders (DTHs) in order to block the proposal even if curators accepted it (see **vote** method above).

executeProposal(uint proposalID ...);

Called by the curator after voting is complete. Will call your proposal's **‘sign**() method. Game developer can send the funds directly to game contract.

addCuratorToWhitelist(address curartor);

Called by the DAO creator. Will populate curators list with new curator item.

newContract(address newContract);

Called by a proposal (internal call) to update Dao.Casino contract with a new one. This can effectively update the main DAO contract.

newProposal(address proposalAddress ...);

It adds the proposal to DAO proposals so that curators can vote for it. DTH can block the proposal.

Duration of the voting for the new curator is 14 days and the cost of this operation is 100 Eth(in Dao.Casino tokens). The minimum quorum for re-election should be 25%. Two days before the end of the elections one can only vote against the new curator.

receiveGameReward(

address playerAddress,

address refererAddress,

address platoformAddress)

This function must be called from withtin game’s **sendRewardToDao()** method. See below.

getReferrerByAddress(address player);

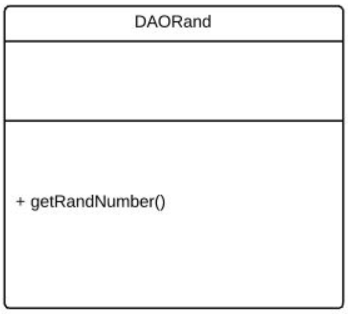
This function should be called by game to get referrer address to send reward to.

addReferrer(address player, address referrer);

This function should be called by platforms only to set the player->referrer.

addPlatformAddress(address newPlatform);

This should be called only by curatorors to add new platform address to list.
DAORand.sol

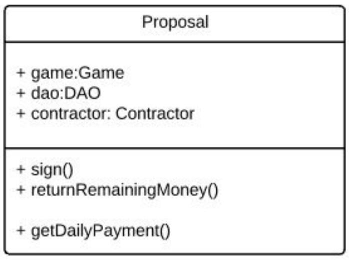


getRandNumber(...)

Can be called from the game contract. Will do the callback. Works like Oraclize.it.

GameProposal.sol

This contract is used to connect DAO.sol with a Game.sol.



sign()

Required.
This function is called when **executeProposal()** method is called by curator. That means that proposal is accepted and the game contract can be used. It should collect all funds and send it to the game contract (if needed).
Must call **game.proposalIsAccepted**() function.

returnRemainingMoney()
Required.

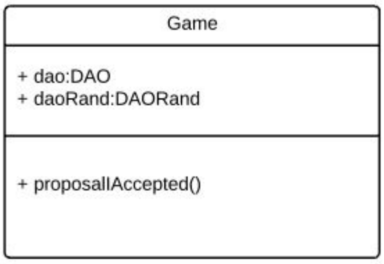
This function can be called by a DAO only to get the money back from your contract. It must send it to the DAO.

getDailyPayment()
Optional.

This function can be called by a contractor (i.e. game developer) to get daily payment (if needed). Some proposals have daily payments instead of one-time lump sum transfer. You can combine these 2 styles of payments together.

Game.sol

This is your main game contract. The ‘game.sol’ is used just as an example. You can name it ‘my_ether_game.sol’ or ‘dice_roll.sol’.



Must contain sendRewardToDao() function that:

a. Sends 25% to developer

b. Sends 25% to referer (get by calling **getReferrerByAddress**)

c. Sends 25% to platform (check that passed address is really the platform by calling **isPlatformAddress**)

d. Sends 25% to **daoCasino.receiveGameReward()** (*see above)*

proposalIAccepted()

Required.

This function is called from proposal’s **sign()** (*see above*) method when proposal is accepted. Do all game contract initialization here and if needed receive one-time funds from the proposal.

5. The platform

«Dao.Casino Platform» is an online platform similar to the AppStore (frontend) for placement by the developers of gambling games based on smart contracts. The platform displays the games and makes them available for the players. This centralized solution that addresses issues of communications with players, as well as the ranking of the available games.

«DAO.Casino Platform», on the one hand, solves the problem of developers in the search for customers, on the other hand, solves the problem of the customer in choosing the best offers from developers.

The platform software code will be fully open, which enables to create new platforms, and also constantly improve the code and ranking algorithms, to create regional versions, using the synergy of all the participants. And get from 25% to 50% of gains obtained from the players.

«DAO.Casino Platform» is designed in such a way that each user would be motivated, and the referrers, in turn, add the multiplier effect in the development of DAO.Casino.

5.1. The platform tasks

- Keep and maintain a list of games;
- Propose the most suitable games for the customer (ranking);
- Create conditions for easy entry of new customers;
- Hold and return previously attracted customers;
- Attract new customers;
- Deposit and withdraw funds;
- Maintain an affiliate program, the referrer's office;
- Propose a sample code, wikis, developers’ documentation.

5.2. Thematic priorities of the platform

- Lottery;
- Slot machines;
- Card games;
- Betting terminals;
- Betting on the events.

5.3. The platform for the developer

- Provides convenient tools for adding and integrating games (API);
- Simplifies the connection of games to DAO.Casino;
- Attracts customers;
- Wikis, tutorials, examples, instructions;
- Accounts.

6. Management

As a basis, we took TheDAO scheme, version 1.0, and improved it. We have introduced a number of additions:

1) Only curators can make proposals. To the large extent, it reminds a work scheme of corporations with a specially assigned Board of Directors. At first glance, such an approach deprives of power common owners of tokens (DaoTokenHolder, DTH - abbr.). But taking into account the existing experience of TheDAO and (for example) BitShares - voting on each proposal did not work as intended. If DTH considers that the proposal would harm him or DAO - he can always sell the tokens through a stock exchange and get his investment back or have the ability of blocking (item 3).

2) In order to motivate the curators to vote and qualitatively work for DAO, we give them 10% of the DAO profit as a reward. Payments to the curators are made once in half a year. If the curator has ceased to participate in the management of Dao.Casino or DAO owners have decided to dismiss the curator, all the accumulated funds of the curator remain in the DAO.

3) Instead of splits we have added the ability to block proposals by conventional DTH. Every token holder is entitled to vote for cancellation of the proposal within 14 days after the decision has been taken by the curators. To cancel the decision of curators more than 50% of all DTH have to vote.

4) DAO basically (but not necessarily!) makes payment after the completion of work by the contractor (those who made the proposal). This differs from TheDAO approach, where the funds are usually allocated immediately at the beginning of the project.

6.1. Curators

The number of curators - 11 persons.

Quorum - majority of not less than 6.

Functions of the curators:

- Approval of proposals;

- Audit of contracts / proposals;
- Evaluation;
- Distribution of profits of the Company.

6.2. Election of curators

The founders of Dao.Casino will initially choose 11 curators and add them to DAO. In order to replace the curator, any DTH can prepare a proposal.

The cost of adding - 100 Eth.

Voting for the new curator lasts 14 days.

The minimum quorum for re-election should be 25%.

Two days before the end of the elections one can only vote against the new curator.

6.3. DTH responsibilities

1. Introduction of new Proposals;

2. Election of curators;

3. Blocking of Proposals, quorum of more than 50% of all DTH votes;

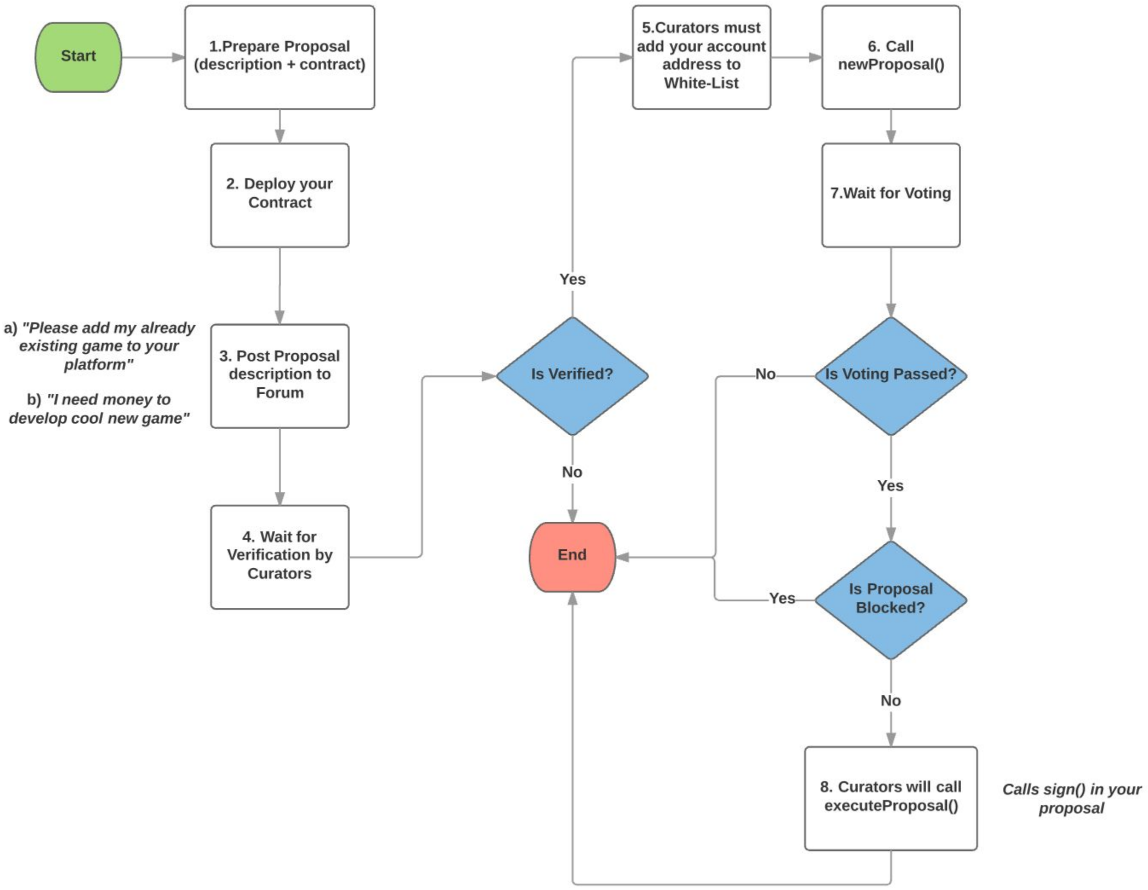
4. Voting for the transition to the new DAO contract, quorum of more than 50% of all DTH votes.

6.4. Placement of proposals

1. Only DTH can place a proposal;

2. Deposit for placement of proposal - 50 Eth. After acceptance or rejection of proposal the funds are returned;

3. The proposal must be economically profitable for DAO.


Start
1.Prepare Proposal (description + contract)
2. Deploy your Contract
a) "Please add my already existing game to your platform"
b) "I need money to develop cool new game"
3. Post Proposal description to Forum
4. Wait for Verification by Curators
Is Verified?
Yes
No
End
5.Curators must add your account address to White-List
6. Call newProposal()
7.Wait for Voting
Is Voting Passed?
No
Yes
Is Proposal Blocked?
Yes
No
8. Curators will call executeProposal()
Calls sign() in your proposal

7. Conclusion

Dao.Casino is a project which will allow to launch a new era in the industry of gambling games and lotteries. Having united, all the developers will be able to create and manage their own Las Vegas.

The developer will be able to gain more income than he would gain by running a lottery or gaming machine by himself.

The players will get absolutely transparent model of the casino, eliminating fraud and change of conditions .

The investors will get profit.

Only having united, the gambling market could become better !