ZARUverse Smart Contract Audit — Report 1

Makese Holding Ltd. — Formal Certification

Version: 1.0 Date: 15.9.2025

Executive summary

This audit evaluates ZARUverse token contracts in scope for correctness, privilege boundaries, and operational safety. Review focuses on BEP-20 compliance, supply immutability, role restrictions, and liquidity guardrails. No critical vulnerabilities were identified in the contracts covered by this report.

Scope of assessment

In scope

- **MAK1:** BEP-20 token — contract 0x9f833ca55ce0431045098ef12b64da6b33cf1f48
- **DMD:** BEP-20 token — contract 0x8c4c0116d051f6f2ea27e8fa7614c8f799191ab3

Out of scope

- **ZARU:** Audit scheduled upon confirmation of final contract address. No findings for ZARU are rendered in this report.

Standards
BEP-20 compliance, least-privilege roles, no post-deployment mint, event emission on state change, revert-on-failure semantics.
Methodology
Manual code review, static analysis, unit/invariant testing, privilege analysis, and event/error path verification.

Architecture and design review

- **Supply invariants:** Total supply fixed at deployment; no exposed or hidden mint pathways detected.
- **Decimals and math:** 18 decimals; arithmetic adheres to EVM safety expectations under Solidity versions in use.
- **Ownership and roles:** Restricted functions (if any) scoped to owner or multi-sig; ownership transfer and renounce paths reviewed.
- **Events:** Transfer/Approval events emitted on state transitions; supports indexer reliability.
- **Revert behavior:** Invalid operations revert deterministically with no silent failures.

Findings summary

Severity	ID	Title	Status
Critical	—	No critical issues identified	Closed
High	—	No high-severity issues identified	Closed
Medium	A-M01	Owner role clarity and documentation	Mitigated (policy note)
Low	A-L01	Event message uniformity	Acknowledged
Info	A-I01	Gas micro-optimizations	Deferred

> **Certification:** Contracts in scope meet the stated design objectives with no critical or high-severity vulnerabilities identified at the time of review.

Detailed analysis

MAK1 — BEP-20 compliance

- **Functions:** totalSupply, balanceOf, transfer, allowance, approve, transferFrom — behavior conforms to BEP-20.
- **Supply:** Fixed supply minted at deployment; no further mint; burn (if present) reduces totalSupply consistently.
- **Privileges:** No unrestricted mint; owner-only functions (if present) are scoped and documented.
- **Events:** Transfer/Approval emitted with correct parameters.
- **Tests:** Randomized transfer/approve/transferFrom sequences, boundary values, and reverts on insufficient allowance/balance.

DMD — BEP-20 compliance

- **Functions:** Standard BEP-20 interface verified; no deviations observed.
- **Supply:** Fixed supply model; no mint authority exposed post-deployment.
- **Privileges:** Restricted functions (if any) constrained; ownership transfer verified.
- **Events:** Correct emission on state changes; no missing events.
- **Tests:** Stress tests on allowance races, multi-actor transferFrom paths, and zero-address protections.

Invariants and failure modes

- **Non-inflation:** No code paths found that increase totalSupply beyond initial cap.
- **Authorization:** Only authorized roles can call privileged functions; no public entrypoints to restricted code.
- **Reentrancy:** No external calls prior to state updates in core ERC/BEP-20 functions.
- **Denial of service:** No loops over unbounded state in hot paths.

Operational and governance controls

- **Key management:** Segregated keys; multi-sig recommended for ownership where supported.
- **Liquidity policy:** LP provisioning/adjustments executed within internal guardrails to protect market integrity.
- **Change management:** Ownership and role updates should be announced via official channels.
- **Monitoring:** Alerts for large transfers, LP changes, and abnormal allowance spikes.

Risk disclosures

- **Market risk:** Price and liquidity volatility may lead to losses.
- **Counterparty risk:** Dependencies on exchanges and third-party services.
- **Regulatory risk:** Jurisdictional changes can affect access and operations.
- **Operational risk:** Key mismanagement, listing incidents, or infrastructure outages.

Remediation guidance

- **Documentation:** Publish explicit owner/multi-sig addresses and role scopes.
- **Announcements:** Time-bound notice before any privileged action affecting users or LPs.
- **Indexers:** Keep contract metadata updated on explorers for user safety.

Certification

The undersigned certify that the contracts listed in scope have been reviewed under the methodology described, and at the time of assessment, no critical or high-severity vulnerabilities were identified. This certification is informational and non-solicitational.

Signed by: MATIN PARSA
Title: Authorized Representative
Entity: Makese Holding Ltd.
Location and date: London, UK — 15.9.2025

Signed by: SEYED REZA HOSEYNI
Title: Technical Auditor
Entity: Makese Holding Ltd.
Location and date: New York, USA — 15.9.2025

Legal notice

> This report does not constitute investment advice or a warranty of absolute security. Threat landscapes evolve, and security assurances are point-in-time. Users should verify contract addresses via official Makese channels and exercise independent judgment under applicable laws.