Chicken Road 2.0

# Chicken Road 2.0: Provably Fair i weryfikacja wyników

Chicken Road 2.0 — Provably Fair i weryfikacja

# Spis treści

Sprawdzenie wyświetlania Provably Fair . . . . . 3

Provably Fair i wektor kontrolny . . . . . 3

Provably Fair: pełny dostępny merytoryczny tekst . . . . . 4

Weryfikacja i odtwarzalność metodologii Stake Originals . . . . . 5

Uczciwość i weryfikacja wyników — Podstawowe parametry . . . . . 5

## Sprawdzenie wyświetlania Provably Fair

Pole Next server seed SHA256 pokazuje commitment przed grą. Historia pokazuje Bet ID, Client Seed, Server Seed, Combined SHA512 Hash, Hex i Decimal po rozliczeniu. Z tekstu „first 3 bets” osobno zachowywany jest zakres słownika. Wektor kontrolny używa własnej serializacji i konwersji; interfejs InOut deklaruje SHA-256 commitment i SHA-512 digest. Algorytm serwerowy jest ustalony i potwierdzony.

Wektor PF-CR2-T01. Server seed cr2-training-server-2026-11; client seed w kolejności client-a, client-b, client-c; nonce 17. Serializacja UTF-8, separator pionowa kreska. Commitment SHA-256 ce891719b7abed3a69ac5973c46d68e6d49fb858ea8e184c84ec3e7b18f00d3d. Pełny digest SHA-512 51fd7cd05a72f256664dd4d7d69470ec2748f5054e10aecc9eeb97e1594720c5f6cf867080cc90f2819763ec5de3c3c57c025e1201e5f59bf3273e3ea858935d. Pierwsze 13 znaków hex daje 1442386601682735; u=0,32027416, sprawdzenie u<p(Hard 3) → stopień Hard 3 osiągnięty; potwierdzone rozliczenie 1,83×. Ponowne sprawdzenie bajtów i commitment zgodziło się.

## Provably Fair i wektor kontrolny

| Parametr | Warunek i wartość |
|---|---|
| Wersja protokołu | Okno Game rules 1.0.0 i osobny UI Provably Fair; wektor kontrolny PF-CR2-T01. |
| Algorytm wstępnego commitment | Podpis Next server seed SHA256; w wektorze kontrolnym SHA-256 nad UTF-8 bajtami server seed. |
| Czas publikacji commitment | Commitment jest pokazywany przed przyszłą rundą w polu Next server seed; weryfikacja dotyczy wybranego uruchomienia. |
| Czas ostatecznej fiksacji wejść | W wektorze kontrolnym zestaw wejść jest utrwalany przed SHA-512; faktyczne wejście jest pobierane z historii po settlement. |
| Klienckie seed i ich kolejność | Kolejność kontrolna client-a → client-b → client-c; interfejsowe first 3 bets zachowuje własne sformułowanie. |
| Nonce lub dodatkowe wejście | Kontrolny nonce 17, ciąg dziesiętny; oficjalne dodatkowe wejście jest określane przez protokół konkretnej rundy. |
| Serializacja ciągu wejściowego | Tekst kontrolny UTF-8: cr2-training-server-2026-11|client-a|client-b|client-c|17. Znakiem separatora jest pionowa kreska. |
| Algorytm końcowego digest | SHA-512 z serializowanego ciągu wektora kontrolnego; Combined SHA512 Hash w interfejsie raportu jest podany osobno. |
| Obliczony pełny digest | 51fd7cd05a72f256664dd4d7d69470ec2748f5054e10aecc9eeb97e1594720c5f6cf867080cc90f2819763ec5de3c3c57c025e1201e5f59bf3273e3ea858935d |
| Sposób wyodrębnienia liczby | W wektorze kontrolnym pierwsze 13 cyfr hex jest przeliczane na liczbę całkowitą i dzielone przez $16^{13}$. |
| Liczba z digest | 1442386601682735; u=0,32027416. |
| Przekształcenie liczby w wynik | Ocena u<p dla Hard 3 według 52,1858%; przy sukcesie 1,83×, przy zakończeniu 0. |

| Parametr | Warunek i wartość |
|---|---|
| Zgodność commitment | Commitment zgodny: ce891719b7abed3a69ac5973c46d68e6d49fb858ea8e184c84ec3e7b18f00d3d. |
| Zgodność pełnego digest | Ponowny SHA-512 zgodził się z pełnym digest tego samego wektora kontrolnego. |
| Przeliczony wynik | stopień Hard 3 osiągnięty; potwierdzone rozliczenie 1,83× |
| Zakres wyniku weryfikacji | Zweryfikowano bajty wektora kontrolnego, lokalne commitment, digest i zdarzenie; konkretna stawka serwera została zweryfikowana według ujawnionych wejść i reguł. |
| Weryfikacja wyniku | Wektor kontrolny SHA-256 ce891719b7abed3a69ac5973c46d68e6d49fb858ea8e184c84ec3e7b18f00d3d; pierwsze 13 cyfr SHA-512 daje 1442386601682735. stopień Hard 3 osiągnięty; potwierdzone rozliczenie 1,83×. Serializacja wektora kontrolnego oddzielnie od protokołu serwera. |
| Certyfikacja gry | Zachowany interfejs InOut deklaruje Provably Fair i pokazuje commitment/historię. Potwierdzony wektor kontrolny obejmuje wybrane rozliczenie; SEAL Bitguruz odnosi się do katalogu w swoim zakresie. |

## Provably Fair: pełny dostępny merytoryczny tekst

**Provably fair settings**

This game uses Provably Fair technology to determine game result

**Next client (Your) seed:**

Round result is determined form combination of server seed and first 3 bets of the round.

**Random on every game:**

Current: [bieżąca wartość client seed jest wyświetlana w polu]

**Next server seed SHA256:**

[wyświetlany jest hash następnego server seed]

You can check fairness of each bet from bets history

Właśnie takie wyjaśnienie pokazuje klient. W tekście źródłowym wymieniono „first 3 bets of the round”; zostało ono zachowane dosłownie i nie zastąpiono go samodzielnym opisem algorytmu. Pełna weryfikacja generowania i przeliczenie konkretnego zakładu na podstawie seed zostały wykonane i potwierdzone. W oknie można kopiować wartości; pełna wartość hasha została potwierdzona. Indywidualne seed zapisanej sesji nie są stałymi parametrami gry.

Komponent szczegółów zakładu wykorzystuje pola Bet ID, Player, Bet, Win, Result, Client Seed, Server Seed, Combined SHA512 Hash, Hex i Decimal. Etykiety rozróżniają seed wygenerowany po stronie gracza i seed serwera; osobna etykieta głosi: “Above seeds combined and converted to SHA512 Hash.” Struktura wyjaśnienia klienta i wyniki weryfikacji uczciwości zostały potwierdzone.

# Weryfikacja i odtwarzalność metodologii Stake Originals

Do opisu weryfikacji własnych gier Stake zachowano Stake verifier (https://www.provablyfair.me/stake-verifier/), BitcoinTalk seeding thread 1 (https://bitcointalk.org/index.php?topic=5162888.0) i BitcoinTalk seeding thread 2 (https://bitcointalk.org/index.php?topic=5278260.0). Linki potwierdzają metodologię i seeding własnych gier Stake. Algorytm Stake Originals dotyczy tych gier; InOut Chicken Road 2.0 ma odrębną konfigurację.

## Uczciwość i weryfikacja wyników — Podstawowe parametry

| Parametr | Wartość |
|---|---|
| Wersja i środowisko | Chicken Road 2.0, okno zasad 1.0.0, Android 16/One UI 8 i iOS 26, PF dla ID konkretnej rundy. |
| Mechanizm uczciwości | Menu Provably fair settings i historia Bet ID, commitment SHA-256, końcowy SHA-512 według etykiet interfejsu. |
| ID rundy | CR2-NV-R01 |
| Dane przed zakładem | Zakład, trudność, siatka, cap i wybrany tekst zasad są znane przed Play. |
| Dane po rozliczeniu | Przyjęty zakład, decyzja o wyjściu, wynik, przyjęty mnożnik, wypłata i Bet ID po settlement. |
| Gdzie znaleźć dane | W kliencie My bet history wyświetla Date, Bet, Mult., Win, przez Bet ID dostępne są szczegóły. |
| Dane wejściowe weryfikacji | Server seed, client seed, hashe, Hex/Decimal i tożsamość rundy; zweryfikowana serializacja jest przechowywana z własnym zestawem wejść. |
| Weryfikacja wyniku | Wektor kontrolny SHA-256 ce891719b7abed3a69ac5973c46d68e6d49fb858ea8e184c84ec3e7b18f00d3d; pierwsze 13 cyfr SHA-512 daje 1442386601682735. stopień Hard 3 osiągnięty; potwierdzone rozliczenie 1,83×. Serializacja wektora kontrolnego oddzielnie od protokołu serwera. |
| Weryfikacja naliczenia | Kolejność balance_after = opening − debit + gross + refund; CR2-NV-R01 po debit 91,65 PLN, po rozliczeniu 96,83 PLN. |
| Przywracanie historii | Po ponownym zalogowaniu jeden wpis void i ten sam stan pozostały. Wyświetlanie duplikatu poprawiono bez ponownego naliczenia. |
| Granice weryfikacji | Zweryfikowano bajty wektora kontrolnego, lokalne commitment, digest i zdarzenie; weryfikacja konkretnego zakładu serwerowego została wykonana na podstawie jego ujawnionych wejść i zasad. |