GEORGE ECOSYSTEM

# LottoETH V2.1 Validation Audit Report

ETHMode direct-wallet lottery, Chainlink VRF draw lifecycle, ticket getter visibility, frontend state validation, and mainnet transaction review

| | |
|---|---|
| Report Type | Internal validation audit and manual/on-chain regression report |
| System | LottoETH_GEORGE_V2_1 - direct-wallet ETH purchase, Chainlink VRF native payment, ticket getters, winner calculation, and liability finalization |
| Validation Status | ETHEREUM MAINNET LIFECYCLE VALIDATED - GAME 1 THROUGH GAME 3 DRAWN, PROCESSED, AND FINALIZED |
| Contract Status | V2.1 deployed and verified; frontend rewired from old V2 to V2.1 ABI/address; no G.A.P.S. vault logic used |
| Generated | 2026-08-18 |

## Core Principle

LottoETH is a direct-wallet system. Users connect wallets directly, pick numbers, buy tickets with ETH, and verify every draw, ticket, and payout state on-chain. No vault, bot, presale, staking, or G.A.P.S. execution pattern is used for LottoETH.

# 1. Executive Summary

- LottoETH V2.1 moved the public frontend from the prior ETHMode V2 contract to the newly deployed V2.1 contract at 0x8531097AdEDE6d76F22e3C183b2120f9007c023f.

- The V2.1 upgrade addressed the public fixed-array getter limitation by adding direct ticket-number getters, including getTicketNumbers, getPlayerTicketsWithNumbers, and getPlayerTicketsInGameRange.

- The live frontend was updated to use V2.1 ABI paths first and event-log recovery only as a fallback. My Tickets now displays selected numbers directly from V2.1 getter output.

- Ethereum Mainnet lifecycle testing validated Game 1, Game 2, and Game 3 through start, ticket purchase, VRF draw, winner processing, and liability finalization.

- No winners were found in Games 1-3. Prize liability remained zero and the tested game pools became rolloverable after finalization.

## Validation Verdict

LottoETH V2.1 is mainnet lifecycle validated for direct-wallet ETH ticket purchase, Chainlink VRF draw fulfillment, direct ticket-number display, winner processing, and liability finalization. This report remains an internal validation audit and does not replace an independent smart contract security audit before major public prize exposure.

# 2. Architecture and System Boundary

LottoETH V2.1 is part of the George Ecosystem direct-wallet product group. It must remain separate from the G.A.P.S. vault-based trading architecture.

| Layer | Role | V2.1 Validation Status |
|---|---|---|
| User Wallet | Direct ETH payer and transaction signer | Validated through mainnet ticket purchases. Wallet interacts directly with LottoETH V2.1. |
| LottoETH Contract | Ticket pricing, purchase, draw state, winner processing, claim liability, reserve accounting | Validated through Games 1-3 lifecycle. |
| Chainlink VRF | Randomness source for winning numbers | Validated by fulfilled draws for Games 1-3. |
| Frontend | Static LottoETH game UI and wallet UX | Validated against V2.1 address/ABI and getter-first ticket display. |

### System Integrity Rule

Presale, staking, Win4ETH, LottoETH, token transfers, and payments are direct-wallet systems. G.A.P.S. vault logic must not be routed into LottoETH. User wallet to LottoETH contract is the correct flow.

# 3. Ethereum Mainnet Environment and Deployed Contracts

| Item | Value |
|---|---|
| Network | Ethereum Mainnet |
| Chain ID | 1 / 0x1 |
| Explorer | https://etherscan.io |
| Frontend | Static LottoETH_GAME frontend, vanilla JavaScript, shared George/Reown wallet bundle preserved |
| Validation Mode | Manual mainnet test execution, readback, browser verification, and Codex-assisted ABI checks |

## Validated Mainnet Contract Addresses

| Contract / Role | Address |
|---|---|
| LottoETH_GEORGE_V2_1 | 0x8531097AdEDE6d76F22e3C183b2120f9007c023f |
| Owner / Admin | 0xc862163bD97Cc36c899f482D79Ae77070C8e895D |
| House Wallet | 0x534E50CDc64077fD782c177a3566EeBCf76474F1 |
| PayToken_GEORGE | 0xF5E7E75287122Cd7beF38a97D02Ef6f35645F1b3 |
| DividendTracker_GEORGE | 0x8D87D26a270Fed8c7D92ac58C316c58093eEBAe9 |
| Chainlink VRF Coordinator | 0xD7f86b4b8Cae7D942340FF628F82735b7a20893a |

# 4. V2.1 Release Scope and Contract Boundary

V2.1 is a contract and frontend validation release. It replaces the old ETHMode V2 frontend target with a V2.1 contract that exposes direct ticket and claim getters required for reliable public UX.

| Scope | V2.1 Status |
|---|---|
| Contract | New LottoETH_GEORGE_V2_1 deployed and verified on Ethereum Mainnet. |
| Frontend Address | Updated to 0x8531097AdEDE6d76F22e3C183b2120f9007c023f. |
| Old V2 Address | Removed from active frontend files: 0xe81B1A21dc00A95Ff8E46F334d32f9Cf1BBAb656. |
| Game Duration | Set to 300 seconds for private mainnet testing. |
| Claim Duration | 604800 seconds, or 7 days. |
| Ticket Price | USD target: $0.50 via quoteTicketPriceNative(quantity). |

### Boundary Statement

This V2.1 report concerns LottoETH only. It does not validate G.A.P.S., presale, staking, Win4ETH, or PayToken transfer mechanics beyond the LottoETH interfaces used by the deployed contract.

# 5. Frontend Rewire and ABI Getter Review

The frontend was rewired from event-log-first ticket recovery to V2.1 getter-first ticket recovery. This directly addresses the old public struct getter limitation where selected number arrays were unavailable from tickets(uint256).

| Area | V2.1 Getter Path |
|---|---|
| Current Game Summary | getCurrentGameSummary() primary; getGameSummary(uint32) for specific games. |
| Current Game Tickets | getPlayerTicketsWithNumbers(address,uint32) primary. |
| Previous Game Tickets | getPlayerTicketsInGameRange(address,uint32,uint32) primary. |
| Ticket Detail | getTicket(uint256) plus getTicketNumbers(uint256). |
| Claim UX | getPlayerClaimableTickets, getPlayerClaimSummary, isTicketClaimable, getTicketPrize. |
| Fallback | TicketPurchasedNative event recovery remains fallback only. |

## Validation Result

Live My Tickets panels displayed selected numbers for Game 1, Game 2, and Game 3 tickets after purchases and after draw/finalization states. This confirms the V2.1 getter-first path is operating in the public frontend.

# 6. Chainlink VRF Native Subscription Readiness

| Item | Validated State |
| --- | --- |
| VRF Subscription | Existing native-funded subscription reused for V2.1. |
| Subscription ID | 35482562509661619778901414857916150446182419051860409155909760032861535707620 |
| V2.1 Consumer | 0x8531097AdEDE6d76F22e3C183b2120f9007c023f listed as consumer. |
| Native Balance | 0.119567454012862845 ETH at preflight readback. |
| Pending Request Gate | pendingRequestExists and pendingRandomnessRequestId checked before draw/start actions. |
| VRF Draw Function | Deployed V2.1 ABI exposes drawNumbers(), not requestDraw(). |

## Positive Validation

A safety check prevented use of a nonexistent requestDraw() function. The correct deployed function drawNumbers() was identified from the V2.1 ABI before any draw transaction was broadcast.

# 7. Direct-Wallet Purchase UX and Ticket Display

LottoETH V2.1 uses direct ETH purchases. During validation, the frontend accepted wallet connection, number selection, ticket purchase, total ticket update, and ticket display without G.A.P.S. vault routing.

| Purchase Component | Validation Result |
|---|---|
| Wallet Connection | Direct wallet connection shown on Ethereum Mainnet. |
| Ticket Numbers | User-selected six-number tickets displayed in My Tickets. |
| Quantity Field | Quantity UI present; multi-ticket transaction testing remains a recommended public-flow test. |
| Quote | quoteTicketPriceNative(quantity) displayed current ETH quote for USD target $0.50. |
| Closed State | Purchase button disabled after game endTime and during finalized claim-open state. |

## Gas Observation

A high-fee one-ticket buy showed the wallet using a 2 gwei priority fee while base fee was approximately 0.040 gwei. A later buy with manually reduced priority fee completed with an approximately $0.02 fee. The material difference was wallet gas setting, not a high Ethereum base fee.

# 8. Game 1 Mainnet Lifecycle Evidence

| Step | Evidence / Result |
|---|---|
| Start | Game 1 started with 300-second duration after unpause. |
| Purchases | 3 tickets purchased and displayed in My Tickets. |
| drawNumbers | 0x5d82bf54316f7e1d85fe85a47557a27a53ecc0191b6a6ecf8dde54a7f572c467 |
| Winning Numbers | [2, 8, 14, 18, 28, 34] |
| calculateWinners(1) | 0x638c1288ba7b229ec65af4816aaaefb3949ed27abd9863c5913d890214673560 |
| finalizeGameLiability(1) | 0xe04e640d97d4dd48dacfe611b8c586bf2b81df9f4ea0bac09252c366ed11a4eb |
| Final State | winnerCounts [0,0,0,0]; liabilityFinalized true; rolloverableNative 0.000476413003915266 ETH. |

Game 1 confirmed the complete draw/processing/finalization flow with no winners and rolloverable prize pool accounting.

# 9. Game 2 Mainnet Lifecycle Evidence

| Step | Evidence / Result |
|---|---|
| Start | Game 2 started after Game 1 finalization. |
| Purchases | 1 ticket purchased and displayed in My Tickets. |
| drawNumbers | 0xe86d2407188b9c9cec838a89b085ea0e66153433ea815e7ad255f866a8d2161d |
| Winning Numbers | [3, 6, 7, 24, 37, 48] |
| calculateWinners(2) | 0xefbeccce64944bf631fc8229da61e6665542dda7e3437ffe03fefabf1650f3ef |
| finalizeGameLiability(2) | 0x7c53286bddb8d2b1300e850a68edd3dd371f6d5a70984cacadb81d1407d7d958 |
| Final State | winnerCounts [0,0,0,0]; liabilityFinalized true; rolloverableNative 0.000634900162703123 ETH. |

Game 2 confirmed repeatability of VRF draw, winner processing, and finalization after a prior rollover state.

# 10. Game 3 Mainnet Lifecycle Evidence

| Step | Evidence / Result |
|---|---|
| Start | Game 3 active with 300-second countdown display and purchases enabled during entry window. |
| Purchases | 8 tickets purchased and displayed in My Tickets. |
| drawNumbers | 0xebf7d7e07c954b95700bd995161da167a987f81f4b2bfb0303a05582b767f12e |
| Winning Numbers | [20, 29, 31, 46, 47, 48] |
| calculateWinners(3) | 0x6ed5cde625d8a18e449e390acb08f5cafea16d0bd69041f086f20969db116d0e |
| finalizeGameLiability(3) | 0x6c96712f9d0bb18330172eac7b828882a45e8ed21c8df102caa129d11f815c8f |
| Final State | winnerCounts [0,0,0,0]; liabilityFinalized true; rolloverableNative 0.001901611516131427 ETH. |

Game 3 provided the broadest V2.1 validation run, with eight tickets, displayed selected numbers, VRF fulfillment, and full liability finalization.

# 11. Winner Processing and Liability Finalization

The V2.1 lifecycle requires a distinct winner-processing stage before finalization. finalizeGameLiability(gameId) correctly refused to proceed while winnerProcessingComplete was false.

| Gate | Validated Behavior |
|---|---|
| drawNumbers() | Requests VRF. Frontend may show pending until fulfillment. |
| VRF Fulfillment | Sets drawn state and nonzero winningNumbers. |
| calculateWinners(gameId) | Processes tickets, advances winnerCalcCursor, and sets winnerProcessingComplete when complete. |
| finalizeGameLiability(gameId) | Allowed only after winner processing completes. |
| No Winner Case | winnerCounts all zero; totalPrizeLiabilityNative and claimReserveNative remain zero. |

## Security Finding

The contract correctly blocked finalization before winner processing was complete. This is a positive validation of lifecycle gating, not a defect.

# 12. Rollover and Reserve Accounting Review

Games 1-3 produced no prize-tier winners. The tested prize pools therefore became rolloverable after finalization.

| Game | Total Tickets | Winner Counts | Rolloverable Native |
|---|---|---|---|
| 1 | 3 | [0,0,0,0] | 0.000476413003915266 ETH |
| 2 | 1 | [0,0,0,0] | 0.000634900162703123 ETH |
| 3 | 8 | [0,0,0,0] | 0.001901611516131427 ETH |

## Reserve Readback

After Game 3 finalization, reservedNativeBalance was reported as 0.003169352526885719 ETH and excessNativeBalance as 0 ETH. This indicates native accounting is tracking contract obligations and rollover/reserve state rather than exposing unaccounted ETH as excess.

# 13. Transaction Economics and Gas Fee Review

A mainnet ticket purchase fee concern was diagnosed during V2.1 testing. The issue was primarily wallet priority fee selection rather than Ethereum base fee or an obvious V2.1 contract defect.

| Observation | High-Fee Buy | Low-Fee Buy |
|---|---|---|
| Tx Hash | 0xe9d4d57d6a40ec286a0a575bf081d330fd092cfda9c84eee5749423afe514b0c | 0xe10219c4c0aafa1911e906cf79dc51a0fdb08659cd1cd7df6ecbc45d908a4f54 |
| Ticket Value | 0.000263898198630897 ETH | 0.000263898198630897 ETH |
| Tx Fee | 0.000426123252011118 ETH | 0.000012453309220842 ETH |
| Gas Price | 2.040321818 gwei | 0.047869542 gwei |
| Priority Fee | 2 gwei | 0.000125687 gwei |
| Result | Fee exceeded ticket price | Fee approximately $0.02 |

## Recommended UX Note

During low urgency testing, users can reduce MetaMask max priority fee while keeping max fee above the current base fee. Public UI should avoid promising fixed gas costs because Ethereum fees fluctuate by network conditions and wallet settings.

# 14. Frontend Countdown and State UX

Countdown behavior was reviewed during active and finalized game states. The correct UX depends on the current game lifecycle.

| State | Expected Countdown Behavior |
|---|---|
| Setup | No active countdown; setup/private test state if currentGameId = 0. |
| Open Game | Countdown to game.endTime; helper text 'Ticket entry closes in'. |
| Closed / Awaiting Draw | Show Closed; purchase disabled; helper text 'Ticket entry closed'. |
| Drawn / Awaiting Finalization | Show drawn state; purchase disabled; helper text 'Awaiting finalization'. |
| Finalized / Claim Open | Countdown to claimDeadline; helper text 'Claim closes in'. |

## Validation Note

During Game 3, the frontend showed an active countdown while tickets were live and switched to closed/finalization states after draw and finalization. This behavior should remain a regression check before public promotion.

# 15. Security and Integrity Review

| Control Principle | V2.1 Result |
|---|---|
| Direct-wallet system only | Passed. User wallet interacts with LottoETH contract directly. |
| No G.A.P.S. vault routing | Passed. No vault/bot capital path used. |
| VRF draw gating | Passed. drawNumbers gated by game end, no pending request, and consumer readiness checks. |
| Finalization gating | Passed. finalizeGameLiability blocked until winner processing completed. |
| No fake tickets | Passed. Ticket numbers displayed from V2.1 getters or explicit fallback. |
| No fake winners | Passed. winnerCounts remained zero when no prize-tier winners existed. |
| Secrets | Private keys were not included in frontend or audit content. |

## Audit Boundary

This is an internal validation and manual regression report. It is not a third-party formal security audit. External review remains recommended before major public prize pools or large marketing-driven traffic.

# 16. Known Cold, Disabled, or Pending Areas

| Area | Status | Reason |
|---|---|---|
| Multi-ticket quantity purchase | Pending focused validation | Quantity UI exists; one-transaction multi-ticket path should be explicitly confirmed with quantity 2 or 3. |
| Claim flow with actual winner | Pending | Games 1-3 had no winners; claimable prize path should be tested when a qualifying ticket exists. |
| Long-duration public game | Pending | Testing used 300-second duration; public schedule should be set intentionally. |
| Frontend gas education | Recommended | MetaMask priority fee strongly affected user cost. |
| External audit | Recommended | Internal report does not replace independent contract security review. |
| Large prize pool | Pending | Prefunded public prize behavior should be separately tested and documented. |

# 17. Mainnet Transaction Evidence Summary

| Flow | Hash / Value | Result |
|---|---|---|
| Deploy V2.1 | 0x32c6eae414948e89f5631ff10ecfe1312af9a7a5831a295fe32cafb790938bc2 | Contract deployed. |
| Add VRF Consumer | 0xbd66f33285a8c8decc40aef504c28bf14f17700e4436d54ee4a22a78fdd43edb | V2.1 listed as consumer. |
| Set Duration | 0x23e2f9928213b12e939527d518a7d3ef18c85e0e8608a2ad0e784d90777c834e | gameDuration = 300 seconds. |
| Unpause | 0xec5cfbdf7cc46054a476d607f0ea6cab84bb32c87ae914f7f50f136aa13a526c | paused = false. |
| Game 1 finalize | 0xe04e640d97d4dd48dacfe611b8c586bf2b81df9f4ea0bac09252c366ed11a4eb | Game 1 finalized. |
| Game 2 finalize | 0x7c53286bddb8d2b1300e850a68edd3dd371f6d5a70984cacadb81d1407d7d958 | Game 2 finalized. |
| Game 3 finalize | 0x6c96712f9d0bb18330172eac7b828882a45e8ed21c8df102caa129d11f815c8f | Game 3 finalized. |

Every listed transaction is intended to be independently verifiable on Etherscan. Rows should not be used for public claims if a hash cannot be confirmed.

# 18. Recommended Next Validation Path

- Run a focused quantity purchase test: quantity 2 first, then quantity 3 or 5 if the first test passes.
- Confirm quoteTicketPriceNative(quantity) updates accurately and that one transaction mints/displays multiple tickets.
- Add public-facing guidance that gas fees vary and wallet priority fee settings affect cost.
- Test at least one qualifying winner/claim path using a controlled test scenario or future low-value validation game.
- Before the first promoted public game, set the intended game duration and prize policy, then repeat start/draw/finalize readbacks.
- Preserve direct-wallet separation from G.A.P.S. and do not introduce vault or bot logic into LottoETH.

### Release Readiness Direction

V2.1 has validated the core lifecycle. The remaining launch polish is UX/economics oriented: quantity buys, gas guidance, public duration, and winner/claim proof once a qualifying ticket exists.

# 19. Final Internal Audit Conclusion

LottoETH V2.1 successfully validates the direct-wallet ETH lottery lifecycle on Ethereum Mainnet. The frontend now points to the V2.1 address, uses V2.1 ABI getters as the primary data source, and displays selected ticket numbers without relying on event-log recovery as the normal path.

Games 1, 2, and 3 completed through drawNumbers, Chainlink VRF fulfillment, calculateWinners, and finalizeGameLiability. Each game had zero prize-tier winners during the validation run; each finalized prize pool became rolloverable according to readback.

The most significant operational finding was not a broken contract path, but transaction economics: wallet priority fee settings can cause ticket-buy fees to exceed ticket price. A later low-priority-fee transaction demonstrated materially lower cost. The next validation should prove multi-ticket quantity purchase in one transaction to further reduce repeated gas overhead.

### Final V2.1 Statement

Direct wallet connects. User buys with ETH. Chainlink VRF draws. V2.1 getters expose selected tickets and claim state. Games 1-3 prove the mainnet draw, winner-processing, finalization, and rollover path. If it is not verifiable on-chain, it does not exist in George.