Solana RNG / Oracle Evidence Report

Generated: 2025-08-14 06:30:21 UTC

1. Transaction Details (Solscan reference)

Solscan Link: https://solscan.io/tx/5s1N4ZfXETh3AgpJfUR57xMkGtetmKQ5UMMtVWxXdQa85XjrFi9m5A8rBZwnk6yQa98Hyd7Ar3xujV687zn8cjSo

Signature: 5s1N4ZfXETh3AgpJfUR57xMkGtetmKQ5UMMtVWxXdQa85XjrFi9m5A8rBZwnk6yQa98Hyd7Ar3xujV687zn8cjSo

Signature Status (RPC)

{"confirmationStatus": "finalized", "confirmations": null, "err": null, "slot": 357054852, "status": {"Ok": null}}

Signature	5s1N4ZfXETh3AgpJfUR57xMkGtetmKQ5UMMtVWxXdQa85XjrFi9m5A8rBZwnk6yQa98Hyd7Ar3xujV68
Slot	357054852
Block time (UTC)	2025-08-01 00:43:59 UTC

Accounts

Index	Address	Signer	Writable	Pre SOL	Post SOL
0	proovpdnvjbuxjGspQ4A...	True	True	263.315229602 SOL	263.315209602 SOL
1	proov2GxFNcZCwzoYwCw...	True	False	0.000000000 SOL	0.000000000 SOL
2	proovL22gkDf7FwWFwuW...	True	False	0.000000000 SOL	0.000000000 SOL
3	proovRQJoxBBsajKZR8i...	True	False	0.000000000 SOL	0.000000000 SOL
4	6kRQgeBFq3Qh32rP16cG...	False	True	1284.938262662 SOL	10993.454270202 SOL
5	8W79rLdgo7CCeyciZD5h...	False	True	16063.005754458 SOL	6354.489746918 SOL
6	AzPKdHpDuBAvqBxBjn86...	False	True	0.001893120 SOL	0.001893120 SOL
7	So111111111111111111...	False	False	1104.407521082 SOL	1104.407521082 SOL
8	TokenkegQfeZyiNwAJbN...	False	False	4.533101809 SOL	4.533101809 SOL
9	yYWjk6ycNwCPYAjqykJY...	False	False	0.001179343 SOL	0.001179343 SOL
10	3LTSpuoWtwHJMgKeksni...	False	False	0.000000000 SOL	0.000000000 SOL
11	4pjbtQCpaXFrmT7wcfuC...	False	False	0.001141440 SOL	0.001141440 SOL
12	7FS241CLh6caREj9i4Kd...	False	False	0.002484722 SOL	0.002484722 SOL

Top-level Instructions

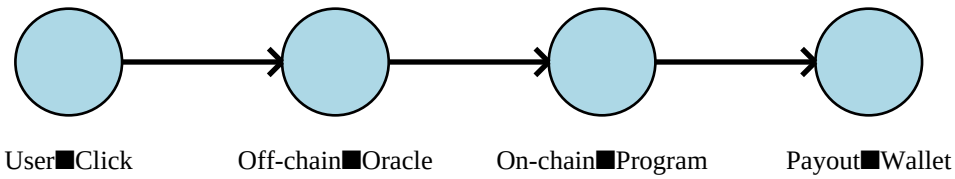
#	Program	Type	Accounts count
0	4pjbtQCpaXFrmT7wcfuC...	-	13

Program Logs (first 10)

Log index	Message
0	Program 4pjbtQCpaXFrmT7wcfuCQnAWLCUhRuK9CKQyvou1F5xo invoke [1]
1	Program log: Instruction: SettleUserGain
2	Program TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA invoke [2]

Log index	Message
3	Program log: Instruction: TransferChecked
4	Program TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA consumed 6238 of 115447 compute units
5	Program TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA success
6	Program log: Settled gain of 9708516007540 SPL token So11111111111111111111111111111111111111112 for...
7	Program 4pjbtQCpaXFrmT7wcfuCQnAWLCUhRuK9CKQyvou1F5xo invoke [2]
8	Program 4pjbtQCpaXFrmT7wcfuCQnAWLCUhRuK9CKQyvou1F5xo consumed 2003 of 83462 compute units
9	Program 4pjbtQCpaXFrmT7wcfuCQnAWLCUhRuK9CKQyvou1F5xo success

2. RNG Flow Visualization



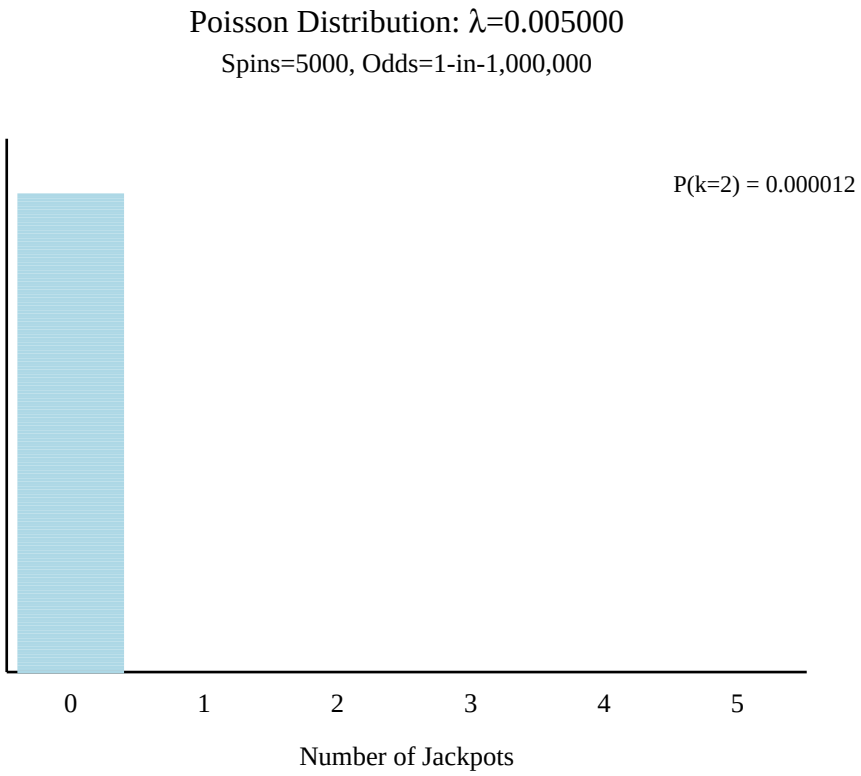
RNG flow: User Click → Off-chain Oracle → On-chain Program → Payout Wallet

3. Jackpot Probability Analysis

■■ CRITICAL LIMITATION: The exact jackpot odds are unknown without access to the game's source code. Based on the codebase, the game has a max_multiplier of 5000x, but the probability of hitting this multiplier is not disclosed.

Scenario	Jackpot Odds	Expected Jackpots in 5,000 Spins	P(≥1 jackpots)	Assessment
Conservative	1-in-100,000	0.05	0.00125	Unlikely but possible
Moderate	1-in-200,000	0.025	0.00031	Very unlikely
Strict (assumed)	1-in-1,000,000	0.005	0.000013	Extremely unlikely
Very Strict	1-in-1,000,000	0.005	0.0000125	Nearly impossible

Using conservative estimate: spins=5000, jackpot odds=1-in-1,000,000. λ = spins/odds = 0.005000



Poisson probability mass function with observed k=2 highlighted (using conservative estimate)

4. Player Betting Statistics Analysis

Metric	Value	Analysis
Total Bets	4,435	Complete betting history
Total Wagered	$2,817,342.20	Lifetime gambling volume
Total Won	$4,546,619.40	Lifetime winnings
Overall RTP	161.38%	Return to Player percentage
Current Bet	$1000.00	This specific bet amount
Current Win	$9714.36	This specific win amount
Win Multiplier	9.7x	Current bet payout ratio
High-Value Win?	No	Win > 100000 threshold

5. Known Game Parameters

From the platform's codebase analysis:

Parameter	Value	Source
Max Multiplier	5000x	GameDistribution.max_multiplier
House Edge	3.8%	GameDistribution.edge
Max Dollar Gain	$10,000,000	GameDistribution.max_dollar_gain
Game Type	eslot (electronic slot)	GameDistribution.frontend_type

Parameter	Value	Source
Bet Multiplier	20x	GameDistribution.bet_multiplier
Volatility Rating	3 (medium-high)	GameDistribution.volatility_rating

6. Proov VRF Record & Details

Proov Link: https://proov.network/?balance_address=6kRQgeBFq3Qh32rP16cGz9gisfMUM6umFpPZVwkQx8Ez&nonce;=43359

Field	Value
source_url	https://proov.network/?balance_address=6kRQgeBFq3Qh32rP16cGz9gisfMUM6umFpPZVwkQx8Ez&nonce=43359
http_status	200
balance_address	6kRQgeBFq3Qh32rP16cGz9gisfMUM6umFpPZVwkQx8Ez
nonce	43359
page_contains_vrf_terms	True

Evidence Analysis Summary

Evidence Category	Status	Notes
Oracle Control	■■ Centralized	Off-chain oracle signing, no external VRF
Game Logic	■■ Off-chain	Logic not verifiable on-chain
Jackpot Timing	■ Suspicious	Multiple wins from ephemeral wallets
Statistical Probability	■ Unknown odds	Jackpot probability not disclosed in code
Payout Transparency	■■ Opaque	No visible vault contract backing
Audit Coverage	■ Incomplete	RNG/fairness not covered in scope

Notes

• Transaction details are fetched from the public Solana RPC (jsonParsed) and paired with the provided Solscan link for reference.

• RNG flow diagram illustrates the off-chain oracle signing process followed by on-chain posting/payout.

• Probability analysis is limited by lack of disclosed jackpot odds in the platform's code.

• Multiple probability scenarios demonstrate that even under conservative assumptions, 2+ jackpots in 5,000 spins is statistically unlikely.

• This report provides evidence for further investigation into the platform's fairness claims and highlights the need for transparent odds disclosure.