
FOXCASINO
WHITE PAPER

FOXCASINO ICO / WHITE PAPER

FoxCasino Initial Coin Offering (ICO) of FXN tokens (FXN) hosted on the foxcsn.com website

White Paper

Project:
FoxCasino – Blockchain protocol for gambling.
Website: https://foxcsn.com

Abstract.
Online gambling for now is a 10% of the total legal turnover in the gambling world, while trusted third parties online casinos remain a black box for players and the market is still difficult to enter for game developers.
We offer a decentralized public system for the gambling industry.
FoxCasino consists of: a) an automated cost allocation protocol acting as an incentive mechanism and expressed in the Ethereum contract system; b) a system capable of providing equally unpredictable pseudo-random numbers for games.

We show how applying crypto-economics and implementing such a system on Ethereum can solve some common problems in the traditional online gambling industry by eliminating the need for trust (i.e., automating key elements of the online gambling industry that usually require trust, reduce the risk of fraud and exaggerate the even greater potential of the business model for development), and can also minimize overhead for casino operators, which allows higher pay-outs to players and the developers to monetize their work. The audibility and cryptographic verifiability of the software provided by Ethereum potentially simplify the certification process for gambling.

This document discusses the design and implementation of such a system from the social and technological point of view to the abstract level: the role of the participant and their interaction, the generation of random numbers for a deterministic virtual machine, the mechanisms of economic incentives for participants. We describe the MVP, which will be released in late 2017 and further development plans.

FOXCASINO ICO / WHITE PAPER

1. Introduction

FoxCasino is a protocol that defines the interactions between unreliable participants in the context of the online gambling industry. This includes two levels: the game level - the player's confidence in a particular casino operator in the context of the game (provably just gambling) and the level of the business model: that is, the game developer should not trust the casino operator to receive a reward. Simply put, all the participants who are needed for the functioning of the system, should not trust each other to cooperate.

A reliable third party that is needed in the traditional online gambling industry for work is replaced by smart contracts that act as stand-alone agents that automatically reward all key players: game developers, referers and operators of independent platforms needed to open the game. The fact that the reward system is fully automated and transparent allows you to enter the crowdfunding element into the bankroll of each game and to encourage security audits at the community level.

Obtaining the randomness necessary for gambling in a deterministic virtual machine is not a trivial task, therefore, in addition to the technical production of pseudo-random values, the level of economic incentive should be introduced. Similarly, unpredictable random numbers that determine the results in each game are provided by economically stimulated participants interacting with the PRNG contract.

This system can provide the P2P market for game developers and support a large number of independent interface platforms where players can open and play various gambling games.

At first, we can expect that existing licensed online casino operators can integrate with the protocol to reduce costs, while long-term new rules can appear, more suitable for decentralized, transparent and automated systems. The long-term objective of the FoxCasino project, in addition to providing experimental software and implementing the main components of the protocol, is to promote the development of new forms of certification of online gambling. So far, gambling on Ethereum remains in the gray legal field, but this should not be so, since technologies such as Ethereum offer opportunities for much more effective protection of customers.

Internal FXN token - FoxCasino - is used as a system of points for stimulation, as well as the sub-currency that is used in games. The FXN Token is the standard Ethereum ERC20 token.

1.1 Gambling

The legal turnover in the world of gambling reached 50 billion. In 2017, with a projected turnover of 60 billion, 60% of online casinos are owned by 22 leading networks. Another 30% are subsidiaries of known offline casinos, and the remaining 10% are owned by private individuals. Taking into account these monopoly phenomena, the developer has little chance to attract the necessary number of audience members to start his project in this market.

Online gambling games cause mistrust on the part of players in most cases, but until the development of technologies providing a platform for automating trust, such as Ethereum, there was no way to provide any alternative.

1.2. General issues in the online gambling industry

We can generalize existing problems in the online gambling industry.

Common problems faced by players:
-After transferring funds to a gaming account, they are not credited
-After withdrawing funds from the deposit, they were not credited to the card
-The player did not receive the promised bonuses
-Hidden fees: casinos charge a fee for making a profit
-The player can only withdraw funds at a certain time

Some of the existing problems in the online gambling market that the FoxCasino protocol can solve:
-The risk of fraud on behalf of online casinos
-Inability to check the result of the lottery
-High and hidden charges
-High level of access for game developers
-The high cost of running an online casino
-Posting costs for transactions, such as the integration of payment systems and the management of the balance of user accounts

2. The FoxCasino Protocol

The purpose of the FoxCasino protocol is to provide a sustainable model that benefits all parties involved in the online gambling business process. (i.e. The developer should be more profitable to use the FoxCasino protocol, rather than working independently and less expensive for the casino operator to provide the best service for the players. The players should have access to a more diverse range of games from independent developers with a higher level of security , than in traditional online casinos).

Single moments of failure - the process of transferring the cost in which a trusted third party is required in the regular online gambling business, is replaced by code sequentially executed by the Ethereum network - the intellectual contract system. These contracts - it's just an escort, which can be caused by the concrete actions of the participants and nothing else. These actions correspond to the value that participants add to the ecosystem. When there are no human subjects with administrator permissions that can change the processes of cost allocation, there is no risk that such entities can become corrupt and make changes in their favor. This code sequence is quite useful in the context of gambling.

System security is achieved through transparency, consistency and cryptographic verification of software used to automate processes related to trust and economic incentive mechanisms for its participants.

The proposed distribution of awards:
FoxCasino distributes the tokens accumulated by the game contracts as follows, rewarding all participants equally, however, independent platform operators can choose their own reward distribution scheme.

-Developer of the game - 25%
- Casino Operator * - 25%
-Referrer - 25%
-Bankrollers - 25%

*Operator / platform of the casino, game developer, referrer bankrollers can be one object

Despite the cost of required to run Ethereum-based software, the fee must remain lower than on a traditional server-based online gambling. This is due to the fact that is paid for the operation and only for the used operations and storage.

The front of the game can be stored either on the server or on the network, using decentralized file storage systems, such as IPFS on Ethereum. Using Swarm will also allow you to program the game to pay for its own external storage.

3. Goals of the FOX CASINO protocol

-Remove the need for a trusted party in all aspects of the online gambling industry
-Thus, reducing the operating costs of online gambling provides higher payouts
-Reduce the risk of fraud
-Remove the need and responsibility with online casino operators to maintain a balance of the player's account
-It allows game developers to monetize their work while keeping their IP-address
-Provides game developers access to the bankroll for their game without additional responsibility for managing it
-Includes an open ecosystem, a provably honest interactive online casino

Integrate a system of replicated patterns and a stimulated audit so that game developers who are not familiar with Solidity can take advantage of the new paradigm of value transfer that Ethereum offers.

2.1. Roles

Participants of the system.

During the initial design, we defined a number of roles that are necessary for the development and operation of the system. Some of these are common to the traditional online gambling industry, for example, casino operators, referral developers, game developers, other roles (bankroll supporters, casual providers) have been added to the decentralized architecture.

-Games Developers
-Platform Operators
-Sources
-Providers of random numbers
-Bankroll-backers
-Players
-Autonomous agents (contracts without superusers)

2.1.1. Developers

The developers refer to both game developers and contract developers. Anyone who provides a functional piece of software automatically receives tokens to from FoxCasino system in proportion to the use of this software. Independent game developers should be able to interact more effectively with platform operators, retain IP rights in the game and be able to receive lifetime rewards for their work automatically.

The developer of interfaces, capable of creating a good game, should not develop a smart contract with gambling, but use existing ones. In this case, the developer's awards will be divided between the contract creator and the creator of the front-end.

Over the past year, we have seen the growth of gambling and gambling on Ethereum. However, we cannot expect that every good game maker will learn to program for EVM, while independent game developers have a lot of talent. To use existing game development skills, proven smart contract templates can be used by several teams.

2.1.2. Platform Operators

The FoxCasino system can host multiple interface platforms that are configured for different user groups and regions. They remain independent when using the same management protocol and value exchange. Therefore, the platform level of the system is merged. Platforms receive tokens to their EOA accounts, proportional to use. If the platform attracts new players to the game, it becomes Referrer and receives rewards.

Front platforms built on the FoxCasino system should not have additional account balance systems, since balances and balance history are stored in the Ethereum block chain.

Existing operators of online casinos can create interface platforms for interaction with the token system. We can estimate that as the system develops, independent teams of game developers will be able to create groups and become casino operators with the appropriate resolution.

In a federated model, casino operators still provide value to their customers by customizing platforms for a specific group of users, creating their own ranking systems and recommendations. The operator must follow the KYC procedures required in their jurisdiction and securely store sensitive user data in accordance with the laws on the protection of personal data. The user accounts in the entire system are EOAs, the only data that is written on the block chain is their balances and tx-history.

2.1.3. Sources of information

Referrer is a member of the affiliate program that led the referral (new player). A referral is a member of the affiliate program, which was signed on the recommendation of other participant.

In a decentralized system, the opening can be facilitated by participants stimulating the economy. Affiliate programs are usually used to promote products and services. The only difference is FOXCASINO system that referrers, as well as all other active participants are being paid automatically, and can be assured that they will receive a reward. Another difference is that the reward depends on whether the referral is an active player.

Sources receive a percentage of tokens generated by the game, which they help to promote, while their referral is actively using it.

2.1.2. Platform Operators

The FoxCasino system can host multiple interface platforms that are configured for different user groups and regions. They remain independent when using the same management protocol and value exchange. Therefore, the platform level of the system is merged. Platforms receive tokens to their EOA accounts, proportional to use. If the platform attracts new players to the game, it becomes Referrer and receives rewards.

Front platforms built on the FoxCasino system should not have additional account balance systems, since balances and balance history are stored in the Ethereum block chain.

Existing operators of online casinos can create interface platforms for interaction with the token system. We can estimate that as the system develops, independent teams of game developers will be able to create groups and become casino operators with the appropriate resolution.

In a federated model, casino operators still provide value to their customers by customizing platforms for a specific group of users, creating their own ranking systems and recommendations. The operator must follow the KYC procedures required in their jurisdiction and securely store sensitive user data in accordance with the laws on the protection of personal data. The user accounts in the entire system are EOAs, the only data that is written on the block chain is their balances and tx-history.

2.1.3. Sources of information

Referrer is a member of the affiliate program that led the referral (new player). A referral is a member of the affiliate program, which was signed on the recommendation of other participant.

In a decentralized system, the opening can be facilitated by participants stimulating the economy. Affiliate programs are usually used to promote products and services. The only difference is FOXCASINO system that referrers, as well as all other active participants are being paid automatically, and can be assured that they will receive a reward. Another difference is that the reward depends on whether the referral is an active player.

Sources receive a percentage of tokens generated by the game, which they help to promote, while their referral is actively using it.

If the referrer is not available, and the player came onto the platform on their own through their own channels of the platform, then the platform itself is considered to be a reference, which means that it receives a reward. A player who wants to fill the balance of the rates may become referrer. This applies to other participants.

2.1.4. Providers of random numbers

Suppliers provide random values to contract, which then generates a value that defines and starts at the game and receives a token in exchange.

In the realized PRNG contract for both sides of the game Random Provider and Bankroll Backer - are one person. Future versions may include a hybrid system of economically stimulated oracles.

Participants in the oracle promotion system: In addition to the pseudo-random algorithm, an economic algorithm is needed to ensure that the providers of random numbers cannot use their partial access to the data used in PRNG, so that the results of the games remain equally unpredictable for all parties. Random numbers provider system is a hybrid between the generation of randomness to EVM and using the authenticated data feeds (oracles).

To participate as a provider of random numbers, the participant must: a) lock your token in the contract; b) send data to the RNG contract from which the PRNG will be created. Intentional or unintentional, malicious behavior, it is an attempt to predict the outcome of the game will result in that locked tokens will be distributed as awards to other participants. Because of this marking system of random data in some way similar to the miners in the PoS system.

2.1.5. Bankroll Backers

Any token holder can support any particular game, taking on the role of defender of the bankroll. Bankroll Backers blocks your token in the gaming contract of their choice and will automatically receive a reward.

Behavior of the Bankroll Backer may vary depending on the gaming contract and what kind of PRNG system used. In the first implementation Bankroll Backer provides FXN tokens for the game bankroll and the value of which is derived result of the game.

2.1.6. Players

Players open games through platforms and use their tokens as a game currency. A player can get a token, becoming an active participant, such as Random provider or the Referrer, or support of the crowdfunding startup campaign. The casino operator can exchange tokens to ordinary cryptoresources.

During the past year we see more and more gambling, built for Ethereum. We can expect that the early adopters will be enthusiasts of Ethereum and decentralization. Game contracts available through the Ethereum clients, but in an ideal situation, the player does not need to know anything about the Ethereum, or the technology to play and discover games.

2.1.7. Offline agents

Autonomous agents - are intelligent contracts that run on Ethereum, who perform tasks that would normally require trust.

We refer to these entities as agents, because a) their role is just as important as all the human actors in the system (with the only difference being that they cannot deceive and do not need stimulation). B) after they have been designed and deployed, they do not have a man capable of shooting tokens with balances on accounts or control contract in other ways. Instead, the contract will "decide" whether to reward the EOA, in accordance with its rules. The rules cannot be changed by one side. If the contract will be considered invalid and the rules do not satisfy the needs of the participants, it will simply be abandoned by the majority of participants or all participants. Similarly, an entire blockade can be left by miners.

All contracts that are considered part of the protocol must be autonomous agents controlled by the honest and authorized behavior of the participants. The contracts, which are deployed for crowdfunding and FXN release, are not considered part of the protocol, but it is a step in the design, deployment and improvement, and in this sense are not autonomous – controlled by legal entity.

2.2. Token system

Internal FOX CASINO token called FXN – is a ERC20 token. It is used as a game currency for all gaming contracts integrated with the protocol, and to provide the FOX CASINO reward system. Internal currency and reward system are free.

We can assume that the reward system that allows people to collect tokens, which can be used in games, provides the best incentive mechanism than a pure system of reputation points.

Overtime history of FXN accounts can be used as a reputation system and for the ranking of games and players. For example, most popular games will have more transaction history.

Keys to the rate may be stored in platform purses by players and any client or Ethereum or more advanced Ethereum users or a paper wallet. It is not recommended to store a large number of bets in the browser, although, as sub variant, it can be less prone to theft than widespread and commonly known cryptographic token, such as Ether.

Ingame amount
In traditional gaming and online gambling industry's biggest online gaming companies prefer not to have a game token that works in all games, because it violates their business model. However, when it comes to small, independent game makers, the availability of interoperable token makes sense, because it eliminates the need to maintain the balance of the user accounts. Interaction between games also makes the marker useful for players, not having its intrinsic value.

Using sub-currency based on Ethereum instead of Ether reduces the risk of attacks of the rational type on the system after scaling. If the system is compromised by an attacker, the token will be useless, so attacking the system will not be a reasonable goal.

Compensation system
As described above, all participants contributing to the ecosystem in one form or another, automatically rewarded by FXN rate to their accounts.

2.3. Main components and releases
2.3.1. MVP: The components (which will be released by the time of start of the token)
Contracts:
- Random Contract 1.0 Signidice algorithm implementation, integrated with the gaming contract below

- Game contract fxnslot integrated with the system module ref
- Hack game contract is integrated with the system module ref
- Reward Distribution contract 1.0, integrated with the above game for spread bets: referrals, developers, platform operators.
- Register of the referral contracts that calls referral contract
- ERC 20 is integrated with 1 game

Other
- Frontend test platform (only for Ethereum test network)
- The front part for 1 game.
- The legal infrastructure, conducting further research and development

The components listed above provide the minimum functionality of the system. However, a fully decentralized system requires additional components and other implementations of PRNG, suitable for multi-player games.
To conduct crowdfunding campaign will use a standard Crowdfunding contract.

2.3.2. The components that were released in later 2017 after the launch of the token
After starting FXN we can test a running system with a large number of partici pants. The percentage of the funds raised during the crowdfunding campaign will be used to implement, test, and production of the following components:

Distribution fees contract 2.0 - added reward for compensation in Bankroll Back-ers.

EXAMPLE of certificates certification for games - Register for audited addresses of gaming contract with reference to the PFS hash and its contract in Solidity.

In this release, the aspect of the bankroll is complete. The FOX CASINO proto-col is publicly available, and everyone can check the game contracts, but we cannot expect each player to read the source code. For this reason, it is useful to use the system for trusted games whitelisting. Platform operators can use their own contract for the certification of games that they have checked. During this period, research and testing of possible PRNG solutions continues.

2.3.3. Further developments
The first editions of FOX CASINO focused on the components working at the Ethereum, and the client-browser that allows you to navigate the games without the centrally located user interface.

Once these components have been implemented and tested, the focus of the project should move towards implementing new developers and make the system more attractive to traditional casino operators and more usable. Work plan for the end of 2017, starting in 2018 and beyond:

Contractual license to use FOXFactory. Smart contracts, since any software requires a license to determine the rules of use, distribution and relationship with the patented work. The unique thing about contracts is that they can be their own license and license, also part of the code. In the context of gambling integrated with the remuneration mechanism, we plan to introduce licensing based on remuneration. This means that anyone can replicate someone's Ethereum contract to the new address, while the author of the original contract still has the right to automatic compensation specified in the license.

Game Factory - system for secure replication of gaming contracts based on FOX CASINO

Our plan is to release several contract templates and documentation that allow game developers without prior knowledge of Ethereum create games.

Integrate the VR test application with FOX CASINO logic. Traditional online casinos are moving in VR, and if we want to decentralize fair gaming to the masses, we will need to release the VR / 3D applications integrated with the FOX CASINO protocol.

3.Receiving of random numbers
In the context of FOX CASINO, the same unpredictability of the results of the game, which is determined by PRNG, makes the game fair.

Getting randomness (RNG), or, more precisely, pseudo randomness (PRNG) in the context of gambling - a complex problem. There are different approaches to obtaining such values. Mathematic evidence and high quality of the chosen method are of great importance. In simple words, a pseudo-random number that determines the outcome of a game must be equally unpredictable for all parties involved. Only in this case we can say that players and casinos are protected from fraud, and this scheme is checked and reliable.

This part describes the existing methods for obtaining pseudo-random numbers in a deterministic virtual machine that were implemented earlier, and the method that FOX CASINO implements for two party games.

Earlier methods implemented using Oraclize data and the inner block chains were also tested by FOX CASINO team. These methods are viable, but cannot be considered sufficiently reliable in the long term. Therefore, in the first edition of FOX CASINO Signidice algorithm will be used, that is suitable for two party games that our team has realized in Solidity.

3.1. Definition

Pseudo-random number generator (PRNG) is an algorithm that generates a sequence of numbers whose elements are almost independent of each other and obey a predetermined distribution (usually uniform).

The random number generator (RNG) is an algorithm that generates absolutely random numbers.

Such generators are mainly used to create unique symmetric and asymmetric encryption keys. They are constructed largely from a combination of cryptographically strong PRNG and external entropy sources (and this combination is generally understood as RNG).

3.2. Methods for generating random numbers in a centralized casino

In a centralized casino (online and offline), various hardware and software that meet certain standards are used to generate randomness.

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

The most common method of generating random numbers is called a linear congruential method. As an alternative, there is an additive congruential method. These methods generate a sequence of numbers that satisfy the randomness condition.

The basis for using these and other methods of generating random numbers is software that generates numbers infinitely, regardless of whether the participant participates in the game or not. This eliminates the possibility that the player determines the generation method used at this point, and "guesses" drawn numbers.

For example, the US law requires that random number generators in gaming machines work all the time. In addition, software vendors directly address this issue.

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

3.3. Existing methods of producing random decentralized games in gambling block chain Ethereum

Random numbers must be equally unpredictable for all parties.
The mechanism for obtaining a random number must be maximally decentralized.

The possibility of interference to deceive the results of the game must be very small.

3.3.1. Internal method

Data derived from the block-chain data itself. Number of blocks, timestamps. This method involves the use of the current block is the value of the hash or hash -block. This method is not considered protected, since it can be manipulated on behalf of miners.

3.3.2. External method

In this case, the value is obtained from external sources. This scheme cannot be considered completely decentralized. Simply put, using a single PRNG source is a bottleneck. One example of this approach is EtherDice project:

The only external dependency is a random number generator, since the definition of locks prevents the safe receipt of a random number in a simple way. The idea is that a certain number of so-called "generations" is contained in the contract. Generation begins when one of the two sources of random numbers produces hashes the suggested values.

Two sources increase the complexity of the compromise; however, they will not completely abolish this opportunity. Hashes are stored, and the contract is waiting for some time to rate were obtained in the current generation. After the first bet, the generation takes the next bet for more blocks, and then closes. The contract is waiting for a few more blocks to turn the generation into a disclosure mode. Sources of random numbers show random values (hash checked), after which the players can get a prize. Several generations work simultaneously and in parallel, so the system can accept rates at any time.

The Oracles (authenticated data feed) - Another external method. External generators of random numbers are translated into a chain of blocks. This approach is used, for example, by etheroll.com. A weak point in this approach is that oracles can also be compromised.

The source of random values is Random.org, we can get through Oraclize.it. The latter allows us to increase the safety of using TLSNotary technology , which can prove that the number has not changed since it was requested Random.org. Unfortunately, there is no easy way to verify it directly from a smart contract. This verification can only be performed after a certain time.

The Commit / the Reveal - quite advanced distribution methods to generate random values. This approach is widely used in RanDAO, Sleth, Maker-Darts.

The feature of this algorithm for finding random values is a scheme of work in two stages. In the first phase, participants send hashes of random values, and lay a pledge. In the second step reveal the value of which is called the received random number.

If one of the participants deceives and does not disclose the proposed number, then his pledge is lost. This motivates all participants of the generation to be honest. This method is subject to DDOS attack, which leads to loss of promises by honest participants.

Various games of chance games have different requirements for the architecture and reliability PRNG. For more images of the jackpot are higher, and in the distribution of cards in poker with a small bet they are much lower.

Each of these approaches has its value. One of the most complex, reliable, long and expensive algorithm is Commit / Reveal (RanDAO).

On the other hand, the simplest one is an internal method. For example, the project Rouleth uses this method. The studies described below have shown that cheating is possible, but is negligible, if the rate does not reach high values.

To combat fraud miners, needs to select parameters such that they are not economically interesting. Analysis showed that the attacker must have at least 3% bandwidth. In this case, an attacker would have to spend about 23 per ETH unit. This value, however, decreases as the ownership attacker computing capability. If he has 10% of the network, the attack requires only 2 ETH per block, and 25% of the power decrease this value to 1.2 ETH. The attacker will be forced to spend 0,5 ETH, if he owns 51% of the network and the whole network is subject to much greater danger than a simple tape measure.

Game developer and architect have deliberately keep the gain level to economically feasible for an attacker to practice deception. Please note that the fraudster can make a lot of bets on the block in order to increase the probability of winning. Therefore, we have set the maximum number of bets on the block 2 (but this can be changed).

In a world as of 2017, there are 7 mountain basins whose capacity is more than 3%.

Draft EthereumLottery uses a hybrid method for generating random numbers: through BTCRelay . Contract receives a new hash block from the network the Bitcoin . The advantage of this approach is fairly high reliability, the disadvantage is the lower performance of the algorithm, since the block bitcoins generated significantly longer than Ethereum . Here is what the author of the project:

-Casino generates a new pair of private / public keys (PrivKey and pubkey) for some deterministic signature algorithm (eg, RSA).
-Casino creates intelligent contract that contains a public key (pubkey), the maximum number of participants and the generosity of the ether. (Optional: Change the casino PubKey existing smart contract).
- The player selects a room rate (B) and a random number (R) in a specific format (e.g., 20 bytes). The player can even specify the number range B, if the rules allow (odd parity against and so on. D.).
- The player sends the transaction (TX), containing the rate Ether , together with the data: B & R.
- The contract validates the format and rooms B and R. Invalid TX rejected.

- In addition, the contract checks whether the R number is * Imagine that the jackpot is $ 5,000, and the attacker owns 5% of the capacity of the entire network of the Bitcoin . Imagine that the attacker buy tickets for $ 5000 and now owns 50% of the ticket, and the jackpot is 10 000 dollars. *
- At the moment, the attacker has the expected amount of 10 000 * 50% * 99.5% (lottery takes a commission of 0.5%) = $ 4,975. In one out of twenty cases (owned by the attacker to 5% capacity) attacker can replace unit which decides the fate of the drawing.
- If he finds a block, and finds out that he has not won the lottery, he discards it (giving it another try), and if he wins, he will send it to the network. This increases the chances of success with 50% to 75%, because only 25% of the 2 attempts to lose.
- But when the attacker throws a block - it loses the reward for mining. The losses amount to $ 4218.75 USD. With the current remuneration equal to 12.5 BTC.

3.4. The algorithm implemented in the MVP of the FOX CASINO protocol
For our first issue, we have decided to implement, and test an algorithm Signidice , proposed for decision in a deterministic PRNG virtual machine and described Gluk256, which proposed a number of other solutions.

Game released for testing to the start time will use this algorithm. We previously tested the external method (using Oraclize) and internal method described above to test games, but chose this particular method. Signidice been proposed for the games based on Ethereum using ether. Our implementation is adopted for use FXN . " Ether generosity " , referred to in the algorithm below, it is also replaced FXN . Bounty - is, in fact, the layout system.

This algorithm is suitable for those games based Ethereum , where the outcome of each round, the player depends only on the RNG, and (optionally) the number selected by the player, but not from the actions of other players. For example . It may be suitable for roulette, slots, and so on.

D., but not for those games where the outcome depends on the other players, or only on their number, as it can be in the sweepstakes. For example, the roulette game can be modeled as a series of rounds in which one player plays against the casino. In this case, a pseudorandom number may be generated by the following algorithm.

- Increased chance of winning gives the expectation in the amount of US $ 10 000 * 75% * 99.5% = 7,462.50 dollars. The attacker spent $ 5,000 for tickets and lost 4218.75 dollars per unit. This means that such fraud is not cost-effective. He becomes profitable only when the jackpot is more than 10 000 dollars.

- Casino generates a new pair of private / public keys (PrivKey and pubkey) for some deterministic signature algorithm (eg, RSA).

- Casino creates intelligent contract that contains a public key (pubkey), the maximum number of participants and the generosity of the ether. (Optional: Change the casino PubKey existing smart contract).

- The player selects a room rate (B) and a random number (R) in a specific format (e.g., 20 bytes). The player can even specify the number range B, if the rules allow (odd parity against and so on. D.).

- The player sends the transaction (TX), containing the rate Ether , together with the data: B & R.

- The contract validates the format and rooms B and R. Invalid TX rejected.

- In addition, the contract checks whether the number of R already used by that player in the previous rounds, and in this case the TX rejected. (This step is necessary if the contract is re-used for multiple rounds of the game).

- Contract combines the random number R with a public location (A) account Ether Ether player that sent the TX: V = A + R. The resulting value V is stored in the contract. Size V is always the same: the amount (V) = size (A) + size (R). In this step rounds the result (win or loss) becomes deterministic.

- casino must sign the summary of V with its PrivKey , creating a digital signature = S sign (PrivKey , V) and sending a corresponding TX, containing S.

- Contract restores the actual public key (K) from the digital signature S and verifies that it is equal to the previously published pubkey (the K == pubkey). If not correspond APK PubKey , or if the casino does not perform step 8 for a predetermined time interval, this amounts deception. In this case, the contract sends the player generosity with the initial rate, and the contract is closed through suicide. (In case of multiplayer games bounty is distributed among all players).

- Contract S uses as seed for the predetermined algorithm PRNG (for example based on SHA-3), which creates a lucky number (L), for example. Between 0 and 36.

- If B matches of L, the player wins, otherwise the casino wins. Contract sends bid winner.

- Now, the casino may close the contract and recover the bounty, or to initiate a new round of the game. Alternatively, the contract may be programmed to automatically switch to the next round if the casino will not close it.

After the casino has chosen PrivKey , his actions are determined. A player cannot predict the result of the digital signature, and therefore his choice a random number R may affect the result only in the same way as roll dice in real life (hence the name of the algorithm). Thus, none of the participants cannot manipulate the results in any significant way.

Bounty, which shall enter into a casino with a contract must be sufficiently high to compensate for any potential players the opportunity loss. The time interval should be long enough so that it could occur any violation of the network. Although it gives the casino the opportunity to delay the result, he has no incentive to do so, because the result is still deterministic. Postponement without a valid reason will only lead to reputational losses, while the financial benefits possible. If the casino wants to keep a good reputation, he can even intercept TX player before the next block of the webcast will be launched immediately calculate the outcome of the game and reward the player, if he wins, even before it happens step 7 (to the corresponding TX is included in the following mined block). Instant gratification will also help prevent reputational losses in the event of a long delay (eg due to a network failure). It may also allow the player to start a new round, not waiting for the next block to be produced.

The same clever contract can be reused several times, provided that the player never chooses the same number R twice (or he can predict the outcome). Consequently, the need to step 5 - shall reject any contract TX, where the same double-player uses the same number of R in one and the same contract. Alternatively, the casino can regularly change the couple PrivKey / pubkey , publishing pubkey before each new round. But this requires additional TX, which leads to unnecessary delays and extra transmission costs.

Nothing should prevent multiple players to simultaneously use the same smart contract. Different players selected even number N, the previously used by other players: V is unique since A unique. The number of possible participants is limited only by the reward that the casino wants to do.

The game of roulette at an online casino is used merely as an example. Algorithm Signidice can be used in any case where a transaction takes place between the two parties. In this case, Signidice better than RANDAO: players do not need to trust the oracle (in the case of an external oracle) and not to disturb the next round of the game, refusing to disclose the number of fixed (if the players are oracles).

4.Team

Roman Tokarev - Full Stack and Game Developer.

He graduated from the Taganrog College of Marine Instrumentation, I am currently a student of the Southern Federal University, actively engaged in scientific activities. Certified specialist in the field of network technologies (cisco ccna routing and switching, cisco ccna discovery) and business (certificate of the bank center invest). More than 5 years I have been engaged in web development. Freely I know PHP, JS, CSS, HTML, C, C ++, CLR, Sign with perl, python, solidity.

Quote: “We will make a secure system and a zone of trust for both sides of the online gambling market!”

4.1 Team

Kirill Romanenko - Protocol Architect and Blockchain Developer, Game Developer.

Graduated with honors from Taganrog College of Marine Instrument. Making. Student of the Southern Federal University. Certified Expert in Network Technologies (cisco ccna discovery). I develop on JS, CSS, HTML, C, C ++, Java, Solidity.

Quote: “Our future is the future of Blockchain!”

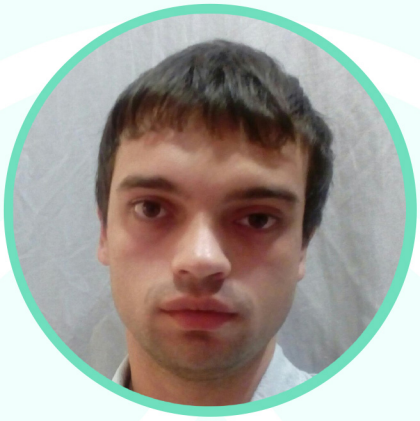
4.2 Team

Stanislav Aleynikov - Branding and Games Design.

With dignity he graduated from the University of Contemporary Art.
He has extensive experience working with major brands and branded agencies in the field of graphic design and branding. Worked with: Vodafone, Joyable, Zomato, Netflix.

Quote: “We wants to make this casino truly unique, combining stylish design and modern musical accompaniment!”

4.3 Team

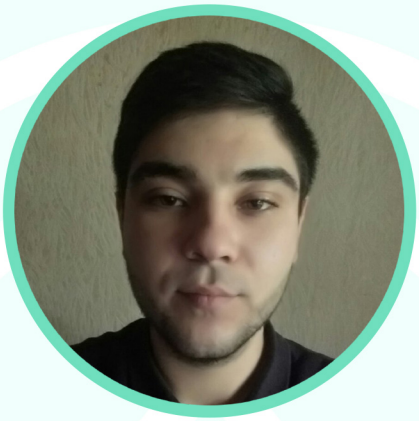


Alexander Alexandrov - Marketing Executive and Project Manager.

With dignity he graduated from the University of Marketing.
Actively engaged in scientific activities. Certified specialist in the field of network marketing and business (certificate of bank center invest). More than 4 years of experience.

Quote: “Marketing is not about your agency winning awards. It's about your organization winning business!”

4.4 Team



Roman Svetlichny - Sound Designer and Musician.

Graduated from the Rostov State College of Arts with honors. Actively develops his skills in music and writes his own compositions.

Quote: “Music will be one of the key moments in the game process, we make a modern online casino!”

Conclusion
We believe that the game of gambling with intelligent contract is gaining momentum, we believe that the options of using gambling for Ethereum can be developed outside of a few experimentally demonstrable games, stable ecosystem - a foundation that is suitable for all aspects of the gaming industry.

To do this, you must solve three issues:
There should be a system of incentives for all parties that enhance the value of the system. In addition to demonstrable fairness of the game, it will contribute to the acceptance and further development.

Reliable PRNG. Most likely, the different sources of randomness for different games and, most likely, provided the economy, not just the technical aspects.
Must be a way for game developers to create games on Ethereum without deep knowledge of Solidity : replicated contracts templates, samples, and documentation.

Must be a way to start the platform operators to create a platform that connects to Ethereum and displays the game from independent creators without a deep and detailed knowledge about the Ethereum ecosystem.