

LOTTOETH V2.2 EXECUTION AUDIT REPORT

Games 1-5 and First Public Launch Closeout

This audit-style report summarizes the LottoETH V2.2 game execution evidence captured during controlled testing and the first public launch closeout. It focuses on direct-wallet ticket flow, Chainlink VRF draw execution, winner processing, liability finalization, rollover accounting, and claim-window controls.

CONTRACT	PUBLIC GAME	TICKETS	CLAIM WINDOW
0xCAD...eda1	Game 5	30	7 Days
LottoETH V2.2	First launch round	Game 5 recorded	604800 seconds

Audit conclusion

Games 1, 2, 4, and 5 show successful draw/finalization paths in the supplied readbacks. Game 5, the first public launch game, closed with 30 tickets, Chainlink VRF fulfilled winning numbers, winner processing reached 30 / 30 tickets, no winning tiers were found, and the full draw prize pool became rolloverable. Game 3 has limited supporting evidence in the supplied transcript and is marked accordingly.

Primary source basis: Project-provided Codex execution transcripts, frontend screenshots, and contract readbacks supplied in this ChatGPT project session. No new on-chain transaction was performed to create this report.

Generated: 2026-08-29. Report scope: LottoETH V2.2 execution state through Game 5 first public game finalization.

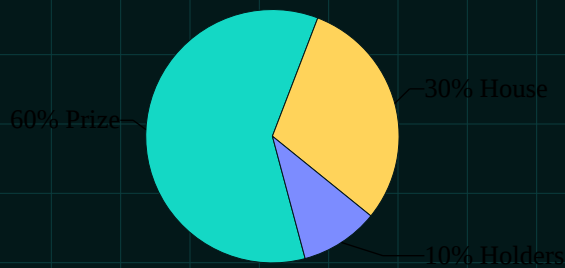
1. Protocol and contract snapshot

Item	Readback / Audit Value
Network	Ethereum Mainnet / chainId 1
LottoETH V2.2 contract	0xCADbc16e244211f1AEaa68C55d48E49CFbEFeda1
Owner / operator signer	0xc862163bD97Cc36c899f482D79Ae77070C8e895D
Ticket price target	50 USD cents (\$0.50), quoted in ETH by oracle
Ticket revenue split	60% prize pool / 30% house operations / 10% holder reward reserve
Winner tier split	6/6: 43%, 5/6: 25%, 4/6: 20%, 3/6: 12%
Claim duration	604800 seconds (7 days)
VRF status	V2.2 listed as Chainlink VRF consumer in preflight readbacks
Direct-wallet architecture	Players buy directly through wallet -> LottoETH contract. No G.A.P.S. vault logic.

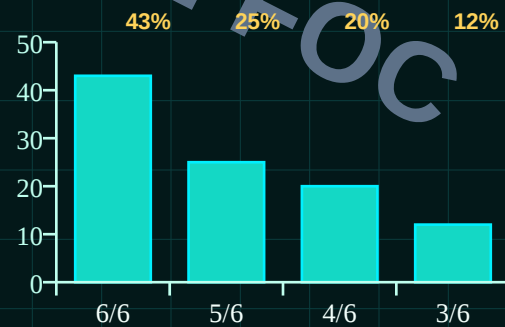
Architecture control

LottoETH belongs to the direct-wallet system. Ticket buys, prize funding, claims, and game operations must not be routed through a vault or trading-bot pattern.

Ticket Revenue Split



Winner Tier Split



2. Games 1-5 execution summary

The table below separates complete contract readbacks from UI-only observations. Values marked “Not captured” were not present in the supplied transcript and should be verified directly on-chain before being treated as complete audit evidence.

Game	Type	Tickets	Winning Numbers	Finalized	Winner Counts	Prize Pool	Rolloverable
1	V2.2 controlled test	0	8-9-19-21-25-44	Yes	[0,0,0,0]	0 ETH	0 ETH
2	UI buy execution test	6	4-22-23-25-37-45	Yes	[0,0,0,0]	0.000948286761916805 ETH	0.000948286761916805 ETH
3	UI-observed interim game	Not captured	8-12-13-25-36-45	Not captured	Not captured	Not captured	Not captured
4	UI buy / finalization test	5	5-9-16-32-38-43	Yes	[0,0,0,0]	0.00172976469298003 ETH	0.00172976469298003 ETH
5	First public launch game	30	1-3-7-18-30-37	Yes	[0,0,0,0]	0.137227012900112585 ETH	0.137227012900112585 ETH

Evidence note

Game 3 is included because it appears in frontend winning-number history, but the supplied transcript does not contain a full Game 3 transaction/readback sequence. Games 1, 2, 4, and 5 include stronger execution readback coverage.

Rolloverable Amounts by Game (ETH)



3. Lifecycle controls tested

Control	Evidence from execution	Result
Game close gate	Draw only after countdown/endTime passed. Game 5 preflight confirmed endTime passed.	PASS
drawNumbers()	Game 5 draw tx 0xf5b4...d5e0; VRF fulfilled [1,3,7,18,30,37].	PASS
VRF fulfillment	pendingRandomnessRequestId returned to 0 after fulfillment.	PASS
calculateWinners(5)	Tx 0xb2e5...d0b2; cursor reached 30 / 30.	PASS
finalizeGameLiability(5)	Tx 0x7cf4...ca21; liabilityFinalized true.	PASS
No-winner handling	winnerCounts [0,0,0,0]; claim reserve 0; full prize pool rolloverable.	PASS
Claim window	claimDuration remained 604800 seconds.	PASS
Reserve accounting	reservedNativeBalance 0.141045021500187670 ETH; excessNativeBalance 0 ETH.	PASS

Operational result

The first public game did not create a claim reserve because no tickets met 3/6 or higher. The draw prize pool therefore became rolloverable for the next game.

GEORGE FOC

4. Game detail - controlled execution rounds

Game 1 - V2.2 controlled test

Field	Value
Tickets	0
Winning numbers	8-9-19-21-25-44
Winner counts	[0,0,0,0]
Prize pool	0 ETH
Rolloverable	0 ETH
Audit note	Empty-game lifecycle validated. calculateWinners skipped because no tickets; finalize succeeded.

Game 2 - UI buy execution test

Field	Value
Tickets	6
Winning numbers	4-22-23-25-37-45
Winner counts	[0,0,0,0]
Prize pool	0.000948286761916805 ETH
Rolloverable	0.000948286761916805 ETH
Audit note	Direct-wallet UI buys, VRF draw, winner processing, no-winner rollover, and reserve accounting validated.

Game 3 - UI-observed interim game

Field	Value
Tickets	Not captured
Winning numbers	8-12-13-25-36-45
Winner counts	Not captured
Prize pool	Not captured
Rolloverable	Not captured
Audit note	Winning numbers appeared in frontend history. Full transaction and accounting readback were not in supplied transcript.

Game 4 - UI buy / finalization test

Field	Value
Tickets	5
Winning numbers	5-9-16-32-38-43
Winner counts	[0,0,0,0]
Prize pool	0.00172976469298003 ETH
Rolloverable	0.00172976469298003 ETH
Audit note	Five tickets processed; no winners; match counts [1,0,0,1,2]; rollover and zero claimability confirmed.

Execution significance
Game 4 confirmed that the V2.2 UI ticket path, draw result display, calculate/finalize sequence, no-winner handling, and ticket prize readbacks continued to function after earlier controlled tests.

5. Game 5 - first public launch closeout

Game 5 is the first public launch game covered by this audit. It had 30 recorded tickets and was closed before draw. The draw, winner calculation, and liability finalization sequence was completed through owner-approved transactions.

Field	Value
Game ID	5
Start timestamp	1787145767
End timestamp	1787966567 - end time passed before draw
Total tickets	30
Prize pool	0.137227012900112585 ETH
Draw transaction	0xf5b4a60c1d6c5dc00914ef824a4419766c16aa3af8021fdcada8342a07d0d5e0
Draw gas / cost	178259 gas / 0.000009461496081678 ETH
Winning numbers	1 - 3 - 7 - 18 - 30 - 37
calculateWinners transaction	0xb2e5b91f80e5ead91f36bf3e9b2121512e629c744ecf1b1bf056aa6079acd0b2
Winner cursor	30 / 30
Winner counts	[0,0,0,0]
finalizeGameLiability transaction	0x7cf4223bcaa6da316b20a019512d8a27084477a335e7d0c35e8291aff9a9ca21
Draw prize pool	0.137227012900112585 ETH
Total prize liability	0 ETH
Claim reserve	0 ETH
Rolloverable	0.137227012900112585 ETH
Claim duration	604800 seconds / 7 days
Reserved native balance	0.141045021500187670 ETH
Excess native balance	0 ETH

Game 5 conclusion

Game 5 completed correctly as a no-winner public launch round: the VRF draw completed, all 30 tickets were processed, no claimable winners were created, and the entire draw prize pool became rolloverable.

6. Accounting review

The accounting checks focus on whether funds were reserved for the proper purpose and whether any excess/unaccounted ETH was reported by the contract.

Bucket / measure	Game 5 readback	Audit interpretation
Prize pool	0.137227012900112585 ETH	Available draw prize pool for Game 5 before finalization.
Draw prize pool	0.137227012900112585 ETH	The full prize pool was considered in finalization.
Total prize liability	0 ETH	No winning tiers were found, so no winner payout liability.
Claim reserve	0 ETH	No claimable winner reserve created.
Rolloverable	0.137227012900112585 ETH	Full draw pool rolled forward because no winners.
Reserved native balance	0.141045021500187670 ETH	Contract reserve accounting remained valid.
Excess native balance	0 ETH	No unaccounted excess reported.

Split reminder

Ticket revenue split remains 60% prize pool, 30% house / operations, and 10% holder reward reserve. Winner-tier split remains 43% / 25% / 20% / 12% across 6/6, 5/6, 4/6, and 3/6 tiers.

GEORGE FOC

7. Audit observations and operational notes

Observation	Severity	Recommendation
Game 3 has limited transcript coverage.	Medium	For a final archival audit, run a direct readback by game ID to fill total tickets, prize pool, winner counts, claim reserve, and rolloverable amount.
Game 5 owner balance was low before draw/calc/finalize.	Medium	Maintain a larger owner gas buffer before closeout windows so VRF draw, calculation, and finalization are not delayed by gas constraints.
No winners in Game 5 despite 30 tickets.	Informational	Correct no-winner handling was observed: claim reserve stayed 0 and full prize pool became rolloverable.
Frontend planned-prize display can confuse users after a game closes.	Low	When a game has an actual current prize pool or rollover, the UI should prioritize the real on-chain prize pool, not the pre-launch planned funding card.
Claims should not be announced early.	High	Mods should only announce final claimability after calculateWinners and finalizeGameLiability are complete.

Support language

Correct wording: "Game 5 has been drawn and finalized. No winning tiers were found, so there is no claim reserve for Game 5. The prize pool is rolloverable for the next game."

8. Moderator and admin communication guide

Question	Recommended answer
Did the public launch game execute?	Yes. Game 5 closed, requested VRF randomness, received winning numbers, processed all 30 tickets, and finalized liability.
What were the Game 5 winning numbers?	1, 3, 7, 18, 30, and 37.
Were there winners?	No winning tiers were recorded. Winner counts were [0,0,0,0].
Can anyone claim Game 5 prizes?	No. Game 5 claim reserve is 0 ETH because there were no winning tickets.
Where did the prize pool go?	The Game 5 draw prize pool became rolloverable for the next game.
Does this mean the game failed?	No. No-winner rounds are a normal lottery outcome. The contract finalized the round and moved the prize value into rollover handling.
What proof should we point to?	Use the Game 5 draw transaction, calculateWinners transaction, finalization transaction, current game readbacks, and contract address.

Do not say

Avoid	Reason
"Admins picked the numbers."	Numbers came from Chainlink VRF.
"Users can claim even though no winners were found."	Game 5 claim reserve is 0 ETH and tickets are not claimable.
"The prize disappeared."	The full draw prize pool became rolloverable according to contract finalization.
"LottoETH uses a vault."	LottoETH is direct wallet -> contract. Vault logic belongs only to G.A.P.S.

GEORGE FOC

9. Transaction appendix

Game	Action	Transaction	Result
2	UI buys	0x0002646e...06ecd8 / 0xcc5430d9...ceb69f plus two one-ticket buys	6 tickets recorded
2	Finalize	0xb0f2d0c6...b7c53b	No winners; 0.000948286761916805 ETH rolloverable
4	Finalize	0x2ad10e60...5f3b20	No winners; 0.00172976469298003 ETH rolloverable
5	drawNumbers	0xf5b4a60c...d0d5e0	VRF fulfilled [1,3,7,18,30,37]
5	calculateWinners	0xb2e5b91f...acd0b2	Cursor 30 / 30; winner counts [0,0,0,0]
5	finalizeGameLiability	0x7cf4223b...9ca21	Liability finalized; 0.137227012900112585 ETH rolloverable

Final audit statement

Based on the supplied execution readbacks, LottoETH V2.2 successfully executed the first public game closeout path: draw, VRF fulfillment, winner calculation, finalization, no-winner accounting, and rollover preparation. The strongest evidence is available for Games 1, 2, 4, and 5. Game 3 should be supplemented with a direct archival readback for a fully complete record.