PROVABLY FAIR TECHNOLOGY

A BITCOIN FEATURE that Makes Online Gambling TRANSPARENT

Thanks to Provably Fair, a technology that uses cryptography values, you can now play online betting games and prove that the game is fair or not. In fact, the technology, which is at the foundation of Bitcoin, gives the transparency of a physical casino to an online one. The games are random, just like brick-and-mortar gambling

THE BITCOIN TECHNOLOGY ANSWER

It eliminates the need to trust the casino, a third party or anyone else for that matter. This is because; there is no way to manipulate a wager that uses ***hashing proof***.

The system uses a cryptographic algorithm using hash functions (SHA-256), which are almost impossible to decode and unbreakable for practical purposes.

Randomness of online games can be verified by players themselves in real time after each round played.

Using ***Provably Fair*** does not necessitate an online casino to accept bitcoins. It is only a technology that is borrowed from Bitcoin.

To understand how the concept of Provably Fair works, it is important to wrap your head around the term ***hashing***.

WHAT IS HASHING?

Hashing is a computer process that converts any form of data into a unique fixed string of characters, which are meaningless if read by humans.

The hashed same data, gets the same result. If the data is modified in any way or differs even slightly from the original one, the result changes too.

Gambling → apply hash → e440a8e6372f5bda794863672e4e59750d5c9dde44e192e6fb40b0b2279d6ce2
Gambling3 → apply hash → 6d4b60cbbf53c312fc7a66861f3c6599a45ed7474b307876942d8be00064fc65
Even if only one character is altered, the resulting string will be completely different.

You can hash different words, images, or any form of data.

SHA256 hash function is popular for online data security and encryption.

SHA256, invented by the NSA (US National Security Agency), is the most popular hashing technique; a secure and irreversible process.

APPLICATION IN PROVABLY FAIR ONLINE BETTING GAMES

This same hashing can be used to cut the deck and confirm that it has not been tampered with, just like in a real casino. It verifies and self-audits wagers to ascertain they are fair. Let us use a game of online cards as an example:

1. INITIAL-SHUFFLE

→ The online casino shuffles the deck as normal. Casinos that do not use Provably Fair will hand you the deck at this point.

2. SEEDS AND HASHES GENERATION

The house generates a **server-seed** (random data) which is combined to the **intial-shuffle*** and hashed.
*This combination is called **Secret.**

→ You get this hash before you start gambling.

→ You provide a random seed, automatically or manually generated in your browser (client side, not on the server) that the site cannot see or predict.

X

Y

Z

Your seed changes the **intial-shuffle** to something unknown for you or the site. This is the online equivalent of cutting the deck to the dealers shuffle.

3. DEAL

The hand is dealt.

The initial deck is laid out.

4. VERIFICATION

→ The server-seed is revealed so you can verify it with the hash and check the house did, in fact, use the shuffled cards that you cut.

→ You can also check that the cards were then changed in accordance with the seed you provided.

If these are both the case, then you confirm that the results were actually calculated fairly and that you have just played a provably fair hand!

HOW TO VERIFY MANUALLY

You can use the **"Verify"** button to prove that the spin matches the hash the site showed you before the game. Or you can check the game for fairness on another website, it is very easy to do. These are the steps:

1. Find a third party hash calculator like online-encoder.com, quickhash.com or convertstring.com.
2. Select SHA-256 as your hashing algorithm.
3. Copy the Result+Secret field from the game, paste it into the input box of the third party calculator, and press "Generate" or "Encrypt".
4. The resulting hash should exactly match the hash provided to the player before the game.

FACTS AND TIPS ABOUT PROVABLY FAIR TECHNOLOGY

As the client-seed is only known by you, it is impossible for the house to distort the outcome.

Hashes are irreversible, there is no way to work backward and unearth your client-seed.

With the server hash in hand, you can always independently verify that the initial-shuffle + server-seed have not been manipulated.

Because a hash is unique to every set of data; as long as the hash is the same, you can be sure nothing has changed.

While it enables you prove that the game was fair, the Probably Fair, however, does not protect you from a casino that may choose not to honor a payment after a fair win.

Conclusion: it's always important to bet with a **high quality and trustworthy** bitcoin casino where the games are beautiful and **provably fair**.