PROVABLY
FAIR GAMING
EXPLAINED

Provably fairness is the process which allows players from all over the world to manually and personally verify the fairness of the games that they're playing online. In order to achieve this, casinos that work on the blockchain use a special code called the provably fair algorithm.

The algorithm generates an encrypted key with the end results of the game, sends it to the player alongside another key that will allow them to verify the correctitude of the games at the end of the session.

Provably Fair Casino VS. Regular Casino

Provably Fair Casino

- Use the provably fair algorithm that generates the hands and keeps them in a hash that can later be verified by players;
- Don't need to use third party companies thanks to the provably fair algorithm and the blockchain, which is a public ledger.
- Don't need to use third party companies thanks to the provably

Regular Casino

- Use random number generators for the outcomes of hands that are played;
- Don't allow players to personally verify the correctitude of the hands that are played;
- Are only trustworthy if you trust the third party companies that review casinos for legitimacy.

fair algorithm and the blockchain, which is a public ledger.

- Thanks to the provably fair algorithm and the blockchain, which is a public ledger, they don't need to be acknowledged by authorities.

HOW DOES PROVABLY FAIR CASINO WORKS?

There are more than one ways to implement the provably fair method to online casinos. We will stick to the most common one here. The algorithm calculates a roll-result each time there's a new hand that's been played, by using three variables:

- **Serverseed**: this is provided by the casino itself;
- **Clientseed**: this is provided by the browser you're playing on;
- **Nonce**: with each new hand, this variable increases by one so you can keep track of which hand is which by the end of the session.

Before you start you will get a hash of the serverseed, which is encrypted. This hash contains the entire game you're about to play, so the casino cannot change it no matter what. Also, because it comes to you in an encrypted code, you yourself cannot calculate any results for the hands you're about to play.

VERIFY THE RESULTS

When you start playing, you're not getting the unhashed serverseed beforehand. That would imply you being able to read it and play all hands as a winner given that the seed holds the information about all of the results of the hands you're about to be dealt. Instead you will get a hashed serverseed when your session is over, which you will use to reveal the old, unhashed serverseed. In order to verify if you've been cheated on or not, you have to go through 2 easy steps:

- Step 1: Make sure that the hashed serverseed that the site is throwing at you is the actual hash of the unhashed serverseed. If this is the case, you're fine. You know that the site has given you the right serverseed and you can go ahead and verify the fairness. For all you know, the site can be throwing a fake serverseed your way.

  To verify the seed, use an online tool like Xorbin to generate the SHA256 hash of the unhashed serverseed. Once you do that, you can check to see if the two hashes are the same. If they are, you can calculate the results and compare them to the ones provided.

- Step 2: You will have to generate each roll result by yourself, and then compare it to the rolls you made on the site. This will take some time if you’re doing it manually, which is why it is better to use an online tool and speed things up.

Data

287d5d2ddd365f54759283a8097ab — Unhashed

SHA 256

4tb59780d512265230d5efb3cc2388 — Hashed

CALCULATING WITH THE NONCE

There can be tens, hundreds, even thousands of bets one makes during one session. Which makes manual calculations and comparing the results of the serverseed with your actual results a tad hard.

The best thing you can do is to use a provably fair verifier. Most of the popular sites that deal with provably fair games have verifiers, so you can easily make sure the rolls or hands played were dealt fairly.

Result

We generated the same server seed hash.
Check if the rolls are correct.

Your Rolls:

Nonce: 3 - roll: 27.76
Nonce: 2 - roll: 74.44
Nonce: 1 - roll: 61.18
Nonce: 0 - roll: 79.69

VERIFY YOUR CALCULATIONS

All one has to do is to come with the seeds and the number of bets that have been made and then let the verifier check the serverseed hash and come back with the list of results.

The list can be compared to the results at the casino. If the results match, provably fair algorithm is implemented correctly and that the games you have played were completely fair.

PROVABLY

FAIR GAMING

EXPLAINED