DICE2.WIN WHITEPAPER

DICE2.WIN TEAM

Abstract. This is a stub. It is meant to reside at `https://dice2.win/whitepaper.pdf` while *dice2.win* team works on a new whitepaper with detailed formal proofs and full coverage of specifics of operation. This should be available by 16 Sep 2018, and possibly before that date. Until that date, it is just a rendition of the official FAQ in PDF form.

1. What is provably fair on-chain gambling?

Simply put, provably fair means that any bet outcome can be independently verified and that the operator or other players have no means of tampering with the result.

2. Is *dice2.win* provably fair?

Yes. The whole gameplay is controlled by Ethereum Smart Contract that computes random numbers based on operator inputs and blockchain data (block hashes). Any party can audit the contract as well as inspect any transaction to make sure that neither *dice2.win* nor malicious players are influencing the results.

3. How are you different from the other gambling sites?

Placing a bet on *dice2.win* has much lower transaction fee compared to competing websites — this allows supporting bets as low as 0.01 ETH. Our games are very simple & easily understandable, just like tossing a coin or rolling a dice.

And, of course, we have jackpot!

4. Is there any catch? Explain how it works like I'm five.

This is where we have to get a bit technical:

: *dice2.win* picks a secret random number and provides you with its hash.
: You send your bet in Ethereum transaction to our smart contract along with the hash from previous step.
: At this point *dice2.win* has already commited to a number, prior to you chosing an outcome.
: Once your transaction is confirmed by the network, the contract stores the hash and bet details.
: Our croupier bot "reveals" the number by sending a bet settling transaction.
: The contract accepts the transaction if and only if the hash of provided number is the same as the stored one.
: The contract mixes the number and block hash of the bet transaction to get a random number.
: The contract decides whether you won or lost and sends you the winning amount of Ether.

Can *dice2.win* tamper with the results? Nope, as the contract keeps track of secret number's hash, meaning the operator cannot change the number after the bet has been accepted. Mixing the block hash with the numbers makes the result totally random yet disallows miners from crafting winning bets. On the other hand, *dice2.win* themselves cannot control bet outcomes either because of block hash component. This is a well-known "commitment scheme" which enables *dice2.win* to provide gambling-grade random number generation allowing for big bets, jackpots and quick settlements while being fully transparent.

5. What if I want to really verify that everything you say is actually true?

Feel free to study our Smart Contract - it's available on Github. In case you have any questions or hesitations, drop us a line via Telegram, Twitter or e-mail.

6. What are the fees?

Every bet is deducted 1 % (but no less than 0.0003 ETH) in favour of the *dice2.win* (to help us pay the bills and keep the game running) and 0.001 ETH more gets accumulated in the jackpot for bets of 0.1 ETH and up (which also makes these bets participate in jackpot!)