CAKE MONSTER

RESEARCH WHITEPAPER

A protocol-evidence and risk framework for the legacy MONSTA system

Research edition 1.0 / 25 August 2026

Independent research publication. Not the historic project whitepaper, a revived dApp or a statement from the original team.

Executive summary

- Cake Monster was designed as a BNB Chain protocol in which MONSTA transaction activity, token-supply reduction, liquidity operations and reserve-vault accounting interacted across recurring cycles.
- The documented MONSTA address is an upgradeable proxy. Address identity, implementation code and administrator control must therefore be checked as separate layers.
- Historic formulas describe intended behavior, not a current entitlement. Present-tense claims require a named block, callable implementation, verified custody and executed transactions.
- This independent paper is educational. It provides no wallet connection, trade execution, price target, return promise or claim instruction.

1. Purpose and publication boundary

This is an original Cake Monster Research publication. It is not the historic project whitepaper, a revived dApp, a replacement token specification or a statement from the original Cake Monster team. It reconstructs the legacy protocol model from documented terminology and tests that model against a dated set of public BNB Chain records.

The distinction matters because protocol documents answer a different question from contract state. A design paper can show what a version intended to do. An explorer can show which address exists and which transactions executed. Verified implementation code can show callable behavior. None of those records alone proves that a website, team, reward process, reserve claim or support channel remains active today.

The goal is to give readers a durable method. Every important statement should be classed as historic design, direct observation, external technical context or unresolved inference. If a claim cannot be assigned to one of those categories, it should not be treated as established fact.

- Independent research, not official project documentation.
- Historic rules are labeled as historic.
- Current observations name a block and date.
- Unknown custody, eligibility or activity is left unknown.

2. Protocol identity and system layers

Cake Monster refers here to the legacy BNB Chain DeFi protocol built around the MONSTA token. The documented token address is 0x8a5d7fcd4c90421d21d30fcc4435948ac3618b2f. A complete address is necessary because a name, ticker, logo or matching prefix cannot establish identity.

The token address is a transparent upgradeable proxy rather than a permanently self-contained contract. Calls sent to the proxy can delegate execution to a separately stored implementation. A proxy administrator can change that implementation when authorized. Researchers must therefore record three identities together: proxy, current implementation and administrator.

Interfaces form another layer. An old Cake Monster website can disappear while the proxy still exists. A token can transfer while reward functions, vault maintenance or development are inactive. A newer MONSTA-branded system can publish different rules without silently changing the legacy contract. Status must be evaluated component by component.

- Network: BNB Chain.
- Legacy proxy: 0x8a5d7fcd4c90421d21d30fcc4435948ac3618b2f.
- Observed implementation: 0x68f9ce4817f7edb62f8981c6d399a687f930922c.
- Observed proxy administrator: 0x5e92adf8145342c18f373e70dc75fe6e7d75b235.

3. Reconstructed historic protocol model

The legacy design joined management, policy and transaction volume. MONSTA transfers were described as feeding a five-percent tax: one half associated with supply reduction and one half associated with a temporary-vault path. The temporary balance could then support liquidity operations and the acquisition of external reserve assets. This paper preserves that model as a historic specification, not as a statement that every current transfer follows it.

Supply was framed in cycles rather than as a simple fixed maximum. A cycle began from a documented ten-billion-MONSTA scale and used burns or related mechanisms to contract supply. End conditions could open settlement phases, remove or restore liquidity, make reserve shares available under defined eligibility rules and later restore supply for another cycle. Calling the system merely deflationary omits the possible relaunch side of the model.

Reward concepts included reserve slices, Crumbs, staking, vault management incentives, inactivity processing, NFTs and games. Each depended on its own contract, state, threshold, snapshot or interface. Holding MONSTA alone did not prove that every feature was callable or that a reserve share existed at a later date.

- Model tax: 5% total, historically described as equal burn and temporary-vault halves.
- Model cycle scale: 10 billion MONSTA before documented contraction mechanics.
- Reserve concept: acquire and hold assets distinct from MONSTA.
- Settlement concept: eligibility, snapshot, claim window and relaunch were separate states.

4. Evidence hierarchy

Executed transactions and reproducible contract reads are the strongest evidence for what happened on-chain. Verified implementation code explains possible execution paths, but code presence alone does not prove that a method ran, remains economically useful or is supported by a working interface.

Historic specifications and first-party announcements establish intent, terminology and publication sequence. They remain important because later summaries can compress several different versions into one story. They do not overrule the deployed implementation or prove that a promised feature shipped exactly as described.

Trackers provide useful market, token and TVL context. Their numbers have scope limits. Market capitalization does not prove reserve backing; TVL does not capture every token behavior; a token price does not establish liquidity depth; and a verified contract label does not resolve upgrade authority.

- First: executed chain records at a named block.
- Second: verified implementation code and proxy storage.
- Third: dated technical specifications and announcements.
- Fourth: independent technical documentation and market directories.

5. Dated BNB Chain observation

Cake Monster Research read the legacy system at BNB Chain block 117,963,261 on 25 August 2026. Two public RPC nodes agreed on the proxy implementation, administrator and reported total supply used in this publication. Static values are deliberate: a reader can reproduce the observation rather than mistake an old response for a live feed.

At that block the proxy pointed to implementation 0x68f9ce4817f7edb62f8981c6d399a687f930922c, and the EIP-1967 administrator slot resolved to 0x5e92adf8145342c18f373e70dc75fe6e7d75b235. The reported total supply was 8,215,483,781.704558 MONSTA.

The principal MONSTA/WBNB pair used in this research held 397,135,827.093735 MONSTA and 1.070050 WBNB. Its stored reserve timestamp corresponded to 14 January 2025 at 17:35 UTC. That old timestamp is a liquidity-activity warning. It is not a live price, proof of abandonment or proof that no other pool exists.

- Observation block: 117,963,261.
- Reported supply: 8,215,483,781.704558 MONSTA.
- Principal pair: 0x55c49d1cd54126c69f22c2e9eebd1fef5e620fa.
- Unresolved in this snapshot: definitive Gravity Vault custody and a current claim path.

6. Material risk framework

Upgradeability creates change risk. A stable proxy address can execute different code after an authorized upgrade. Review the EIP-1967 slots, implementation bytecode, administrator history and relevant upgrade transactions before assuming that an older analysis still applies.

Liquidity creates execution risk. A displayed token price can be derived from a pool too shallow or stale to support the proposed transaction. Reserve ratios, recent swaps, route fees, token taxes and expected price impact should be modeled together. A market-cap figure based on a thin quote should not be compared casually with a vault value.

Reserve claims create custody and eligibility risk. A reserve must be tied to identifiable addresses, assets, balances and control rules. A claim additionally needs an eligible supply definition, snapshot, allocation, deadline and executable method. A whitepaper formula or dashboard number is not a substitute for those records.

Wallet interactions create security risk. A research site has no need to request a seed phrase, approval, signature or deposit. Readers should inspect calldata, spender addresses and current implementation behavior before authorizing any transaction through another interface.

- Proxy and administrator risk.
- Thin-liquidity and fee-on-transfer risk.
- Reserve custody and claim-eligibility risk.
- Interface, approval and wallet-signature risk.

7. Reproducible verification workflow

Begin with identity. Copy the complete MONSTA proxy from a trusted record and compare all 42 characters. Read the implementation and administrator slots at one block. Record the RPC provider, block number, response and timestamp so another researcher can reproduce the result.

Move next to the specific claim. For a tax question, simulate or inspect a transfer receipt. For a vault question, identify custody and reconcile asset balances. For a supply question, separate circulating, contract-held, pool-held and burned amounts. For an activity question, check transactions, liquidity syncs, callable functions, interfaces and maintained code independently.

Finish by stating the boundary. An observation supports only the component and block inspected. If evidence is missing, publish the missing field rather than filling it with a promotional assumption. Update the visible modification date and retain older observations when material state changes.

- Name the address, method, block and data source.
- Keep historic intent separate from executed state.
- Test one claim at a time.

- Record uncertainty and unresolved fields.

8. What the Cake Monster record supports

Cake Monster remains a notable example of early BNB Chain experimentation with transfer taxes, token burns, liquidity routing, reserve assets and game-like protocol cycles. Its design cannot be summarized accurately by a token chart or the word deflationary alone.

The public record supports the identity of a legacy proxy, a dated implementation and administrator, a reported supply and a principal-pair observation. It also supports a historic model involving tax, reserve and cycle mechanics. It does not, without further evidence, establish a current dApp, supported reward program, claimable reserve, active maintainers or safe transaction path.

A useful whitepaper should make a system easier to test. This research edition therefore ends with a method rather than a promise: verify identity, version, custody, liquidity, eligibility and execution separately; record the block; and never turn an unresolved field into certainty.

References

Primary technical records used by this research edition:

1. MONSTA legacy proxy
https://bscscan.com/token/0x8a5d7fcd4c90421d21d30fcc4435948ac3618b2f

2. Observed MONSTA implementation
https://bscscan.com/address/0x68f9ce4817f7edb62f8981c6d399a687f930922c#code

3. Observed proxy administrator
https://bscscan.com/address/0x5e92adf8145342c18f373e70dc75fe6e7d75b235

4. Principal MONSTA/WBNB pair
https://bscscan.com/address/0x55c49d1cd54126c69f22c2e9eebd1fef5e620fa#readContract

5. Recorded implementation upgrade
https://bscscan.com/tx/0x45b37617197b90d713fc0522d2c0a6b9154cdf9355eb831cfea14d6a326e5f12

6. EIP-1967 proxy storage standard
https://eips.ethereum.org/EIPS/eip-1967

7. Historic Solidity Finance review
https://solidity.finance/audits/CakeMonster/

8. Cake Monster tracker methodology
https://defillama.com/protocol/cake-monster

Publication boundary

Cake Monster Research does not request wallet connections, approvals, signatures, seed phrases or deposits. This paper is educational and does not promise a reserve claim, project revival, price outcome or return.