

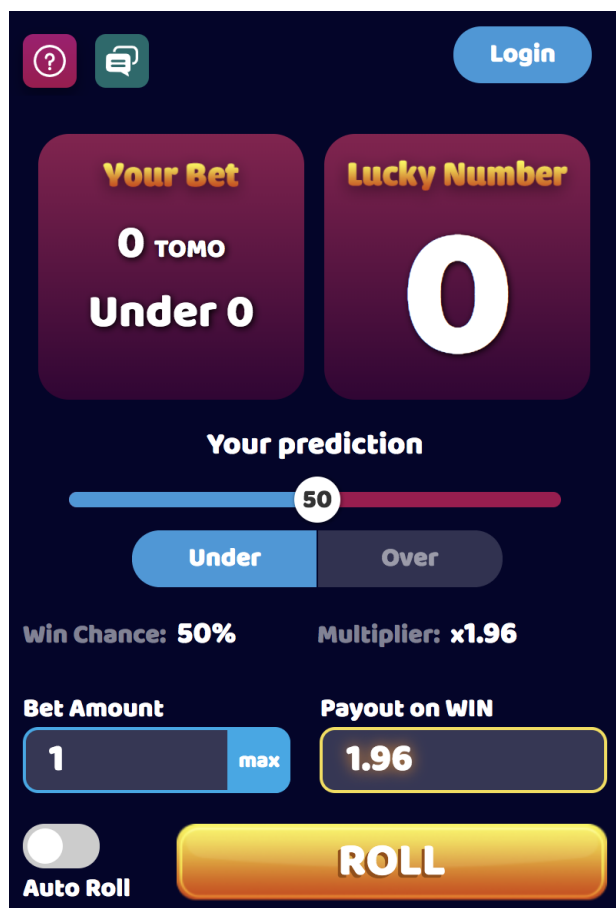
01. THE UNIQUENESS OF MAXBET

The gaming industry has been becoming increasingly widespread and popular in entertainment. Gambling games including those in Casinos as well as online games become popular. While most existing games achieve somewhat user payment security through integration of mainstream payment systems such as Paypal or MasterCard, some issues related to fairness and transparency lie in the centralized architecture of those systems. It is not uncommon that in most of those centralized gambling systems, e.g. a dice gamble, players do not know how the interacting system draws a lucky number for the game. Cheating in those systems is not a surprise.

Recent emergence of blockchain technologies opens new opportunities for transparency for those gambling systems. Several blockchain-based gambles have been developed and its appearance has been spread to a significant number of players, compared to other decentralized application types. Typical gambles are TronDice and EtherRoll run on the Tron blockchain and the Ethereum blockchain, respectively.

While the fairness and transparency of those blockchain-based gambles have been improved, compared to the classics, most of those blockchain-based gambles rely on a certain oracle service such as Oraclize to generate random numbers, or operate under the host-player model. While relying on an oracle service provides the gamble with a sufficient level of fairness, the gamble turns out to be dependent on the used oracle service, thus resulting in a relatively centralized gamble where the result can be influenced by the oracle service operators. Furthermore, the single host-multiple players model also tends to be centralized in itself.

MaxBet aims to become a new standard dice game run on the scalable TomoChain blockchain with its innovative decentralized solutions for its underlying economics mechanism. Instead of having a single host, there can be multiple hosts, namely investors, staked into the gamble smart contract. On the other hand, the randomization function in MaxBet is designed with rigorous security and decentralization considerations, which will be detailed later in this document.



The screenshot shows the MaxBet game interface. At the top left are a help icon (?) and a chat icon. A blue 'Login' button is at the top right. The main area has two purple boxes: 'Your Bet' showing '0 TOMO Under 0' and 'Lucky Number' showing '0'. Below these is a 'Your prediction' section with a horizontal slider set to 50, and 'Under' and 'Over' buttons. The 'Win Chance' is 50% and the 'Multiplier' is x1.96. At the bottom, there's a 'Bet Amount' input set to 1 (with a 'max' button), a 'Payout on WIN' box showing 1.96, an 'Auto Roll' toggle switch, and a large yellow 'ROLL' button.

02. THE STAKING SYSTEM

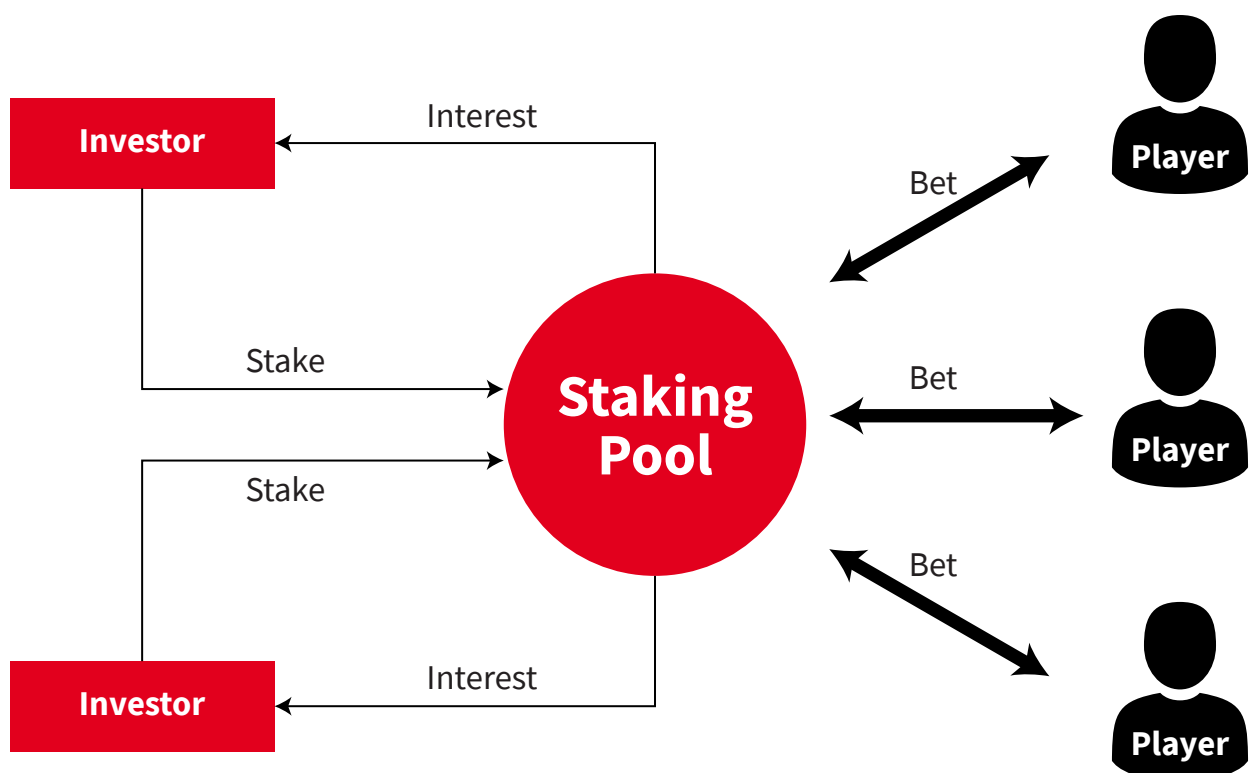
We design the most sophisticated and decentralized Dice gamble where there are not only one host, but many hosts that can stake into a staking pool. There are two types of actors. **Any TOMO holder can become an investor by making the deposit, which is technically done by sending a transaction with a minimum investment amount to the MaxBet smart contract.** The current minimum investment amount is set at 500 TOMO.

There is a limited number of investors in the Staking Pool, which is currently 15. That means, **if there are more than 20 investors staking into the pool, the top 20 investors with the most TOMO staked become the investors, which can earn profits based on the results of the game.** The mechanism is inspired by the voting and rewarding system of TomoChain.

The amount of TOMO staked by investors is locked in the smart contract, but can be withdrawn at anytime. **Each withdrawal of investors is taxed by a rate of 10% of the profits of the staker plus 10 TOMO.** It means if the pool and the withdrawing staker are losing, there will be only 10 TOMO for withdrawal fee. The withdrawal fee is sent to MaxBet's foundation account - the PigFarm team for development and marketing.

If an investor decides to quit the staking pool by making a withdrawal transaction to the smart contract, another waiting staker will automatically be promoted to be an investor.

The Staking Pool has the MaxBet main smart contract, which allows investors to stake/invest into the system and players to send their bets



03. THE PLAYERS

Typically, a player selects a number in between 1 and 99 as the betting number (betNum) and guesses whether the lucky number to be under or over the betting number (rollType=UNDER or OVER). Depending on the betting number, rolling type and the lucky number (luckyNum), **the winning amount for a player with the betting amount (betAmount) computed as follows:**

$$\text{WINNING AMOUNT} = \frac{100}{\text{betNum}} * \text{betAmount} * (1 - \text{houseEdge})$$

if luckyNum < betNum & rollType = **UNDER**

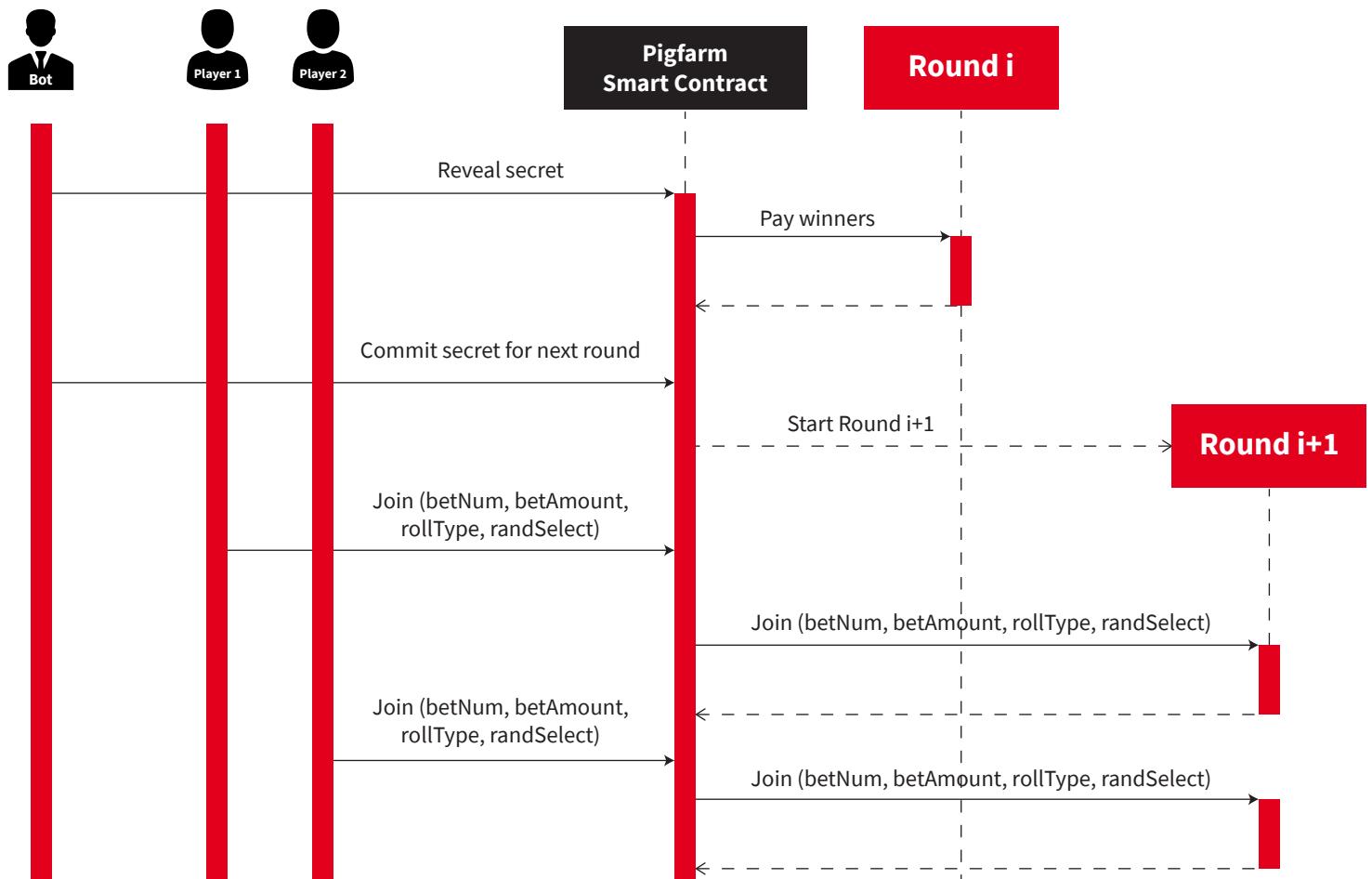
$$\text{WINNING AMOUNT} = \frac{100}{100 - \text{betNum}} * \text{betAmount} * (1 - \text{houseEdge})$$

if luckyNum >= betNum & rollType = **OVER**

There is a minimum betting amount, which is currently set as 0.1 TOMO.

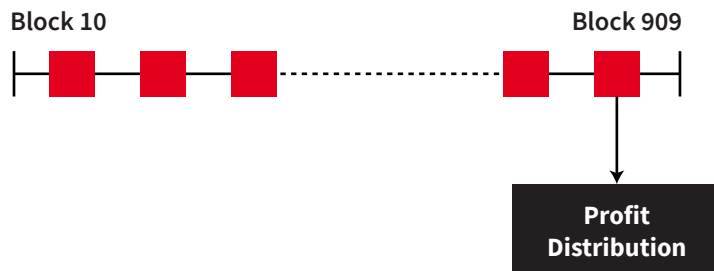
In each block, there will be a single game/round started. Any player can join the game by using our mobile friendly web application at maxbet.pigfarm.io to send a betting number, the rolling type, and a seed number, namely randSelect that will be used for lucky number generation. If the game is started at block i, it will be settled at block i+1.

The lifetime of a game/round is within a block. That means if a betting transaction is not included in the current block, it will not be part of the game/round in that block. The settlement of the game at block n is done at block (n + 1).



04. REVENUE SHARING MODEL

Revenue of the Staking Pool in MaxBet is shared between the investors, based on the staked amount of the individual investors. The revenue sharing will be computed once every 900 blocks. The set of investors dynamically changes every 900 blocks or if a new investor or an existing investor stakes more than the least staked staker of the top 20 stakers, depending on the staked amount of individual investors. During the period of 900 blocks, if an investor opts to withdraw from the pool, the investor won't receive profit in the next revenue sharing computation. Note that, the revenue sharing is all executed in the MaxBet smart contract to ensure decentralization.



05. LEADERBOARD

There is a leaderboard prize that pays to the player who has the highest betting volume. The prize is contributed by 0.1% fund of every bet. The prize will be given to the leader every 43200 blocks, approximately 1 day.

06. SMART CONTRACT SETTINGS

Parameter name	Value
House Edge	2%
Maximum payout per bet <small>Max payout can be changed by the game operator</small>	if (pool > 1000000 TOMO) payout = 500 TOMO; else if (pool > 500000 TOMO) payout = 200 TOMO; else if (pool > 200000 TOMO) payout = 100 TOMO; else if (pool > 50000 TOMO) payout = 50 TOMO; else if (pool > 20000 TOMO) payout = 20 TOMO; else if (pool > 2000 TOMO) payout = 10 TOMO; else payout = 5 TOMO;
Minimum amount per bet	0.1 TOMO
Leaderboard Prize	0.1% of Total Volume, sent to the player with the highest volume every 43200 blocks
Withdrawing fee	10 TOMO + 10% of Staker's profit
Profit sharing period	900 blocks
Maximum number of stakers	20
Minimum stake amount	500 TOMO

07. SECURE RANDOM NUMBER GENERATIONS

MaxBet relies on the commit-reveal scheme with some customizations for better user experience to generate lucky numbers. For better understanding, let us define some common terminologies:

- Commit-reveal scheme is done through two steps:
 - Commit: Send a commitment to a secret value to smart contract. Commitment might be simply the SHA3 of the secret value so that the sender cannot change the secret value later.
 - Reveal: Send the secret value for the smart contract to verify with the previously submitted commitment.
- Round: A round consists of all bets within a block. A round is considered settled if the secret value has been revealed in the reveal phase of the commit-reveal scheme.
- BlockHash: while using block hash as a random number is bad in current blockchains because it might be manipulated by miners, block hash in TomoChain is quite different and hard to manipulate. It is because TomoChain relies on the double validation mechanism. In this latter, once a block is created by a master-node, another randomly selected masternode will modify the signature part of the created block and recalculate the block hash. That means, the masternode block creator is the one which decides which transactions to be packed into the block, but not the one which determines the block hash (because it depends on the signature of the random masternode). On the other hand, the random masternode determines the finally computed block hash but cannot decide which transactions to put in the block.

There will be a commitment-secret pair per round. For simplification, each round is identified by the number of the block in which all bets

for the round happen. The commitment for round x at block x is sent to the smart contract before the block x is created. There is a secret reveal transaction sent to the smart contract to reveal the secret number in the previous block. It turns out that bets in block x will be settled by the reveal transaction in the next block. Knowing that TomoChain's block time is 2 seconds, MaxBet provides the best user experience for players.

The lucky number for round X is computed using the following formula:

$$\text{LuckyNum} = \text{Secret_X} \text{ xor } \text{BlockHash_X} \text{ xor } \text{RandSelect}$$

- **Secret_X:** the secret number committed to the round at block X
- **BlockHash_X:** the hash of block X
- **RanSelect:** the seed number, **randSelect**, submitted by users having participated in round X

The above random number generation scheme is secure because of the following reasons:

- **Masternodes-manipulation resistance:**

As previously described, block hash in TomoChain is somewhat more secure than in Ethereum because of the double validation technique. However, two masternodes still can hand-shake with each other to manipulate the result. In our scheme, LuckyNum is dependent both on a secret and blockhash. It is not feasible for masternode to guess the secret through the commitment, thus being unable to manipulate the result.

- **The bot which sends the commitment and reveals the secret cannot control LuckyNum.** This is because the bot cannot manipulate the block hash. This is critical in order to ensure fairness and avoid any manipulation in the staking pool.

MAXBET

**A PROVABLY FAIR, SECURE, AND UNIQUE
“BETTING AND STAKING” GAME**