



Canswap .live

PROTOCOL WHITEPAPER · VERSION 1.0

Brand Tokens: portable loyalty, programmable participation.

A protocol for fixed-supply community markets that can become verified, brand-operated loyalty economies —powered by transparent exchange, brand-owned market fees and evidence-based Quests.

NETWORK

BNB Chain reference
implementation

PUBLICATION

October 2026

STATUS

Technical working paper

A market for loyalty that begins with community and matures through verified brand participation.

Brand Tokens transform loyalty from a closed merchant database into a user-controlled, programmable economic relationship. The protocol assigns one canonical token identity to each brand, fixes its total supply at 21,000,000 units, reserves 19,950,000 units for the verified brand, and makes community participation possible before formal brand onboarding. Official swaps credit a fixed 5% fee in the market's quote asset to isolated on-chain accounting for the relevant brand.

Native markets use CDO as their quote asset. Before claim the entire fee belongs to the brand; after verified onboarding only future fees split 2.5% to the brand and 2.5% to Candao. Quests extend the model from exchange into measurable real-world participation.

Protocol thesis

Utility is defined by the brand. Price is discovered by the market.
Participation is proven through evidence.

What this paper specifies

- Canonical Brand Token creation and immutable supply.
- The transition from community-created market to verified loyalty programme.
- Brand-owned 5% fee accounting and claim rights.
- Non-custodial settlement and liquidity interfaces.
- Quests, creator proof, UGC and reputation.
- Security, governance, privacy and deployment constraints.

What this paper does not promise

- No equity, ownership, dividends or debt rights.
- No guaranteed price, liquidity or investment return.
- No implied affiliation before verified brand claim.
- No automatic truth from social metrics or AI scoring.
- No production deployment without audit, governance and legal gates.

STATUS AND LEGAL NOTICE

This document describes a protocol design and reference implementation. It is not an offer of securities, investment advice, a guarantee of token utility, or evidence that any illustrated brand participates. Legal classification depends on actual rights, marketing, transferability and jurisdiction.

Structure of the paper

01	Problem and design goals	04	02	System model and actors	05
03	Brand Token lifecycle	06	04	Token and supply specification	07
05	Identity, verification and claim	08	06	Utility and redemption	09
07	Market and fee economics	10	08	Atomic settlement architecture	11
09	Liquidity and market integrity	12	10	Quests: demand to settlement	13
11	Proof, rewards and reputation	14	12	Maps, Live and demand-backed action	15
13	Ghosts, Circles and physical UX	16	14	Security and protocol invariants	17
15	Governance and decentralization	18	16	Privacy, safety and compliance	19
17	Multi-chain identity	20	18	Reference implementation	21
19	Conclusion	22	A	Glossary and references	23

Reading conventions

Must identifies a protocol invariant or release requirement. **Should** identifies a recommended product or security property. **May** identifies an optional implementation choice. “Brand” refers to the verified entity only after successful onboarding; before that point, the associated token is a community-created market token and invitation to collaborate.

Three layers, one product

Brand Token Protocol defines identity, supply, claims and brand economics. **Canswap** supplies discovery, non-custodial markets and liquidity interfaces. **Quests** supplies business demand, proof, creator media, settlement and reputation. None of these layers may silently manufacture affiliation, market data or completed work.

Traditional loyalty traps value in isolated ledgers.

Most loyalty systems are databases controlled by one merchant. Customers earn primarily by spending, redemption follows opaque catalogue rules, rewards are difficult to transfer, and unused value expires or becomes irrelevant.

DIMENSION	LEGACY LOYALTY	BRAND TOKEN PROTOCOL
Custody	Points remain in a merchant database.	User holds tokens in a compatible wallet.
Earning	Primarily purchases.	Purchases, referrals, creation, attendance, Quests, community work and verified milestones.
Utility	One closed redemption catalogue.	Brand-defined redemption, access, membership, gifting and supported exchange.
Portability	Usually none.	Transfer or exchange where permitted and liquid.
Measurement	Spend history.	Evidence-based participation and business outcomes.

Design goals

G1

One identity per brand

Prevent accidental duplicate markets through a canonical registry key.

G2

Fixed supply

No owner, mint function or discretionary inflation after creation.

G3

Permissionless invitation

A community can create a market without falsely claiming endorsement.

G4

Verified activation

Only an authorised brand can claim the reserve, treasury and official profile.

G5

Brand-owned fees

Qualifying market fees accrue for the brand, including before onboarding.

G6

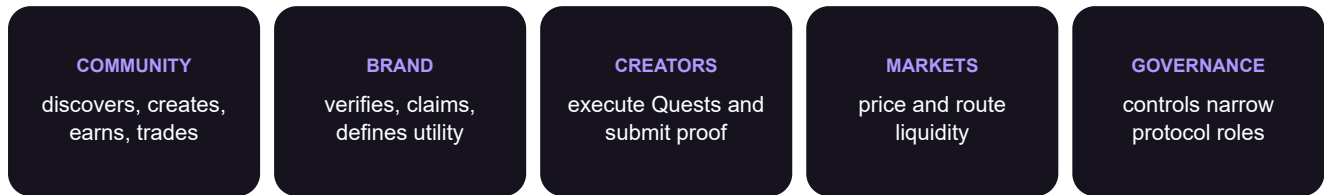
Measurable action

Quests reward real execution rather than empty clicks or self-declared reach.

Non-goals

The protocol is not a universal equity issuance system, a guarantee that every brand will participate, a replacement for all advertising, a promise of permanent redemption value, or a mechanism for manufacturing liquidity. Exchangeability is an exit and discovery path; it is not the only reason the token should exist.

A protocol with explicit roles and trust boundaries.



ACTOR	AUTHORITY	EXPLICIT LIMITATION
Token creator	Creates the unique token and receives the first-buyer window.	Does not become the brand, control its reserve or receive brand fees.
Verified brand treasury	Claims reserve and accrued fees; controls official metadata.	Cannot inflate supply or replace the deployed token.
Trader / holder	Holds, transfers and trades through supported venues.	Receives no company ownership or guaranteed utility.
Quest sponsor	Defines a mission, eligibility, proof and reward.	Cannot change accepted terms retroactively.
Quest participant	Chooses missions and submits evidence.	Must comply with disclosure, safety and evidence rules.
Governance	Verifies treasuries and manages approved adapters/metadata recovery.	Cannot mint, seize reserves, recover settlement funds or bypass timelock policy.

Trust boundary

Wallets sign token, liquidity and claim operations. Smart contracts enforce supply, uniqueness, launch timing, fee accounting and treasury rights. Indexers, search, video and analytics improve usability but must not be required to withdraw, claim or execute a valid on-chain operation. Brand verification remains a real-world assertion and therefore requires governed evidence review.

Canonical terminology

Unclaimed token: community-created memecoin and invitation to collaborate; not endorsed or utility-backed by the named brand. **Claimed token:** immutable token whose verified brand treasury can define official loyalty utility and claim protocol allocations. Verification changes authority and meaning—not contract address or supply.

From discovery to a verified loyalty economy.

1

Canonical discovery

A user searches the local brand registry. Missing brands may be enriched once through an external provider and persisted; repeated page visits do not repeatedly purchase the same metadata.

2

Permissionless creation

The factory accepts the canonical brand identifier, immutable token name, immutable symbol and public metadata URI. A duplicate brand identifier reverts.

3

Atomic allocation

All 21,000,000 units are minted once: community, Candao Foundation and brand reserve. The reserve is registered in the reserve vault in the same transaction.

4

Creator-first launch

For 24 hours, only the creator wallet may make the first market purchase. At the block-time deadline, public access opens automatically without a server or administrator.

5

Community market

Price can be discovered where liquidity exists. The interface must label the token unclaimed and disclose that there is no brand affiliation or promised utility.

6

Verification and claim

An authorised representative proves control. Governance binds a treasury through the registry. That treasury claims the fixed reserve and all accrued market fees.

7

Loyalty operation

The brand publishes benefits, earning rules, redemption terms, Quests and disclosures. Future qualifying market fees continue accruing to the same treasury.

The creator starts a market. Only the verified brand can turn it into an official loyalty programme.

Exactly 21,000,000 units, minted once.

FIXED BRAND TOKEN SUPPLY

21,000,000



1,000,000

finite Genesis market · 4.7619%

50,000

Candao Foundation · 0.2381%

19,950,000

verified brand reserve · 95%

ERC-20 properties

- The reference token is non-upgradeable and has no owner.
- There is no public or privileged mint function after construction.
- The supply uses 18 decimals and is created atomically by the factory.
- The community and foundation allocations are transferred to predefined receivers.
- The brand allocation is held by a dedicated reserve vault until verified treasury claim.

$$\begin{aligned}
 S &= 21,000,000 \times 10^{18} \\
 S &= C + F + R \\
 C &= 1,000,000 \times 10^{18} \quad \cdot \quad F = 50,000 \times 10^{18} \quad \cdot \quad R = 19,950,000 \times 10^{18}
 \end{aligned}$$

Supply invariants

INVARIANT	REQUIRED CONDITION
Fixed ceiling	<code>totalSupply()</code> = S for the lifetime of the contract.
Allocation conservation	$C + F + R = S$ at deployment.
One reserve	Each canonical <code>brandId</code> registers one token and one reserve.
One-time claim	The reserve can move once, only to the registry's verified treasury.
No replacement	Metadata may change; the canonical token address may not.

"Pre-minted" in the economic model means the full fixed supply is created during token construction. The 19,950,000-unit brand allocation is not community inventory; it remains isolated in the reserve vault until claim.

Immutable token, controlled official context.

ERC-20 does not encode a logo, brand authority or rich loyalty terms. The registry binds those layers to a canonical brand identifier without replacing the token contract.

Registry record

FIELD	MEANING
brandId	Deterministic identifier derived from the canonical brand record.
token	Immutable Brand Token contract.
creator	Wallet that initiated permissionless creation; not the verified brand.
treasury	Verified brand-controlled wallet, ideally a multisig.
metadataURI	Public name, logo, description, utility and disclosure document.
verified	On-chain state confirming treasury binding after evidence review.

Claim sequence

1. The brand prepares one immutable claim covering its canonical domain, token, treasury, Brand Fee wallet and independent Reserve/Genesis/Fee choices.
2. The treasury signs that exact EIP-712 claim.
3. The canonical domain publishes its hash and wallet in a DNSSEC-protected TXT record.
4. An authenticated brand email passes strict DKIM, SPF and DMARC alignment and matches the same claim.
5. The designated approver signs the same hash but cannot edit or redirect it.
6. After the 72-hour cooldown, a fresh DNSSEC proof authorises finalisation.

Editable after claim

Logo, description, benefit catalogue, Quest links, redemption terms and official communication.
Metadata history should remain auditable.

Never editable

Token address, original supply, allocations, historical transfers and the fact that the market existed before claim.

Wallet and explorer visibility

Token logos are not stored natively in ERC-20. Wallets may obtain them from verified explorer metadata, curated token lists, indexers or user imports. Canswap therefore publishes a canonical metadata URI and token list, verifies source on the chain explorer, and stores durable logo assets. External wallet display remains subject to each wallet's ingestion policy.

Tokens should be useful before they are tradable.

A durable Brand Token economy starts with reasons to earn, hold and use the token inside a real relationship. Exchangeability provides portability; it cannot substitute for utility.

EARN

Purchases

Campaign rewards, repeat visits, subscriptions and qualified transactions.

EARN

Participation

Referrals, feedback, events, product testing, support and community work.

EARN

Quests

Verified visits, creator media, tutorials, local actions and measurable outcomes.

USE

Redemption

Products, services, upgrades, delivery, discounts and checkout rewards.

USE

Access

Early products, private events, priority reservations and gated communities.

USE

Membership

Transparent tiers, partner offers, gifts and brand-defined privileges.

Required programme disclosures

- What holders can receive and which entity supplies it.
- Whether redemption is fixed, dynamic, capacity-limited or time-limited.
- Eligibility, geography, refund treatment, expiration and transfer restrictions.
- Whether a benefit depends on holdings, earning history, identity or Quest completion.
- How programme changes are announced and whether accepted promises are grandfathered.
- Which activity is sponsored and which disclosure rules apply.

GOOD LOYALTY LANGUAGE

“50 tokens provide free delivery during the published campaign period, subject to the listed countries and capacity.”

PROHIBITED INVESTMENT FRAMING

“Buy because company growth will increase token value” confuses utility with expected profit and changes risk.

A brand defines what the token does. A market decides what traders pay. These values must never be presented as the same thing.

A fixed 5% fee belongs to the brand.

Every qualifying Brand Token swap charges 5% exactly once in that market's quote asset. Native CDO/Brand markets therefore accumulate CDO. Ordinary wallet transfers, rewards, redemptions and liquidity deposits are not swaps and carry no Brand Fee.

```
Given gross quote-asset settlement G:
brand fee f = floor(G × 500 / 10,000)
net settlement N = G - f
```

Single-brand route

For CDO→Brand or Brand→CDO, the complete fee f is recorded in CDO. Before verification it is 100% claimable by the brand. After verification, previously accrued CDO remains 100% brand-owned while future fees split 2.5% to the brand and 2.5% to Candao.

Brand-to-Brand route

There is one 5% fee in total, not 5% twice. Gross settlement is divided into two accounting shares. Each brand receives the fee calculated for its share; integer rounding is deterministic and bounded by settlement-token precision.

```
 $G_1 = \text{floor}(G / 2) \cdot G_2 = G - G_1$ 
 $f_1 = \text{floor}(G_1 \times 500 / 10,000) \cdot f_2 = \text{floor}(G_2 \times 500 / 10,000)$ 
total fee = f1 + f2
```

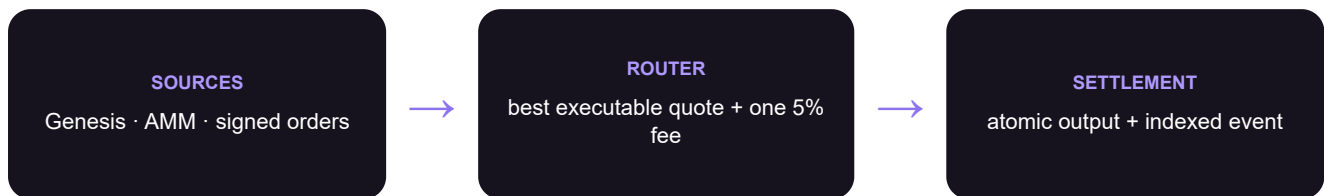
Claim protection

- Every settlement identifier can be processed only once.
- `claimable[brandId][asset]` never exceeds real vault collateral.
- No administrator can redirect a brand balance.
- Claims use checks-effects-interactions and non-reentrancy.
- Reserve, unsold Genesis inventory and accumulated fees are independent choices.
- Genesis CDO sale proceeds are permanent liquidity and never part of a Genesis claim.

SCOPE

The 5% rule applies to qualifying market swaps. Rewards, initial distributions, issuer redemptions and internal protocol movements may use separate disclosed rules. Network gas and external venue fees are distinct and must be shown before signature.

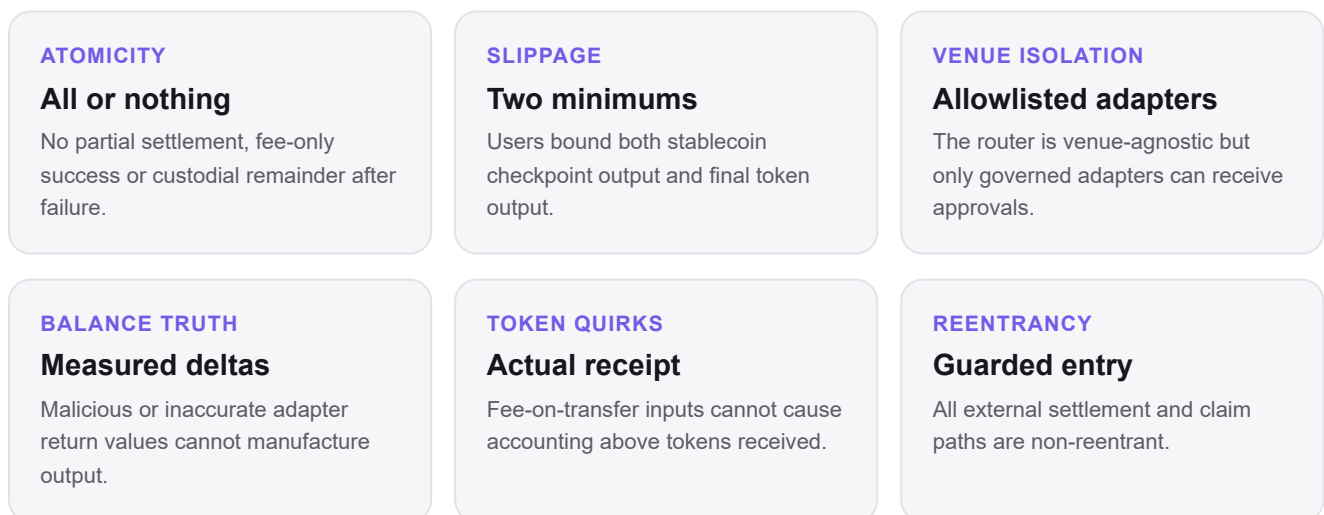
Adapters provide venues; the router enforces truth.



Router sequence

1. Validate token, amount, recipient, chain ID and deadline.
2. Quote finite Genesis inventory and the native CanSwap AMM.
3. Select the best executable source without inventing liquidity.
4. Pull only the required input and measure actual balance changes.
5. Credit BrandFeeVault once using a unique settlement identifier.
6. Apply the 0.30% AMM fee only when the AMM route is used.
7. Transfer output and enforce minimum received or maximum paid.
8. Emit the canonical settlement event for finality-aware indexing.
9. Revert the complete operation when any invariant fails.

Security properties



CanSwap has its own immutable native AMM, finite Genesis market and signed-order settlement. Narrow adapters may additionally consume external liquidity, but only fee-aware authorised venues receive official status.

Creation does not create liquidity.

A token contract can exist with no executable market. Every price, chart, market-cap calculation and quote must originate from confirmed market data, never a design mock or deterministic preview.

Liquidity lifecycle

- **Genesis:** one million Brand Tokens form a finite 0.1–199.9 CDO ask ladder; filled asks never regenerate.
- **Permanent CDO:** Genesis sale proceeds remain market liquidity and cannot be withdrawn by Candao or claimed by the brand.
- **User liquidity:** anyone may deposit CDO and Brand Tokens into the canonical constant-product pool and receives transferable accounting shares.
- **Price discovery:** real fills across Genesis, AMM and signed orders establish last price; users may quote any price in their own orders.
- **Exit:** user LPs may remove their own proportional assets and accumulated 0.30% fee through public contracts without CanSwap servers.

Market integrity requirements

RISK	REQUIRED RESPONSE
Zero liquidity	Disable executable quotes and display the exact pool state.
Thin liquidity	Prominent price-impact and minimum-received disclosure.
Manipulated spot price	Use suitable windows/oracles for analytics; never use spot as unquestioned redemption value.
Wash trading	Flag anomalous volume and avoid reward systems based only on raw turnover.
Fake market cap	Use confirmed circulating supply and live price; undeployed markets show no number.
Wrong token	Show canonical contract and verified registry binding.

Price is not utility

Market price may rise, fall or disappear. A claimed brand should publish utility independently of price. A holder must be able to distinguish current redemption terms, indicative market value and speculative expectations.

CDO ROUTING

CDO is the canonical quote asset of native Brand Token markets. The consumer route may begin or end in USDT/USDC, but the native sequence remains stablecoin → CDO → Brand Token and the reverse. The interface always shows the last recorded fiat value regardless of liquidity.

Ads buy impressions. Quests buy action.

A Quest is a business mission with a legitimate objective, defined participant, measurable completion condition and transparent reward. Creators are independent distribution operators—not anonymous advertising inventory.

1

Create the mission

Location, window, format, action, prohibited claims, disclosures, acceptance and economics.

2

Define the creator target

Geography, language, niche, audience fit, format, reputation and capacity.

3

Match or apply

Invite, approve or permit qualified instant acceptance while slots remain.

4

Execute

The creator travels or performs the remote task under the accepted brief.

5

Submit proof

Upload media, deliverables, codes, links, bookings, orders or other evidence.

6

Accept or dispute

The business reviews subjective quality separately from objective facts.

7

Settle

Release completion and later performance tranches under pre-agreed rules.

Terms must be known before movement

A creator should not cross a city, buy a product or produce media without knowing how acceptance works. Every Quest therefore specifies objective completion criteria, a response deadline and dispute path. Where evidence is objective and the sponsor does not respond, the undisputed portion may auto-release. Contested funds remain locked for the agreed review process.

Completion must mean more than pressing a button.

Layered Proof of Quest

1. **Presence:** opt-in geofence, venue QR/NFC, reservation check-in or one-time code.
2. **Time:** creation and submission occur inside the campaign window.
3. **Content:** platform ID, public link, media hash or creator-authorized API.
4. **Performance:** views, watch time, clicks, bookings, orders or CRM events.
5. **Acceptance:** business confirms subjective brand fit and accuracy.
6. **Settlement:** a durable record explains which condition released each payment.

Reward market

1. **Fixed completion:** highest certainty, bounded upside.
2. **Hybrid:** base completion plus measurable milestones.
3. **Commission-first:** smaller base plus attributed revenue or bookings.
4. **Pure performance:** no guaranteed completion payment; highest creator risk and normally higher potential upside.

Rewards may combine Brand Tokens, stable-value settlement, cash, commission, product/service perks or access where legitimately offered.

Reputation is multidimensional

Repeated execution creates a portable history: reliability, content quality, audience fit, professionalism, accuracy, conversion performance, communication, disputes and repeat hires. Creators also rate sponsors for truthful briefs, venue readiness, fair acceptance and correct settlement.

EVIDENCE PRINCIPLE	IMPLEMENTATION RULE
No perfect oracle	Anomaly detection triggers review; it does not declare guilt.
Cross-source consistency	Platform data, business outcomes and counterparty history reinforce each other.
Disclosure	Rewarded endorsements must be identified and cannot require false positive claims.
Appealability	Attestations preserve reversals and dispute outcomes, not only accusations.
Data minimisation	Store hashes and durable facts on-chain; keep sensitive evidence permissioned.

Digital demand becomes visible, physical opportunity.

Quest Map

Creators can discover nearby missions by location, time, category, reward and eligibility before travelling. Businesses expose operational capacity—creator slots per hour, reservation requirements, available products and venue constraints—so a successful campaign does not overwhelm the physical business.

DISCOVER

Map inventory

Visit, taste, test, attend, demonstrate, teach, interview or document.

RESERVE

Capacity-aware slots

Time windows and admission rules connect campaign demand to real operations.

EXECUTE

Local trust

Micro-creators can prove value in communities ignored by national ad buying.

Canswap Live

Official campaign media explains the mission; community-generated media demonstrates execution. The product keeps them visually and semantically separate. Every submission links to the relevant Brand Token market, Quest terms and creator's Candao profile. Video is evidence and discovery—not proof by itself. The proof record may additionally require presence, timing, disclosure and business outcome.

Demand-Backed Quests

A Quest can also begin with a crowd asking for an outcome. Users express verified interest or conditional commitments; sponsors and venues contribute; an organiser Circle demonstrates delivery capacity; only then is one professional proposal sent to the target. If declined, commitments expire under published terms.

SAFETY BOUNDARY

Demand-backed action must not become harassment, coercion, unsafe dares, illegal activity or automated pressure. The target can decline. The protocol replaces noisy uncoordinated attention with one evidence-backed, reversible proposal.

The scarce inventory is not only screen space. It is human presence, local trust, creator time and communities capable of acting.

Agents coordinate context; people retain authority.

Customer and brand Ghosts

CUSTOMER GHOST

“Make my rewards useful.”

Understands connected wallets, preferences, travel, nearby Quests and redemption goals. It reveals only the facts needed for an offer, under permission.

BRAND GHOST

“Allocate rewards where they work.”

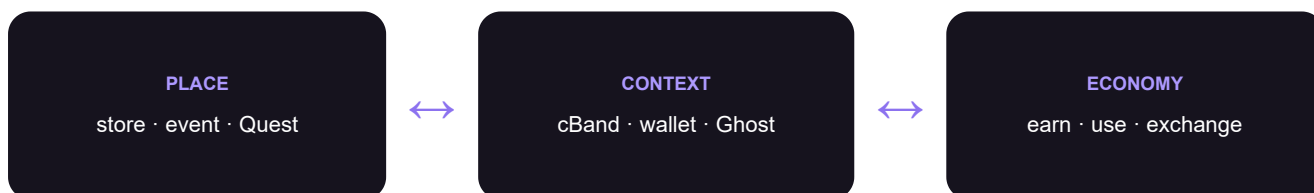
Understands campaigns, inventory, budgets, Quest capacity, redemption rules and market liquidity without receiving unrelated private memory.

Circles as temporary operating networks

A campaign can assemble creators, strategists, local operators, developers, analysts and specialised AI agents. Work is decomposed into measurable tasks; useful intermediate contributions can be rewarded instead of making the entire campaign one winner-takes-all contest. Every high-value or sensitive action remains approval-gated.

cBand and physical loyalty

NFC or proximity can establish the correct venue context, request a narrow permission and present human-readable approval: receive a purchase reward, prove membership tier, spend 120 tokens, join a Quest or review a market exchange. Gas sponsorship or account abstraction may hide chain mechanics, but the user must still understand value, fee and final effect before authorising.



Agent constraints

- No agent may sign a high-value transaction without explicit delegated authority.
- Private profile data is projected minimally, not copied wholesale to brands.
- Recommendations disclose sponsorship, economic incentives and uncertainty.
- Users can disconnect sources and revoke permissions.
- Agent coordination cannot bypass Quest eligibility, evidence or settlement rules.

The protocol is defined by what must remain impossible.

INVARIANT	ENFORCEMENT
No inflation	Non-upgradeable BrandToken exposes no post-construction mint path.
No duplicate brand	Factory and registry reject an existing canonical brandId.
No reserve theft	Only the currently verified treasury can claim, once.
No fee replay	Each settlementId is permanently marked processed.
No fee diversion	Settlement token cannot be recovered by governance.
No partial swap	Both route legs, fee deposit and final delivery share one atomic transaction.
No adapter fiction	Router measures balance deltas rather than trusting return values.
No early public buy	Block time enforces creator-only access for 24 hours, then opens autonomously.
No instant governance	Protocol administration is assigned to a Safe-controlled timelock.

Adversarial test classes

- Expired deadline and zero amount.
- Insufficient first- or second-leg output.
- Unapproved adapter.
- Adapter that lies about output.
- Reentrant adapter/token behavior.
- Fee-on-transfer input and output.
- Repeated settlement identifier.
- Unverified or wrong treasury claim.
- Reserve double claim.
- Brand-to-Brand fee split.
- Vault collateralization.
- Randomized accounting invariants.
- Known BNB Chain contract/fork state.
- Governance role and delay checks.

Residual risks

Smart-contract correctness does not remove oracle manipulation, liquidity failure, compromised governance signers, malicious frontends, RPC censorship, token-standard edge cases, bridge risk, brand identity fraud, legal restrictions or off-chain evidence manipulation. Independent audits, public source verification, bug bounty, monitoring and incident response remain mandatory before production.

Governance controls narrow roles—not user funds.

The reference policy assigns protocol administration to a 3-of-5 Safe that is the sole proposer to a 48-hour timelock. Execution becomes permissionless after the delay.

Timelocked actions

- Add or remove a settlement adapter.
- Verify a brand treasury after documented evidence review.
- Exercise emergency metadata administration.
- Change role membership.
- Recover unsupported tokens—never the settlement token—from a vault.

Outside governance reach

- Fixed token supply and allocations.
- Already deployed token contracts and historical balances.
- Fixed 5% swap fee and 0.30% LP fee calculations.
- Executed Genesis fills and permanent Genesis CDO liquidity.
- User wallet keys, limit orders and LP position ownership.

Signer separation

Five independent hardware-wallet holders across engineering, treasury, legal/compliance, security and independent Candao oversight. No shared seed, device or backup location.

Deployment ceremony

One-purpose funded deployer; verified Safe; reviewed environment; reproducible compilation; source verification; role handoff; deployer renunciation; published manifest and checksums.

Infrastructure independence

One GCP project may host a frontend, API and indexer without holding protocol custody. Decentralization requires public contracts, direct wallet execution, multiple RPCs, replaceable indexers, a static frontend mirror and published addresses. A web outage must not prevent direct claims, withdrawals or pool exits.

EMERGENCY POSTURE

The reference router has no instant administrator pause. Auditors must determine whether a narrowly scoped delay-free pause reduces risk or creates a more dangerous centralised control. Any final mechanism must be explicit, minimal and monitored.

Legal and safety design are product design.

Non-equity boundary

A Brand Token is designed for loyalty, access and participation. It does not represent company shares, ownership, voting rights in the company, debt, dividends, profit participation or a guaranteed return. Nevertheless, classification depends on actual rights, distribution, transferability, marketing and jurisdiction. A label alone cannot determine legal treatment.

Consumer clarity

- Identify whether the brand has claimed and verified the token.
- Separate redemption utility, market value and speculative value.
- Show the 5% brand fee, venue fees, gas, price impact and minimum output.
- Publish redemption, expiry, refund and programme-change rules.
- Do not imply a real partnership by displaying a catalogue brand or logo.
- Apply appropriate restrictions for minors, promotions and location-specific rules.

Quest privacy and safety

- Presence proof is opt-in and purpose-limited; continuous location history is unnecessary.
- Creator-authorised platform data is normalised and revocable.
- Private evidence is stored permissionally; public attestations contain hashes and bounded facts.
- UGC requires consent, moderation, retention and takedown processes.
- Sponsored activity requires applicable disclosure and must not demand false statements.
- Unsafe, illegal, humiliating, discriminatory or harassment-oriented missions are prohibited.

Financial and operational controls

KYC/AML, sanctions checks, tax reporting, consumer disclosures and licensing may apply at particular fiat, custody, exchange, brand-claim or reward touchpoints. The non-custodial protocol does not eliminate obligations of issuers, interfaces, brands, creators or regulated venues.

RELEASE GATE

No public launch should occur before independent contract/application audits, complete testnet E2E, backup approver registration, signer ceremony, production monitoring, failure drills and incident response.

One Brand Token identity, registered representations.

Loyalty volume may require multiple execution networks. The customer should choose the value and action they want—not manually reason about chain architecture.

LAYER	RESPONSIBILITY
Canonical identity	Brand identifier, verified issuer, supply policy, fee policy and metadata root.
Origin deployment	Reference fixed-supply contract and authoritative allocation history.
Chain representation	Explicitly registered contract/mint tied to the same identity.
Supply accounting	Lock/mint, burn/mint or canonical messaging prevents accidental duplicate supply.
Unified interface	Balances, utility and routes are presented as one Brand Token experience.

Candidate execution environments

DEFAULT

BNB Chain

Candao home, EVM tooling, CDO context and reference implementation.

EVM LIQUIDITY

Ethereum and L2s

Wallet reach, mature DEX venues and programmable settlement.

CONSUMER SCALE

Solana

Low-cost reward transactions and consumer distribution patterns.

MESSAGING

TON

Telegram-native distribution and wallet access.

PHYSICAL UX

Abstracted execution

Gas sponsorship and human-readable approvals hide plumbing, not consequences.

FUTURE

Interoperability

Only audited, supply-safe routes become registered representations.

Bridge and fragmentation risks

Cross-chain expansion is not assumed safe by default. Bridge compromise, delayed finality, replay, inconsistent decimals, duplicated metadata and liquidity fragmentation can break the “one token” promise. Each representation requires a supply invariant, recovery plan and visible chain-specific risk. Multi-chain deployment follows—not precedes—secure origin operation.

Canswap on BNB Chain.

COMPONENT	PURPOSE	STATUS
BrandToken	Non-upgradeable fixed-supply ERC-20.	BUILT + TESTED
BrandFactory	Unique creation and atomic allocation.	BUILT + TESTED
BrandRegistry	Identity, treasury, verification and metadata.	BUILT + TESTED
ReserveVault	One-time 19,950,000-unit verified brand claim.	BUILT + TESTED
GenesisMarket	Finite 0.1–199.9 CDO ladder and permanent CDO liquidity.	BUILT + TESTED
Native AMM	Canonical CDO/Brand liquidity and LP-owned 0.30% fee.	BUILT + TESTED
FeeVault	Isolated multi-asset 5% accounting and verified claims.	BUILT + TESTED
Routers + Orders	Atomic native, Brand↔Brand, adapter and EIP-712 order settlement.	BUILT + TESTED
Mainnet deployment	Audited addresses, roles and manifest.	RELEASE GATE
Liquidity/indexer	Executable quotes, candles, volume and activity.	RELEASE GATE

Verification completed in the local reference

Fixed supply and allocation, finite Genesis fills, permanent CDO accounting, AMM reserve/share invariants, exact fee accrual and post-claim split, signed-order partial fills/cancellation/replay protection, DNSSEC and P-256 email evidence, deadlines, slippage, atomicity, Brand-to-Brand fee allocation, malicious adapters, reentrancy, vault collateralization, randomized invariants and BNB fork behavior.

Mandatory production gates

1. Independent Solidity and application audits with remediation.
2. Named hardware-wallet Safe signers and deployed 3-of-5 governance.
3. Jurisdiction-specific legal and token classification.
4. Documented, funded liquidity and manipulation monitoring.
5. Production RPC failover, indexer, alerts, source verification and bug bounty.
6. Dedicated Canswap credentials, DNS/TLS, CSP, deployment manifest and static mirror.

Reference implementation

Native BNB Chain markets use CDO as the quote and Brand Fee asset. Future direct Brand/USDT, Brand/USDC or Brand/WETH authorised venues accrue the fee in that market's quote asset. The vault and interface always disclose the exact asset actually held.

Loyalty becomes an open relationship, not a trapped balance.

Brand Tokens combine a fixed, transparent supply with permissionless community formation, verified brand activation, brand-owned market economics and evidence-based participation.

The model in one sentence

A community can open an immutable market around a brand; only the verified brand can claim its reserve and fees, define official loyalty utility, and turn participation—purchases, referrals, creation, events and Quests—into a transparent token economy.

Why Quests matter

Portable exchange alone would improve the exit path for loyalty, but it would not answer how tokens are earned for meaningful behavior. Quests supply that missing layer. Businesses express demand as measurable missions. Creators and communities choose the work, submit evidence, receive settlement and build factual reputation. Maps connect opportunity to place; Live makes execution visible; Circles and Ghosts coordinate larger campaigns without removing human authority.

Why the claim boundary matters

Permissionless creation enables community initiative, but it must not counterfeit endorsement. The protocol therefore keeps two states explicit. Before claim, the token is a speculative community-created invitation with no issuer-backed benefits. After verified claim, the same immutable token may become an official loyalty instrument under published brand terms. Neither state creates equity.

Why the fee begins with the brand

The pre-claim 5% quote-asset balance is an isolated on-chain claim belonging entirely to the brand; Candao receives zero. Verification never reallocates earlier accrual. Only future qualifying fees split 2.5% to the authenticated Brand Fee wallet and 2.5% to Candao, making the economic transition explicit and non-retroactive.

Reward real behavior. Publish real utility. Let communities carry value without pretending that loyalty is ownership.

Glossary and research basis

Brand Token — immutable 21M token associated with a canonical brand domain.

Brand ID — unique registry key preventing duplicate official creation.

Claim — DNSSEC, wallet, authenticated-email and approver-bound release process.

Genesis market — finite initial million-token ask ladder whose CDO remains liquidity.

Qualifying swap — official settlement route subject to one 5% Brand Fee.

Quote asset — asset in which the market expresses price and collects Brand Fee; CDO on native markets.

Quest — measurable business mission with published terms, evidence and reward.

Proof of Quest — layered presence, time, content, performance, acceptance and settlement evidence.

Circle — team of people and agents organised around a measurable outcome.

Ghost — permissioned user or business agent coordinating relevant context.

cBand — physical/NFC experience for contextual loyalty interactions.

Authorised venue — router, hook, DEX or CEX committed to the Brand Fee policy.

Primary design inputs

1. *Candao Brand Tokens: loyalty becomes a liquid, programmable economy*, concept document supplied for this protocol design.
2. *Candao Quests: business missions that move crowds into the real world*, product concept supplied for this protocol design.
3. CanSwap Solidity v2: BrandToken, Factory, Registry, ReserveVault, GenesisLiquidityMarket, BrandLiquidityPool, native/external routers, signed orders, FeeVault and ClaimManager.
4. CanSwap protocol, governance, architecture, scalability and release-readiness specifications.
5. OpenZeppelin patterns for ERC-20, access control, safe transfers, math, reentrancy and cryptographic verification.
6. BNB Chain and optional authorised external-venue contracts used for routing and interoperability.

Document integrity

This PDF is generated from the version-controlled source `docs/brand-token-protocol-whitepaper.html`. The deployed release should publish the PDF hash beside the protocol address manifest so readers can verify that the document has not been substituted.

BRAND EXAMPLES

Any brand names or marks shown in the Canswap catalogue or product demonstrations belong to their respective owners and do not establish affiliation, endorsement, token deployment or participation.