Vault Reveal

Specification v4 | 2 November 2026 | Model vault-reveal-fixed-1

Virtual-credit prototype. Not laboratory-certified. No deposits, withdrawals or real-money prizes.

Round and fixed prizes

Instant Win / match-three reveal. One wager creates a 3 x 3 fixed board on the server before the first selection. Start with five picks; touch or click an unopened position. The first three identical ordinary symbols settle one gross prize. Awards do not stack. Exhausting picks without a triple returns zero. There is no optional purchase, early cashout or separate bonus wager.

Symbol	Gross return / original bet
Cash	1.5x
Bonds	2x
Gold	3x
Handgun	5x
Diamond	10x

Display theme vault-loot-1: Cash 1.5x, Bonds 2x, Gold 3x, Handgun 5x, Diamond 10x. Only labels/artwork change. Stored codes remain cherry / lemon / bell / diamond / crown respectively, retaining all old rounds, exact payouts and admin traceability.

Keys at fixed random positions

A Key consumes ONE pick and grants TWO: replacement plus one net extra reveal. Zero / one / two Keys are placed with probabilities 83% / 15% / 2%; Keys are not forced into reveal steps 2 or 4. At most two exist. Finding 0 / 1 / 2 Keys permits up to 5 / 7 / 9 physical tiles, including up to 5 / 6 / 7 ordinary symbols. Two Keys can allow all nine tiles to open unless an earlier triple ends the round. A Key revealed only after settlement grants no picks.

Post-loss opening

Only after a round is SETTLED with zero payout, remaining cards may turn over to show their actual original symbols. They are marked Not played, subdued and excluded from winning highlights. These were genuine original positions, not symbols generated after loss. They cannot award prizes, grant Keys or reopen the round. Winning hands leave unused cards closed. Some boards contain no possible triple. No near-miss arrangement is substituted or manufactured. Optional disclosure never blocks Play again.

Full-round results

Metric	Exact documented result
Theoretical RTP	24/25 = 96% overall and for each 0/1/2-Key board inventory
Hit frequency	56008749/100000000 = 56.00874900%
Net-win frequency	56008749/100000000 = 56.00874900%
Variance / SD	207709897/200000000 / 1.0190924811x original bet
Maximum gross / net	10x / +9x original bet
Maximum win probability	14479/6250000 = 0.23166400%
Bonus	Free extension; no separate stake or independent bonus RTP

Exact return distribution bands

Gross return / stake	Exact probability	Probability
0	43991251/100000000	43.99125100%
(0,1)	0/1	0.00000000%
[1,2)	22638839/50000000	45.27767800%
[2,3)	3721689/50000000	7.44337800%
[3,5)	2200029/100000000	2.20002900%
[5,10)	107/12500	0.85600000%
[10,infinity)	14479/6250000	0.23166400%

Construction and proof

The Key inventory is sampled first. For each Key inventory the server chooses a no-triple family or a family with six identical prize symbols plus distinct fillers. Exact integer family tickets are published in the math sheet and JSON. Labels and all nine positions are uniformly shuffled with rejection-sampled cryptographic integers. Inventories are correlated; symbols are not independent draws. Enumerated dominant arrangements: 84, 252 and 252 for 0, 1 and 2 Keys; no-triple arrangements: 1, 9 and 36. Exact terminal-state DP is independently checked by exhaustive arrangement enumeration.

The complete board is sampled and uniformly permuted once, before the first selection. Conditional on any revealed history, every unopened position is exchangeable. Therefore any adaptive choice of an unopened position has the same next-symbol distribution as sampling without replacement. The rules require completion until the first triple or exhaustion of picks, including server auto-completion. Induction over the finite tree proves identical return distributions for all position-selection policies. No hint, optional purchase or early cashout changes that tree. Layouts are correlated inventories, not independent symbol draws.

Bonus accounting and reproducibility

Base and extension contributions

Keys in board	First 5 physical tiles	Extension	Full round
0	24/25	0/1	24/25
1	148/175	4/35	24/25
2	148/175	4/35	24/25

Combined first-five contribution: 823/875. Extension contribution: 17/875. These are returns per original stake, not independently staked RTPs. Grouping by Keys actually found creates outcome-dependent selection; those groups do not each have a 96% conditional return.

Keys found	Group probability	Conditional mean return
0	91.28019998%	97.05750616%
1	7.99097085%	87.52735864%
2	0.72882917%	56.45061784%

Simulation confirms, never replaces, the proof

Seed	Rounds	Observed RTP	SE (pp)	z
0x51a7c0de	100,000,000	95.97728400%	0.01019092	-2.229042
0x20261024	100,000,000	96.00960300%	0.01019092	0.942309
0xc0ffee42	100,000,000	95.98230150%	0.01019092	-1.736692

Three predefined seeds, 100 million actual shuffled-board rounds per seed; 300 million total. Independent reveal/pick evaluation. All |z| values must be at most 3; the command fails otherwise. No seed selection after observing a result. Regenerate with npm run math inside vault-reveal.

Inputs, exact fractions and source SHA-256

Online math sheet | Machine-readable report

Bet ladder and limits

USD: 0.02, 0.10, 0.20, 0.50, 1, 2, 5, 10, 20, 25, 50, 100, 200, 500. Bets are even integer minor units so every 1.5x award is integral for supported currency exponents 0, 2 and 3. Exponent changes require compatible operator configuration and currency integration; the current public demo uses USD / 2 decimals. Maximum USD stake $500 and gross $5,000. Balances, wins and net results are virtual credits.

Server and client responsibilities

Existing Supabase project and Edge Function remain authoritative for RNG, debit, payout and balance. The browser sends actions, position, revision, request ID and explicit model version on a new wager. The entire fixed board remains private until permitted post-loss disclosure. Active and winning responses, normal history, DOM and browser storage contain no unrevealed layout. Loss disclosure is a separate own-session read-only action; it cannot change round state, receipts or the money ledger.

Round/session IDs, recovery and safeguards

vault_rounds persists the model version and private board from wager acceptance; vault_events stores actual game actions. Existing request receipts, revision/concurrency checks, debit/collect idempotency, rate limiting and last-ten UI history remain. Reload resumes the same session and board. A database trigger rejects changing a committed fixed board. Operator-only rollback remains limited to one per session, before any reveal. Backend unavailability disables play; no browser RNG fallback is used.

Time and automatic completion

After 10 minutes without an accepted reveal, or 30 minutes total, the server completes remaining paid picks against the same fixed board and settles at the first triple or pick exhaustion. Accepted actions update idle time; polls, invalid requests and receipt retries do not. The existing once-per-minute Vault scheduler invokes the version-aware current function; network/scheduler delay can postpone presentation. Values are configurable in operator JSON.

Version compatibility and private admin

Existing vault-reveal-b-1 rounds retain their original sequential engine and rules. Old open browser tabs create legacy rounds until they load the updated client; the new client explicitly opts new wagers into vault-reveal-fixed-1. Old records are not rewritten. The restricted read-only admin retains money/event views and receives the original fixed board in its sanitized replay projection; old tapes stay explicitly sequential. Post-loss symbols are never paid actions.

Local alternative and configuration

Node + SQLite runs the same fixed engine locally as an explicitly labelled virtual-credit server. Versioned SQL migrations retain rounds, receipts and append-only events. Configuration holds prizes, integer family tickets, Key inventory/rules, bet ladder, limits, idle thresholds, reminders, locale and presentation timings. Session and pending-request credentials stay in browser storage; service/database/operator credentials remain server-side environment variables.

Release gates and disclaimers

Not laboratory-certified, regulator-approved or ready for real-money use. Physical weak-Android and iPhone HTTPS acceptance (touch, audio unlock, reload, rotation, poor network and tab switching), operator-wallet integration, independent math/security review and applicable regulatory review remain separate release gates. Browser viewport tests and simulation are engineering verification, not certification. No claim of an independently certified provably-fair verifier is made.

Back to site | 40-second operator walkthrough