WES

Whitepaper

WiFi Economy System

Version	1.6
Date	2026-05-12
Network	BNB Smart Chain (chain ID 56)
Token	WES — BEP-20 — 18 decimals
Total Supply	50,000,000,000 WES
Website	epscloud.io

This document is confidential and provided for informational purposes only.

Contents

1 Important Notice 2
2 Executive Summary 2
3 Why WES 2
4 Problem 3
5 The WES Solution 3
6 Vision 4
7 Ecosystem Participants 4
7.1 Venues and Hosts . . . 4
7.2 WiFi Users . . . 5
7.3 Advertisers and Agencies . . . 5
7.4 Agents and Installers . . . 5
7.5 Stakers . . . 5
7.6 Admin and BOD . . . 5
8 Why Blockchain (and the hybrid model) 6
9 Product Overview 6
9.1 Captive Portal Advertising . . . 6
9.2 Multi-Slot Ad Bundle . . . 7
9.3 Venue Registry . . . 7
9.4 Campaign Management . . . 8
9.5 Staking . . . 8
9.6 Lucky Draw . . . 8
9.7 Wallet Login and Personal Deposit Address . . . 9
10 Impression-to-Revenue Flow 9
10.1 1. Venue Onboarding . . . 9
10.2 2. Access Point Provisioning . . . 9
10.3 3. Campaign Creation . . . 10
10.4 4. Portal Delivery . . . 10
10.5 5. Impression Recording . . . 10
10.6 6. Revenue Allocation . . . 10
10.7 7. Settlement . . . 10
11 WES Token 10
11.1 Token Specification . . . 10
11.2 Supply Allocation (revised 2026-05-03) . . . 11
11.3 Public Sale Rounds . . . 11
11.4 Community Airdrop / Quest (Genesis Points) . . . 12
11.5 Angel Investor Tier Structure . . . 12
11.6 Liquidity Launch and Phase 0 Liquidity Support . . . 14
12 Token Utility 15
12.1 Public Sale Participation . . . 15
12.2 Staking and Weighted Staking Rewards . . . 15
12.3 Revenue Dashboard Access . . . 15
12.4 Venue and User Reward Accounting . . . 15
12.5 Campaign Budget Settlement . . . 16

12.6 Claimable Rewards and Withdrawals . . . 16
12.7 Lucky Draw Participation . . . 16
12.8 Treasury Allocation and Ecosystem Incentives . . . 16
12.9 Buyback and Burn Flows . . . 17
13 Revenue Model 17
13.1 Revenue Split . . . 17
13.2 User Rewards (15%): Anonymous MAC Accrual . . . 18
13.3 Buyback & Burn (10%): Phased Triggers . . . 19
13.4 Marketing (8%): Three-Way Split . . . 19
13.5 Withdrawals . . . 20
14 Trust, Integrity & Compliance 21
14.1 Impression Integrity . . . 21
14.2 Ad Fraud Posture . . . 21
14.3 Privacy and Data Policy . . . 22
14.4 Transparency Metrics . . . 23
14.5 Compliance Posture . . . 23
15 Technical Architecture 25
15.1 Hybrid Service Model . . . 25
15.2 Resilience Posture . . . 25
15.3 Gas Efficiency . . . 25
16 Security Model 26
16.1 Wallet Authentication . . . 26
16.2 Role-Based Access Control . . . 26
16.3 Treasury Safety . . . 27
16.4 On-Chain Verification . . . 27
16.5 Smart Contract Hardening . . . 27
17 Governance and Operations 27
18 Roadmap 27
18.1 Phase 1: Core Infrastructure . . . 27
18.2 Phase 2: Public Sale and Staking . . . 28
18.3 Phase 3: Venue and Campaign Expansion . . . 28
18.4 Phase 4: Revenue Settlement and Growth Loops . . . 28
18.5 Phase 5: Ecosystem Maturity . . . 29
19 Risks 29
19.1 Market Risk . . . 29
19.2 Revenue Risk . . . 29
19.3 Smart Contract Risk . . . 29
19.4 Operational Risk . . . 29
19.5 Regulatory Risk . . . 30
19.6 Ad Fraud Risk . . . 30
19.7 Privacy Enforcement Risk . . . 30
19.8 Key Compromise and Operational Security Risk . . . 30
20 Conclusion 30
Appendix A Contracts and Audit Status 31

1. Important Notice

This document describes the WES ecosystem, its token design, technical architecture, and intended economic model. It is not financial advice, a securities offering, or a promise of profit. Participation in WES involves technical, market, regulatory, smart-contract, and operational risks. Users should perform their own due diligence and comply with the laws that apply in their jurisdiction.

2. Executive Summary

WES turns venue WiFi logins into measurable local ad impressions, and shares the resulting revenue across the people who make those impressions possible.

When a user connects to participating venue WiFi, the captive portal delivers a targeted ad. The completed impression becomes a billable event with full attribution to the venue, access point, device, and campaign. Revenue accrues continuously and settles transparently across eight buckets: the venue earns 36%, users earn 15%, stakers earn 15%, buyback and burn consume 10%, and the remainder funds hardware, marketing, development, and charity.

Three things make WES distinctive:

- **Venue-level local targeting.** Advertisers can target real cafes, gyms, hotels, and retail by category, city, and brand — not opaque ad-network surfaces.
- **Anonymous reward accrual.** WiFi users earn from the first impression. There is no signup and no wallet install at the venue; wallet binding happens later, on the user's own time, through an explicit user-initiated device-to-wallet binding flow that can recover eligible reward history across MAC randomization, subject to consent and anti-abuse limits.
- **Transparent settlement.** The revenue split is enforced by published rules and on-chain accounting, with treasury movement gated by a 2-of-3 multisig and visible end-to-end on a public ledger.

A simple end-to-end view:

```
Venue WiFi → Captive ad → Connect → Impression → Revenue split →
Claim or settle
```

The WES token is the unit of denomination for revenue, rewards, staking, and settlement. The blockchain handles ownership, claims, vesting, and treasury authority; high-volume ad accounting runs off-chain for speed and gas efficiency. Token specification, contract addresses, and technical architecture follow in later sections and the appendices.

3. Why WES

WES is not just another ad token. It reshapes the value flow between the three parties who actually make WiFi advertising work — venues, end users, and advertisers — and adds a public on-chain settlement layer on top.

Dimension	Traditional WiFi	Web2 Ad Network	WES
Venue role	Gives WiFi away for free	Pass-through traffic only	Shares ad revenue per impression
User role	Gets nothing	Tracked silently by platform	May claim WES retroactively, opt-in
Advertiser inventory	Doesn't exist	Opaque, platform-priced	Venue-level attributed inventory
Attribution layer	N/A	Weak / cross-site cookies	AP-attributed on-chain settlement
Accounting	None	Closed platform ledger	Public, on-chain settlement records

The summary. Traditional WiFi captures none of the advertising value it makes possible. Web2 ad networks capture most of it and leave both the venue and the user with nothing. WES is designed to pay the parties who carry the cost (the venue's connectivity, the user's attention) directly, and to do so on a settlement layer that anyone can audit.

4. Problem

Local venues often provide free WiFi but receive little or no direct revenue from the attention they generate. Advertisers want real local exposure, but traditional ad networks often lack venue-level targeting, transparent impression accounting, and a clean path for venue participation. Users are frequently asked to watch or interact with ads without receiving a meaningful share of the value they help create.

At the same time, many Web3 reward systems are detached from real-world usage. Token emissions may be distributed without a durable economic source behind them, creating inflation without demand.

WES addresses these gaps by tying token utility to a real operating loop — venue WiFi creates impressions, impressions create revenue, revenue is allocated to participants according to a transparent split. The full impression-to-revenue walkthrough is in Section 10.

5. The WES Solution

WES turns the problem above into a measurable operating loop. The solution is built around the WiFi captive portal as the canonical ad surface, with on-chain settlement bolted on where it earns its keep.

1. A WiFi ad network built around the captive portal. When users connect to participating venue WiFi, the captive portal becomes a measurable ad surface. Slot A is a mandatory short pre-authorization video; Slot B is an optional dwell-time spot after authorization. The portal renders branded creative, records the impression, and authorizes the user's session — all in a single short flow.

2. Venue-level local targeting. Every access point is bound to one venue in the WES location registry, with category (cafe, restaurant, hotel, retail, gym, mall, salon, bar, office), city,

country, and brand metadata. Advertisers target by these attributes — not by anonymous IP ranges or opaque ad-network surfaces.

3. A transparent revenue split. Every billable impression flows into an off-chain ledger and is split across eight buckets at the close of each hourly epoch: Venue 36%, Staking 15%, User Rewards 15%, Buyback & Burn 10%, Hardware 8%, Marketing 8%, Development 5%, Charity 3%. The split is enforced by code, not by negotiation.

4. Reward accrual without wallet friction. WiFi users earn from the first impression. The system records rewards against an anonymous device record and binds the wallet later, when the user is ready. There is no signup, no wallet install at the venue, no chargeback risk to the user's session.

5. On-chain settlement where it matters. Token ownership, staking, vesting, claims, and treasury authority live on BNB Smart Chain. Treasury movement requires 2-of-3 multisig approval from independent signers who are separated from web-app admin identities — a compromise of one surface cannot drain the other.

The result is a WiFi ad network with on-chain financial discipline. Venues monetize attention; advertisers buy real local reach; users earn for their attention; stakers participate in protocol activity incentives according to published rules.

6. Vision

WES aims to become a decentralized WiFi advertising economy where every meaningful participant in the ad loop can share in the upside.

The long-term vision is a network where venues become micro-media assets, users are rewarded for attention, advertisers buy measurable local reach, and treasury flows are visible and governed through multisig-controlled Web3 infrastructure.

7. Ecosystem Participants

7.1 Venues and Hosts

Venues provide the physical location and WiFi access point. They may be cafes, restaurants, hotels, retail stores, gyms, malls, offices, salons, bars, or other public-facing places. A venue earns a proportional share of the venue revenue pool based on eligible impressions generated by its access point.

Onboarding economics. WES uses a three-tier onboarding model matched to the venue's existing infrastructure:

- **Premium / high-traffic venues** (airports, large transit hubs, shopping centres, premium hotels): WES funds the access-point hardware as a CAPEX investment, because the impression volume per device justifies the up-front cost.
- **Small venues with existing WiFi** (independent cafes, restaurants, salons): the venue already operates its own router / access point. WES funds an additional WES-managed access point so the venue keeps its existing connectivity unchanged and the WES surface is fully isolated and updatable.
- **Large existing chains** (regional cafe chains, hotel groups, retail chains): WES partners with the chain's existing managed-WiFi stack. No new hardware investment from WES; the partnership runs through standard managed-WiFi integration paths and a commercial

agreement.

Setup. A WES access point typically takes under 30 minutes per location. The installer plugs the device into an existing upstream cable, and the device self-adopts to the WES management cloud automatically. No on-site technical configuration is required beyond the physical plug-in step.

Payout cadence. Venue revenue accrues in an off-chain ledger on each hourly epoch close. Accrued balances are claimable on demand by the venue's registered wallet via the dashboard. A minimum payout threshold prevents dust withdrawals from consuming disproportionate gas; the threshold and exact cadence are configured at the system level and published in the venue onboarding guide.

Resilience. If a venue's upstream internet connection is unavailable, the access point cannot deliver impressions and therefore cannot accrue venue revenue for that period. WES does not bill the venue for outage time and does not credit the venue for time when the device cannot reach the WES management surface.

7.2 WiFi Users

Users connect to participating venue WiFi and interact with campaign content. The system can credit user reward balances for eligible ad engagement. Users may also participate in staking, lucky draw, and other ecosystem activities.

7.3 Advertisers and Agencies

Advertisers and agencies create campaigns, upload creatives, define targeting, and fund budgets. Campaign targeting can use venue categories, brands, geography, and other metadata maintained in the WES location registry.

7.4 Agents and Installers

Agents and installers help onboard venues, provision access points, and maintain the venue network. Their roles are permissioned and governed through the WES RBAC system.

7.5 Stakers

Stakers lock WES in the staking contract and receive a weighted share of the protocol's activity-incentive pool allocated to staking participants. Incentives scale with actual ecosystem activity and are not a fixed-yield guarantee.

7.6 Admin and BOD

Admin and Board of Directors ("BOD") roles handle approvals, governance operations, treasury allocation workflows, and high-level oversight. Their authority is controlled through hierarchy levels and backend permission checks. Throughout this paper, "BOD" refers to the protocol's operational approval council and does not necessarily imply statutory board authority unless separately documented by the operating entity.

8. Why Blockchain (and the hybrid model)

WES uses blockchain for the parts where blockchain pays for itself, and off-chain infrastructure for everything else. The boundary is deliberate.

On-chain (BNB Smart Chain). Token ownership, transfer, staking, vesting, claim distribution, treasury holdings, and burn operations. These need finality, auditability, and resistance to operator override. They also occur infrequently enough that gas cost is manageable.

Off-chain. Ad serving, captive portal authorization, impression recording, revenue split computation, reward accrual, dashboards, fraud detection, and operational workflows. These need millisecond latency, hour-by-hour throughput, and the ability to evolve quickly. Putting every impression on chain would multiply gas cost by orders of magnitude while delivering no meaningful integrity benefit beyond a good database.

Why this split is honest. The protocol does not pretend off-chain state is trustless. It is trust-minimized by being publicly accountable: every off-chain credit becomes an on-chain transaction at claim time, and any divergence between the off-chain ledger and on-chain balance becomes visible the moment a user claims. Treasury balances are checkable from any synced BSC node. Burn batches are verifiable on-chain. Vesting releases are governed by immutable contracts.

The blockchain provides four things the application layer cannot:

- **Settlement finality** for token movements (claims, withdrawals, vesting).
- **A shared ledger** for revenue allocation that any participant can audit.
- **Multisig treasury controls** that no single operator can override.
- **A portable identity primitive** (the wallet) that lets users carry balance and history across surfaces.

Everything that benefits from finality, shared visibility, or multisig discipline runs on chain. Everything that benefits from speed, throughput, or rapid iteration runs off chain.

9. Product Overview

9.1 Captive Portal Advertising

When a user connects to a participating WiFi network, the portal selects an eligible campaign using venue and location targeting rules. The campaign is shown to the user, and the completed impression is recorded for revenue accounting.

The captive flow is the critical user-facing surface of the protocol: the entire revenue model depends on the popup rendering, the ad playing, and the authorization completing cleanly. WES treats this surface as inviolable infrastructure, optimizes it end-to-end, and keeps the user experience aligned with native operating-system captive-portal behavior rather than working against it.

Every authorization and every impression is fully attributable to one venue, one access point, and one client device. There is no shared global captive state and no anonymous-aggregate accounting; every billable event carries the venue, AP, and device tuple it originated from.

9.2 Multi-Slot Ad Bundle

A single campaign can deliver up to two ad slots in one captive session. This allows advertisers to combine a guaranteed short-form view (Slot A) with an optional dwell-time deep-engagement spot (Slot B), and pricing is additive on top of the base CPM:

Slot	Placement	Format	Required	Duration	CPM weight
A — Pre-auth video	Inside the captive popup, before "Connect"	MP4 H.264, up to 50 MB	Yes	5 seconds mandatory	1.0×
B — Post-auth dwell	Full-screen after "Connect", before captive popup auto-dismisses	MP4 H.264, up to 50 MB	Optional	5–20 seconds, skippable from 5s	0.5×

Slot B uses a graduated charge ladder so that advertisers pay proportional to the attention actually captured:

User dwell time	Charge as % of Slot B CPM
Under 5 seconds (pre-skippable)	0%
5–9 seconds	50%
10–14 seconds	75%
15–20 seconds	100%
User-cancelled	0% (override)

The captive session is held open until Slot B reaches a terminal state (complete, skip, or cancel) so the impression is fully attributable, with a short safety release for accidental disconnects.

CPM weights are runtime-editable governance parameters — Admin or BOD can adjust the Slot A and Slot B CPM weights with a full audit trail. Existing campaigns are frozen at quote-time pricing; weight changes apply only to new campaigns.

9.3 Venue Registry

The venue registry is the canonical operational table for real-world locations. It stores owner, manager, referrer, category, brand, address, city, country, access-point provisioning state, active campaign data, and status.

Coordinates are derived server-side from address data. The client cannot submit arbitrary latitude or longitude values. This protects targeting integrity and prevents location spoofing.

9.4 Campaign Management

Campaigns are created by agencies or authorized advertisers. The campaign workflow supports:

- Budget and schedule setup.
- Venue category and city targeting.
- Brand/category targeting.
- Reach estimation.
- Creative upload.
- AI-assisted moderation followed by human approval when required.
- Campaign suspend and resume controls for Admin and BOD.

Creative media uses a hot-cold storage model. Active creatives live on edge object storage for high availability. Completed or rejected campaign assets can be archived to replicated storage to reduce long-term storage cost.

9.5 Staking

The WES staking contract supports multiple lock durations and reward weights:

Tier	Lock	Weight
Flexible	None	45
6-Month	180 days	75
9-Month	270 days	90
12-Month	360 days	120

The minimum stake is 10,000 WES. Reward weights define a participant's relative share of the protocol's activity-incentive pool for an accrual epoch. They are not a fixed APY, and the size of the pool itself depends on actual measured protocol activity for that epoch (impressions delivered, captive sessions completed, campaign budgets recognised).

Nature of staking incentives. Staked WES functions as a participation lock that gates access to incentive distributions denominated in WES from a protocol-managed activity-incentive pool. The size of this pool varies with measured platform activity for the epoch in question; if no activity is measured, the pool can be zero.

Disclaimer. Staking incentives are protocol-driven participation rewards distributed in WES according to published rules. They **do not represent equity, debt, dividends, ownership rights, profit-sharing, a claim on company revenue, or any guaranteed distribution**. Distribution size, timing, and availability depend on actual protocol activity, legal constraints, treasury policy, and smart-contract conditions; distributions may vary, be delayed, or be unavailable. Holding or staking WES does not confer any right to require a distribution.

9.6 Lucky Draw

The Lucky Draw mechanism is designed as a community engagement surface funded from the marketing allocation path. Unallocated referral amounts and configured marketing skims can flow into the draw pool according to system settings.

Compliance posture. Because the prize pool is denominated in WES, the program is treated as a regulated promotional sweepstakes rather than a wagering or gambling product. Operational details below will be finalised in a separate Lucky Draw Terms & Conditions document published prior to the first draw and reviewed by counsel:

- **Eligibility:** entry is automatic for users who complete an ad impression at a participating venue while connected to the WES WiFi network. There is no entry fee, no token purchase, and no staking requirement to enter or to claim.
- **No purchase necessary.** A free alternate method of entry (AMOE) will be made available where required by local law.
- **Jurisdiction exclusions.** Entry and prize claims are void where prohibited by local law. WES will maintain and publish a list of excluded jurisdictions; residents of those jurisdictions will be blocked from claiming prizes regardless of impression activity.
- **Randomness method.** Winner selection uses a verifiable, reproducible random-draw mechanism over the impression record set for the draw period. The method, seed source, and audit log are published with each draw.
- **Prize claim terms:** prizes are claimed from the user's rewards page within a published claim window (e.g. 30 days). Prizes unclaimed after the window expire back into the draw pool or are burned per documented policy.
- **Compliance review:** the full Lucky Draw rule set is reviewed by counsel against the sweepstakes/promotion rules of each target jurisdiction before each phase change. Material changes are re-disclosed before they take effect.

9.7 Wallet Login and Personal Deposit Address

WES uses wallet-based authentication — no passwords, no email signups. A user connects a wallet, signs a nonce-based message, and receives a session. Each account is also provisioned with its own deterministic BSC deposit address so funds can be sent from any external wallet without manual transaction-hash submission. Detection, sweep-to-Treasury, and off-chain crediting are fully automated and idempotent.

The watcher pipeline, dedup layers, sweep policy, and reconciliation cadence are implementation details deliberately kept out of this public document.

10. Impression-to-Revenue Flow

WES is built around a measurable operating loop. The goal is not to distribute tokens arbitrarily, but to connect token accounting to actual user attention and venue traffic.

10.1 1. Venue Onboarding

A venue is registered in the WES location registry. The venue record includes ownership, address, category, brand, manager, referrer, and provisioning state. Once approved and provisioned, the venue can host WES-compatible WiFi access.

10.2 2. Access Point Provisioning

The WES provisioning layer creates or configures the required WiFi site and SSID settings. Adopted access points are linked back to venue records so impressions can be attributed to the correct venue owner.

10.3 3. Campaign Creation

An agency or advertiser creates a campaign, defines budget, schedule, creative assets, and targeting rules. The campaign may be reviewed by AI-assisted moderation and, when needed, human reviewers.

10.4 4. Portal Delivery

When a user connects to venue WiFi, the captive portal requests an eligible campaign. The ad-serving engine checks active campaigns against venue category, city, brand, and other targeting constraints.

10.5 5. Impression Recording

When the user completes the required interaction, the system records the impression. This event becomes the basic unit for revenue attribution.

10.6 6. Revenue Allocation

Revenue is allocated across the WES split. Venue, user, staking, referral, buyback, hardware, marketing, development, and charity buckets are computed off-chain and written to durable ledgers.

10.7 7. Settlement

Balances can later be claimed, withdrawn, distributed to staking participants, or routed through treasury-controlled flows. WES uses on-chain settlement where finality and ownership are required, while keeping high-frequency accounting off-chain.

```
Venue WiFi -> Captive Portal -> Targeted Campaign -> Impression
    -> Revenue Ledger -> Bucket Allocation -> Claim / Stake / Treasury Settlement
```

11. WES Token

11.1 Token Specification

Field	Value
Token name	WiFi Economy System
Symbol	WES
Standard	BEP-20
Network	BNB Smart Chain
Chain ID	56
Decimals	18
Total supply	50,000,000,000 WES

11.2 Supply Allocation (revised 2026-05-03)

The public-side bucket of 39B WES is split into five strategic sub-allocations rather than sold entirely as direct public sale. This reduces sell pressure, preserves supply for ecosystem growth and liquidity, and funds an activity-based airdrop program.

Allocation	Amount	Percent	Destination
Public Sale	21,000,000,000 WES	42.0%	Treasury Safe / sale allocation
Ecosystem Growth Reserve	9,250,000,000 WES	18.5%	Venue/agency incentives, strategic partners
Liquidity / Market Making	5,000,000,000 WES	10.0%	DEX/CEX liquidity, market depth
Community Airdrop / Quest	750,000,000 WES	1.5%	Activity-based rewards (anti-sybil)
Future Treasury Buffer	3,000,000,000 WES	6.0%	Operations, expansion, grants, contingency
Angel Investors	5,000,000,000 WES	10.0%	TokenVestingAngels Tier 1/2/3 (see Section 11.5)
Team / BOD	3,000,000,000 WES	6.0%	TokenVestingTeam
Hardware / Ops	3,000,000,000 WES	6.0%	TokenVestingHardware
Total	50,000,000,000 WES	100%	

11.3 Public Sale Rounds

The 21B public sale allocation is distributed across three phased rounds (Strategy γ). R1 activates by an irreversible single-click admin action when the product is ready; R2 and R3 then auto-transition automatically when the previous round's window closes. Unsold supply from a closing round carries over to the next.

Round	Supply	Price USD/WES	Raise	Per-wallet max	Duration
R1	7,000,000,000 WES	$0.0010	$7.0M	$100,000	90 days
R2	7,000,000,000 WES	$0.0015	$10.5M	$250,000	60 days
R3	7,000,000,000 WES	$0.0018	$12.6M	$500,000	30 days
Total	21,000,000,000 WES		$30.1M		180 days

Round-to-round price step is intentionally compressed (R3/R1 = 1.8×) to keep the sale

curve fair for participants who enter early without producing the steep climb that creates secondary-market mispricing. Per-wallet caps escalate per round so early rounds remain accessible to broad retail participation while later rounds accommodate strategic buyers and liquidity partners. Minimum contribution is $10 USD across all rounds.

The sale interface supports USDT and BNB payment paths. Each contribution records both the payment currency and the USD-equivalent value, and on-chain transactions on BNB Smart Chain are verified at three or more confirmations before the contribution is finalized. Per-wallet caps are enforced symmetrically across both currencies, summed in USD-equivalent value per wallet per round.

11.4 Community Airdrop / Quest (Genesis Points)

The 750M airdrop pool (1.5% of total supply) is distributed activity-based across one Season 0 (250M) plus ten monthly cycles in Year 1 (50M each). Wallet login alone earns XP/points only — liquid WES is unlocked only by verified real activity (WiFi sessions at participating venues, completed ad impressions, WES staking, venue onboarding with adopted AP, agency campaign creation, real referrals).

Distribution uses **weighted bucket** allocation (WiFi Users 33.3%, Venue Owners 26.7%, Stakers 20%, Referrals 13.3%, Quests 6.7%) so that low-quality actions cannot drain the pool earmarked for higher-quality signals. Per-tranche claim splits 25% immediately + 75% over 6 monthly tranches with **activity gating**: each monthly tranche releases only if the wallet had at least 1 qualifying action in the prior 30 days. Pending tranches remain eligible until M6 + 90 days, then route to the Lucky Draw pool.

Anti-sybil enforcement runs in two phases. Phase 1 (launch): per-wallet hard cap, hashed device fingerprint as a risk signal, captive-portal session evidence tied to a real venue access point as canonical proof of activity, and edge-layer rate limiting. Phase 2 (post-baseline): funding-pattern detection and behavior-similarity scoring.

The official program messaging across landing page, partnership decks, social media, and FAQ uses verbatim:

> WES Genesis Points — Season 0. Earn verified-activity points before R1. After R1 closes, WES will run an anti-sybil review and open the first airdrop claim for eligible users, venues, stakers, and referrers. Token distribution is subject to review and is not a guaranteed allocation.

11.5 Angel Investor Tier Structure

The 5B WES Angel allocation (10% of supply) is structured across three tiers with progressively deeper entry discounts and longer vesting periods. Angel commitments are off-chain agreements finalized before public R1 opens; on-chain release is governed by `TokenVestingAngelsTier1/2/3` contracts, immutable post-deploy.

Tier matrix:

Tier	Allocation	Entry	Raise	Vesting	Commit cap
Tier 1 — Light	2.5B WES	$0.0008	$2.00M	6m cliff (20%) + 6m linear	$50K–$200K
Tier 2 — Standard	2.0B WES	$0.0005	$1.00M	6m cliff (25%) + 9m linear	$100K–$500K

Tier	Allocation	Entry	Raise	Vesting	Commit cap
Tier 3 — VIP slot	0.5B WES	$0.0003	$0.15M	6m cliff (30%) + 12m linear	$10K–$30K
Total	5.0B WES	—	$3.15M	—	—

Vesting mechanics.

- **Vesting start:** Day 0 (Token Generation Event, coinciding with R1 public sale open).
- **Cliff:** all three tiers have a 6-month cliff (Day 180), at which a tier-specific percentage of each angel's allocation unlocks atomically — Tier 1: 20%, Tier 2: 25%, Tier 3: 30%. Higher tiers receive a larger up-front release recognising deeper entry discounts and longer aggregate commitment.
- **Linear release:** the remaining balance releases linearly over the post-cliff window — Tier 1 over 6 months (full vest Day 360), Tier 2 over 9 months (full vest Day 450), Tier 3 over 12 months (full vest Day 540). Total vesting durations: 12 / 15 / 18 months for Tier 1 / 2 / 3.
- **Day 181 alignment:** the cliff is positioned 1 day before pool launch (Day 181), so angels have a meaningful liquid position the moment PCS V3 liquidity goes live — approximately $2.07M USDT-equivalent of WES across all tiers becomes claimable.

Anti-concentration rules.

- No single angel may commit more than 20% of any single tier.
- No single angel may commit more than 10% of total angel allocation (500M WES maximum across all tiers per investor).
- Tier 3 is a scarce-slot VIP early-bird allocation with the deepest per-WES discount of the angel programme. The narrow cheque band ($10K–$30K) and small total pool (0.5B WES, $0.15M max raise) cap individual exposure and incentivise speed-to-commit over cheque size. Tier 3 is positioned as a community/advisor reward rather than a primary capital-raising vehicle.

Use of angel proceeds. The $3.15M raised goes to the Treasury Safe (`0xa79edf5f23a1358e652a9fd19` and funds pre-launch infrastructure, operating expenses through R1, initial ecosystem incentives, and contingency reserve. Angel raise is separate from public sale proceeds ($30.1M); the two pools serve different operational windows.

Lazy funding pattern. Angel allocations are NOT pre-deposited into the vesting contracts at deployment. The 5B WES Angel allocation remains in Treasury Safe custody until specific angel commitments are signed. For each angel commitment, the Treasury Safe executes a single 2-of-3 transaction that atomically (a) transfers that angel's WES allocation from Treasury into the appropriate tier contract and (b) registers the angel as a beneficiary via `addBeneficiary()`. This pattern ensures the vesting contract balance always equals the sum of registered beneficiary allocations — no unallocated WES is ever locked in vesting custody.

Implementation readiness (as of 2026-05-12). The 5B Angel pool is held in the Treasury Safe and ready for lazy distribution under the pattern above. The Tier 1/2/3 vesting contracts have been audited internally (static analysis + comprehensive unit-test coverage) and verified end-to-end on BSC testnet through a compressed-time live claim cycle (deploy → addBeneficiary → `startTGE` → post-cliff `claim()` → post-linear `claim()` → full beneficiary draw). Mainnet deployment is deferred until the first angel commitment is finalised, at which point the three contracts are deployed and the funding transaction is executed in

the same operational batch.

Under-subscription handling. If angel commitments do not fill the 5B allocation cap, the unsubscribed portion remains in Treasury Safe custody. The Treasury Safe may redirect the unsubscribed portion (with public disclosure of the disposition) to one or more of the following: public sale supply extension, Ecosystem Growth Reserve top-up, liquidity pool seed augmentation, strategic partnership reserves, or burn for deflationary supply reduction. No automatic default disposition is hard-coded; each redirection requires a specific 2-of-3 Safe transaction and is disclosed publicly.

11.6 Liquidity Launch and Phase 0 Liquidity Support

PCS V3 liquidity pools are deployed on Day 181 — the day after R3 closes. There is no DEX liquidity during the 180-day public sale window; the official sale is the sole price source until R3 ends.

Pool configuration:

- **WES/USDT pool** — $500K USDT + approximately 277,777,778 WES seeded at $0.0018/WES initial price, aligned with the closing R3 public sale price.
- **WES/BNB pool** — $500K BNB-equivalent + approximately 277,777,778 WES seeded at the equivalent $0.0018/WES initial price.
- **Fee tier:** 0.25% (industry-standard for utility tokens on BSC).
- **Total Day 0 liquidity:** $1M USD-equivalent across both pools, sourced from the 5B Liquidity / Market Making allocation.
- **Approximate WES used for initial liquidity:** 555,555,556 WES, leaving the remainder of the liquidity allocation available for volume-based liquidity ramps, CEX liquidity, market-making reserves, and future ecosystem liquidity needs.

Volume-gated liquidity ramps:

- **Day 7 (Day 188):** if 24h trading volume $\geq$ $200K, Treasury may add up to $500K USD-equivalent of additional paired liquidity at the prevailing pool ratio.
- **Day 14 (Day 195):** if 24h trading volume $\geq$ $500K, Treasury may add up to $1M USD-equivalent of additional paired liquidity at the prevailing pool ratio.
- Ramps are skipped if volume gates are not met. Liquidity scales with demonstrated demand, not on a fixed timeline. Pairing the WES side to the prevailing pool ratio (rather than a fixed price) keeps post-launch ramps fair to whatever market price has emerged.

Phase 0 Liquidity Support (30-day window). From Day 181 to Day 210, the Treasury may conduct protocol-owned liquidity operations during the initial post-launch period to support orderly market formation. These operations are discretionary, capped, publicly reportable, and **do not guarantee any token price, trading volume, liquidity depth, or recovery level**.

- **Operational budget:** $3.0M USDT/BNB, carved from accumulated public sale proceeds (~10% of $30.1M raised).
- **Activation:** operations are engaged at the Treasury's sole discretion. Trigger thresholds, sizing, pacing, circuit breakers, and other operational parameters are governed by an internal Treasury policy and are not published, in order to mitigate predictable-attack vectors against the budget.
- **Treatment of acquired WES:** a portion of WES acquired through these operations is held in Treasury Safe for future liquidity ramps and operational reserves; a portion is burned via the token's burn function, reducing circulating supply. The exact split is set by internal

policy and reported in aggregate.

- **Transparency:** on-chain activity from the Treasury Safe is publicly visible on BSCScan. Aggregate operational activity is reported in public dashboards. The operational principle and total budget cap are pre-disclosed in this whitepaper.

After Day 210, the Phase 0 liquidity-support window closes and the standard revenue-driven Buyback & Burn mechanism (see Section 13.3, 10% revenue bucket) takes over as the primary supply-reduction force. By Day 210, the first 30 days of post-launch impression revenue have begun to flow into the burn bucket, providing organic deflationary pressure.

Day 181 context. Day 181 is a notable convergence point: public sale buyers receive immediate transferability, angel cliff unlocks a tier-specific share of each allocation, and the pool opens. The liquidity-support program is one of several tools available to the Treasury during this window; it is not a guarantee of price, volume, or recovery outcome.

12. Token Utility

WES is the utility and settlement token of the WiFi Economy System. Every economic surface in the protocol — venue revenue, user rewards, staking, advertiser spend, governance allocation, and supply contraction — denominates value in WES, and the token serves as the unit through which on-chain finality is reached for those flows.

12.1 Public Sale Participation

WES is offered through three phased rounds (Strategy γ — see "Public Sale Rounds" above) at fixed USD-denominated prices. Buyers purchase WES with USDT or BNB; backend verification confirms each on-chain transaction at three confirmations before the contribution is recorded. WES purchased in the sale is delivered to the buyer's wallet immediately and is freely transferable.

12.2 Staking and Weighted Staking Rewards

Holders may lock WES in the staking contract across four tiers (Flexible, 6-month, 9-month, 12-month) with reward weights of 45 / 75 / 90 / 120 respectively. The 15% protocol activity-incentive bucket allocated to staking participants is distributed according to stake size, tier weight, and time in stake. Incentives are not a fixed APY — they scale with actual ecosystem activity and reflect both the size and the duration of the staker's commitment.

12.3 Revenue Dashboard Access

Visibility into protocol-level revenue and earnings dashboards is gated by an active stake. Any user with at least one unclaimed staking deposit unlocks the revenue, earnings, and analytics surfaces. The gate evaluates leniently — a stake that has matured but not yet been claimed still counts — so users who participate in staking retain access until they actively withdraw. Admin and BOD bypass the gate by role.

12.4 Venue and User Reward Accounting

Eligible impressions credit venue owners (36% of revenue, proportional to AP-attributed impressions) and end-user MAC accruals (15%). Both flows accumulate off-chain in a transac-

tional ledger with full audit trails, and settle on-chain when the holder claims. The off-chain ledger is the source of truth between epochs; the on-chain transfer is the finality.

12.5 Campaign Budget Settlement

Advertisers and agencies fund campaigns by depositing WES that locks at quote time. The quote rate is sourced at the moment of campaign creation via a tiered fallback:

1. PCS V3 5-minute TWAP post-pool-launch (Day 181+).
2. Active sale tier price during R1–R3 (campaigns created Day 0–89 quote at $0.001/WES, Day 90–149 at $0.0015, Day 150–179 at $0.0018).
3. Last closed sale tier price as transient fallback (used when both TWAP and active-tier sources are unavailable).

Once a campaign is created, the rate is frozen for its lifetime — round transitions, pool launch, or top-up deposits do not re-quote existing campaigns. Holding WES purchased in earlier rounds does not lock historical rates: the rate that applies is the rate at the moment of `POST /campaigns/quote`, not the moment of WES purchase.

Pricing is denominated in USDT (so agencies can budget in fiat-equivalent terms) but settled in WES at the locked rate, isolating the treasury from intra-campaign FX risk. Per-impression accounting deducts from the locked balance at the frozen rate. When the locked WES balance reaches zero, the campaign auto-suspends; the agency may deposit additional WES at the then-current rate to resume delivery. Top-up deposits create new tranches inside the campaign and deduct first-in-first-out (FIFO) order. Campaigns do not have a hard expiry — they run as long as the agency keeps the campaign active and the locked balance remains positive. Unspent WES on campaign completion refunds to the agency's available balance.

12.6 Claimable Rewards and Withdrawals

Off-chain reward balances (venue, user, and referral rewards) become on-chain WES via a claim or withdrawal action. Claims for venue and referral rewards build a Treasury Safe transfer that is signed 2-of-3 by the protocol signers and broadcast on chain. User withdrawals follow the same path with admin approval gating and an automated stuck-batch alerting system (see "Withdrawals" below). The minimum withdrawal is denominated in USDT-equivalent value, ensuring withdrawal economics remain stable across WES price movement.

12.7 Lucky Draw Participation

Lucky Draw rounds run as a periodic engagement surface funded from the marketing residual (phase-dependent — see Marketing 8% split). Eligible participants are determined by recent ecosystem activity, and prize pools are settled on-chain to winner wallets via the Treasury Safe. The mechanism is designed to redistribute marketing budget to active users in growth phases, not as a primary token-acquisition channel.

12.8 Treasury Allocation and Ecosystem Incentives

The 18.5% Ecosystem Growth Reserve and 6% Treasury Buffer are managed through the Treasury Safe with 2-of-3 multisig discipline. Allocations to strategic partners, venue grants, exchange listings, and ecosystem development require signer approval; every disbursement appears on the public Safe ledger.

12.9 Buyback and Burn Flows

The 10% Buyback & Burn bucket accumulates per-impression in USDT-equivalent value and is executed in phased batches (5K / 30K / 50K USDT thresholds — see Revenue Model). Each batch performs an open-market WES buy on PancakeSwap, then permanently removes the purchased WES from circulating supply through the token's burn mechanism. The cycle ties on-chain demand to real off-chain revenue, providing a measurable deflationary counter-weight to circulating-supply growth as vesting unlocks proceed.

13. Revenue Model

WES revenue originates from campaign spend and ad impressions. The system records impressions off-chain, calculates revenue allocation in a durable database, and performs on-chain writes only when needed. This design is intentional: on-chain settlement is used for finality, while high-frequency accounting remains gas-efficient and auditable off-chain.

Revenue is closed into fixed UTC hour epochs. Each closed window is distributed atomically across all buckets — the entire split is committed as a single transaction, so a transient infrastructure failure cannot leave partial credits or double-credit on retry.

13.1 Revenue Split

The canonical revenue split is:

Bucket	Percent	Settlement path
Venue / Host	36%	Off-chain accrual to AP owner, on-chain claim
Staking	15%	On-chain activity-incentive distribution to staking participants
User Rewards	15%	Off-chain anonymous accrual, claimed after wallet bind
Buyback & Burn	10%	On-chain burn from Treasury Safe (phased trigger)
Hardware / Infra	8%	On-chain transfer to Hardware Safe
Marketing	8%	Split between Tiered Referral Program (5% fixed) + Lucky Draw + direct marketing (phased)
Development	5%	On-chain transfer to Development wallet

Bucket	Percent	Settlement path
Charity	3%	On-chain transfer to Charity wallet
Total	100%	

13.2 User Rewards (15%): Anonymous MAC Accrual

WES rewards WiFi end users for ad attention without requiring them to connect a wallet at the moment of the impression. This is a deliberate design choice: requiring wallet-first onboarding kills the conversion funnel for everyday WiFi users.

The lifecycle has three phases:

Phase 1 — Anonymous accrual. When a user connects to a participating venue and completes a captive impression, the impression is recorded against their device identifier. Each hourly epoch aggregates impressions per device, venue, and campaign and credits accrued WES into the device's reward record. The wallet field remains unset at this stage. CPM-weighted proportional share ensures higher-CPM campaigns deliver larger rewards per impression.

Phase 2 — User-initiated wallet binding. When the user later connects a wallet on `epscloud.io` while still on participating WiFi and explicitly opts in to bind their accrued WiFi rewards, the protocol associates that wallet with the anonymous reward records for that device. The bind step is an explicit, consented user action — nothing is bound to a wallet without the user's deliberate confirmation in the rewards page. To preserve rewards across operating-system MAC randomization, sibling device records that share a hashed device fingerprint may be associated with the same wallet at bind time, subject to a published anti-abuse limit. Once bound, the association is immutable: one wallet may hold many bound devices (multi-device + randomization recovery), but one device associates to exactly one wallet. Users may decline to bind, in which case their accrued rewards remain anonymous and expire per Phase 3.

Privacy posture (summary). The data collected, its purpose, retention, deletion paths, and user rights are summarised below; the full Privacy Notice and Data Processing Addendum are published in a separate document before public launch and reviewed by counsel.

- **Data collected:** hashed device identifier; hashed device fingerprint (browser/OS attributes); per-impression timestamp, venue identifier, and campaign identifier; on bind, wallet address.
- **Purpose:** attribution of ad-impression rewards to a specific device so the device's owner may later, at their option, claim the accumulated rewards by binding a wallet they control.
- **Retention:** per-impression records are retained for the duration needed to compute rewards and audit settlement, plus a bounded archival window for dispute resolution.
- **Deletion:** users may request deletion of their device identifiers and unbound reward records via the user-data request channel published in the Privacy Notice. Bound wallets and on-chain claim records are immutable once written.
- **No sale to advertisers:** personal identifiers, raw MAC addresses, and per-device fingerprints are not sold or licensed to advertisers. Advertisers receive only aggregated, anonymised reach and impression metrics.
- **Regional compliance:** the platform is designed to operate consistently with GDPR-style

and PDPA-style regimes. The published Privacy Notice / DPA documents the controller / processor model used in each jurisdiction.

Phase 3 — Claim or expire. A wallet with bound rewards sees a claim summary in the rewards dashboard. Claiming builds a Treasury Safe transfer batch, signers approve 2-of-3, and the transfer is broadcast on chain. Unclaimed rewards expire after 6 months. Expired rewards are not autonomously burned — administrators review a monthly batch and execute the burn through the Treasury Safe. Expired-then-burned WES reduces total supply, compounding the Buyback & Burn bucket's deflationary effect. Users continue to see expired rewards in their history for transparency.

WES is designed to support retroactive reward claiming from anonymous venue-based WiFi sessions, a capability that differentiates it from many wallet-first Web3 reward models. It removes wallet friction from the moment of attention, and routes unclaimed value back to deflationary supply reduction.

13.3 Buyback & Burn (10%): Phased Triggers

The Buyback & Burn bucket accumulates per-impression and is held in USDT-equivalent value until a phase-appropriate threshold is reached. When the threshold is met, an administrator builds a transaction from the Treasury Safe to (a) buy WES from the open market on PancakeSwap and (b) burn the purchased WES, permanently removing it from circulation. Both steps require 2-of-3 signer approval.

Threshold scales with venue network size to balance gas efficiency against deflationary cadence:

Phase	Network size	Burn trigger threshold
Phase 1 — Launch	Few venues	5,000 USDT accumulated
Phase 2 — Growth	1,000+ venues	30,000 USDT accumulated
Phase 3 — Scale	5,000+ venues	50,000 USDT accumulated

Each burn batch is recorded on-chain, attributed back to the contributing impressions, and visible in the public burn ledger. Phase upgrades are admin-controlled and accompanied by a public network-size disclosure.

13.4 Marketing (8%): Three-Way Split

The Marketing bucket funds three sub-channels with phase-dependent allocation:

1. **Tiered Referral Program (5% of total revenue, fixed).** Three-level referral tree pays Level 1 = 3.0%, Level 2 = 1.5%, Level 3 = 0.5% of total revenue. **Referral rewards are paid only from verified ad revenue, not from recruitment fees or token purchases.** Rewards credit to the referrer's off-chain WES balance on epoch close. If a referral chain is shorter than three levels, the unallocated portion rolls back into the Lucky Draw pool.
2. **Lucky Draw skim.** Configurable percentage of the residual marketing budget after referral rewards flows into the Lucky Draw prize pool. The percentage scales with growth phase:

Phase	Network size	Lucky Draw share of residual
Phase 1 — Launch	Few venues	0% (100% residual to direct marketing)
Phase 2 — Growth	1,000+ venues	40%
Phase 3 — Scale	5,000+ venues	70%

3. **Direct marketing.** What remains funds paid acquisition (Google/Meta ads, partnerships, content, events). Phase 1 keeps the full residual on direct marketing because cold-start growth needs aggressive paid acquisition; Phase 3 inverts the ratio because the network self-perpetuates and Lucky Draw prizes drive engagement loops more cost-effectively than ad spend.

The percentage is a runtime-editable system setting; admin changes are auditable and apply to subsequent epochs.

13.5 Withdrawals

User withdrawals move WES from the off-chain locked balance to the user's external wallet through a controlled multi-signature flow. The pipeline is designed to keep treasury custody intact while removing manual transaction-hash bookkeeping from operators.

Minimum withdrawal. The withdrawal minimum is denominated in USDT-equivalent value (currently 10 USDT) rather than a flat WES quantity. The conversion uses the same tiered price oracle that serves campaign quotes (Section 12.5): PCS V3 5-minute TWAP post-pool-launch, active sale tier price during R1–R3, last closed sale tier as transient fallback. If no rate source is available, withdrawals are blocked rather than allowing an unfair conversion. The dashboard shows the live USDT-equivalent next to every WES amount so users see the converted value before submitting.

Approval and execution flow:

1. The user submits a withdrawal request from their balance dashboard. The request enters the queue as pending, the locked-balance amount is reserved, and the destination wallet address is captured.
2. An administrator reviews the queue. The administrator may either approve (proceed to on-chain) or reject with an audit reason (off-chain refund of the locked balance).
3. On approval, the protocol prepares a Treasury Safe transfer for the exact WES amount targeting the user's wallet.
4. Two of the three independent protocol signers review and approve the transaction. No single signer can release funds.
5. Once the second signature lands, a designated executor account broadcasts the transaction on chain. The signers do not pay gas; the executor does.
6. A redundant settlement-monitoring layer observes the on-chain transfer, idempotently matches it to the pending withdrawal record, and finalizes the record with the transaction hash captured automatically.

The user never pastes a transaction hash; administrators never paste a transaction hash. Match-and-credit is fully automated.

Stuck-withdrawal alerts. A daily monitor watches for approved withdrawals that have

not yet been broadcast on chain. It does not auto-cancel, to avoid a race against late-arriving signatures, but it escalates to operators on a graduated cadence: 3-day nudge to signers, 7-day administrator alert, 14-day critical alert, and a 30-day repeat for extended cases. If a withdrawal genuinely needs to be cancelled, an administrator runs a Safe nonce-replacement procedure that invalidates the original transaction before the locked balance is refunded.

Anomaly detection. If WES leaves the Treasury Safe without a matching pending withdrawal, an immediate critical alert is raised flagging a possible governance bypass or compromise. Treasury movement is observable end-to-end whether it originates from the application layer or from a direct Safe interaction.

14. Trust, Integrity & Compliance

Advertisers and venues need confidence that the impressions they pay for and earn from are real. Users need confidence that their data is handled responsibly. Regulators need confidence that the protocol is operating within applicable law. This section describes how WES addresses each.

14.1 Impression Integrity

Every billable impression carries a full attribution tuple — venue, access point, device, campaign, captive session — written to a transactional ledger at the moment of completion. The ledger is the single source of truth for revenue allocation; downstream systems read from it, never write to it.

Real-AP requirement. Impressions are credited only when the captive session originated from an adopted access point in the WES location registry. The registry binds each access-point hardware address to one venue at provisioning time. An impression event without a valid AP-to-venue binding is rejected before it enters the revenue ledger.

Session-bound attribution. Each captive session is keyed by venue, access point, and client device. There is no shared global captive state and no anonymous-aggregate accounting. Every billable event carries the venue, AP, and device tuple it originated from.

Idempotent recording. Impression events are deduplicated on the (session, slot, terminal-state) triple so a network flake or client retry cannot produce double-credit. Wallet binding and reward crediting are wrapped in transactional dedup layers; a replayed webhook cannot double-credit a user.

14.2 Ad Fraud Posture

WES inherits standard ad-fraud challenges (bot traffic, emulator farms, scripted captive hits, installer collusion, wallet sybil) and addresses each with concrete controls:

- **Bot traffic.** The captive portal requires a JavaScript-rendered user agent and a successful WiFi association — a bot scraping a URL does not get a billable impression. Rate-limiting blocks high-frequency single-source attempts.
- **Emulator farms.** Impression events that lack a valid access-point binding are filtered before they enter the revenue ledger. An emulator on the open internet cannot produce an impression — only devices that completed the captive flow from an adopted access point qualify.

- **Installer collusion.** Venue onboarding requires reverse provisioning: an installer cannot self-credit fictitious impressions because the access point must complete adoption against the protocol-operated controller. Installer roles have no impression-creation authority and no revenue-write authority.
- **Wallet sybil for rewards.** Anonymous reward accrual binds a wallet through a captive-session evidence check — a wallet cannot claim rewards for impressions it did not participate in. Per-wallet hard caps, hashed device fingerprints, and behavior-similarity scoring (later phase) further reduce sybil profitability.
- **Measurement transparency.** Aggregate impression counts, per-venue revenue, and burn batches will be visible in public dashboards (Phase 4–5 deliverables). Independent verification against the on-chain ledger is possible at every settlement point.

WES does not claim a zero-fraud network. Ad fraud is an evolving adversarial problem. The protocol commits to publishing what it filters, how, and at what fraction, as the network grows.

14.3 Privacy and Data Policy

WES handles user data with three principles: minimize collection, secure what is collected, and give users visibility into what is bound to their wallet.

What is collected. When a user connects to participating WiFi:

- Device identifier (hardware address) is captured for session attribution and reward accrual.
- A hashed device fingerprint (derived from common browser/OS attributes) is computed for MAC-randomization recovery.
- Session timestamps, the venue and access point involved, and the campaign delivered are recorded.

What is not collected. WES does not collect name, email, phone number, payment details, browsing history, or content of network traffic. The protocol does not deep-packet-inspect user traffic. The protocol does not track users across networks outside the WES venue footprint.

How long. Impression records live in the revenue ledger as long as required for accounting and audit. Anonymous reward records expire 6 months after the last accrual event; expired records are marked for burn and removed from the active claim surface. Specific retention periods are published in a separate privacy notice released with public launch.

Consent and opt-out. The captive portal presents a clear notice that connecting to WiFi will deliver an ad and accrue an anonymous reward record. Users may decline by disconnecting before the ad completes — in that case no impression is recorded. Wallet-bound users can request deletion of their reward records through the dashboard; deletion forfeits unclaimed rewards.

Jurisdiction adaptations. WES is designed to operate under GDPR-style and PDPA-style regimes by treating device identifiers as personal data, requiring consent at the captive surface, and supporting deletion-on-request. Regional adjustments (children's privacy carve-outs, jurisdiction-specific retention caps) are applied at the regulatory layer when WES launches in each jurisdiction.

14.4 Transparency Metrics

To give advertisers, venues, and the community an honest picture of network health, WES publishes a set of operational quality metrics aggregated per epoch and per campaign. Indicative target ranges below are aligned with established programmatic-advertising benchmarks; they are reporting targets, not contractual guarantees. Initial launch-phase metrics may deviate materially from these target ranges until sufficient venue density, campaign inventory, and fraud baselines are established.

- **Invalid traffic rate** (impressions rejected by anti-fraud filters as bot / replay / non-human): target $\leq 2\%$.
- **Rejected-impression rate** (impressions excluded from billing due to short dwell, captive cancel, or quality threshold): target $\leq 5\%$.
- **Suspicious-venue rate** (venues placed under quality review per period due to anomalous behaviour): expected $< 1\%$ of active venues steady-state.
- **Average session completion rate** (sessions that reach reward-eligible dwell): target $\geq 70\%$.
- **Campaign fill rate** (impressions delivered against contracted budget at venue level): target $\geq 85\%$ steady-state.
- **Device-to-wallet bind rate** (share of devices that subsequently bind a wallet within 30 days): expected 5–15% early stage, scaling with on-device prompts and ecosystem value.
- **Claim rate** (share of accrued anonymous reward balances that are actually claimed before the expiry window): target $\geq 15\%$ at scale.

Metrics are recomputed daily and published to public dashboards once the operational scale is sufficient that the figures are statistically meaningful. Material methodology changes are disclosed before they take effect.

14.5 Compliance Posture

WES treats compliance as a launch-blocking concern rather than a post-hoc patch:

- **Token sale.** The public sale interface enforces per-wallet caps, minimum-confirmation gating on USDT/BNB contributions, and on-chain verification of every contribution. Jurisdictional restrictions on sale access (where applicable) are applied at the interface level.
- **Advertising.** Campaign creatives undergo AI-assisted moderation followed by human review before going live. Restricted-content categories (per jurisdiction) are blocked at the moderation layer.
- **Rewards.** Anonymous reward accrual is structured so that users do not need to take any action to participate, but unclaimed rewards expire — preventing indefinite accumulation that could create regulatory complexity.
- **Treasury.** All treasury movement requires 2-of-3 multisig approval. Treasury Safe signers are separated from web-app admin identities, reducing single-point-of-control concerns.
- **Audit trail.** Every state-changing action — campaign approval, withdrawal approval, vesting release, burn batch — is logged with actor identity, timestamp, and parameters. Audit logs are retained for compliance review.

The protocol intends to publish a separate compliance briefing alongside public launch

covering specific jurisdictional postures, KYC/AML thresholds (where applicable), and regulatory adjustment processes. The items below are the operating defaults the platform will use unless jurisdiction-specific rules require a stricter posture; the operational specifics in each row are templates to be finalised by counsel before launch.

KYC / AML threshold (template). Standard wallet-based sign-in does not require KYC. KYC documentation is requested when a wallet's cumulative activity crosses a per-jurisdiction threshold for any fiat-denominated event (sale contribution, withdrawal, payout claim). The default working threshold is the equivalent of $3,000 USD per calendar year, which will be tightened where local AML rules require a lower bar.

Country / jurisdiction restrictions (template). The platform maintains and publishes a list of restricted jurisdictions for each of: public sale participation, venue revenue payouts, advertiser campaign creation, and user reward claims. Geographic gating is applied at the interface layer; entries originating from a restricted jurisdiction are refused. Sanctions-screening checks are run against recognised global sanctions lists for fiat / on-chain counterparties. Additional restricted jurisdictions may include countries subject to sanctions, countries where token sales are prohibited or require registration, and jurisdictions where local counsel advises against participation.

Token sale eligibility (template). Participation in the public sale rounds is open to natural persons and entities resident in a permitted jurisdiction, who are not on any sanctions list and who self-certify they are not a U.S. person or otherwise excluded under applicable securities law. Per-wallet contribution caps and per-round minimums are enforced server-side and on-chain.

Advertising content categories (template). The campaign moderation layer blocks at least the following category set unless explicitly cleared by counsel for a given market: weapons, regulated gambling, adult content, regulated pharmaceuticals, financial scams, tobacco / vaping (where restricted), political-electioneering content (where restricted), and any content prohibited by the host venue's terms. Creatives undergo AI-assisted pre-screen plus human final review.

Minors and children (template). The captive surface is intended for adult use. The platform does not knowingly collect personal data from minors. Venues operating in minors-accessible locations (schools, certain entertainment venues) are flagged in onboarding and routed to a restricted creative pool. Where local children's-privacy law applies, an additional age gate at the captive surface is required before reward accrual is enabled.

Sweepstakes / Lucky Draw compliance. Covered in Section 9.6; the full Lucky Draw rule set is reviewed by counsel before each phase change and is published as a separate Terms & Conditions document before the first draw.

Data controller / processor responsibility. The operating entity acts as data controller for the impression / device-identifier records, and as processor where it carries data on behalf of an advertiser or venue partner. The published Data Processing Addendum defines the controller / processor split per-region.

Tax responsibility. Token sale contributors, reward claimants, and venue payout recipients are responsible for their own tax reporting and tax obligations in their jurisdiction of residence. WES does not provide tax advice. Where local law requires the platform to withhold or report, the platform implements the required collection and reporting at the relevant interface step.

Nature of the token. WES is a utility token used inside the ecosystem for payment of

campaign budgets, distribution of incentives, and on-chain settlement of revenue splits. **WES does not represent equity, debt, dividends, ownership rights, profit-sharing, a claim on company revenue, or any guaranteed distribution.** Holders should evaluate the token on its utility within the ecosystem and on the risks set out in Section 19.

15. Technical Architecture

15.1 Hybrid Service Model

WES separates concerns by where they belong:

- **Authenticated content surfaces** — dashboards and data services for locations, campaigns, partnerships, and role-aware administrative views.
- **API and protocol layer** — wallet authentication, token sale, captive portal, staking, revenue accounting, balances, claims, and creative workflows.
- **Persistent state** — a transactional ledger for canonical business data and an in-memory layer for live state and event coordination.
- **Edge delivery** — standard content delivery and web application firewall surfaces for static assets and creatives.
- **On-chain settlement** — BNB Smart Chain provides token ownership, staking, vesting, claim distribution, and treasury settlement.

This separation lets the protocol move high-frequency accounting off-chain (where it is fast and cheap) while preserving on-chain finality at every settlement point.

WES does not compete with hyperscale cloud platforms on infrastructure scale, nor does it need to. The hot-path workload — captive-portal authorization, impression recording, hourly epoch settlement — is small per event but auditable end-to-end, and the architecture is sized for the network's projected venue count rather than for arbitrary global scale. Capacity is grown as the venue footprint grows; over-provisioning ahead of demand is treated as wasted runway.

15.2 Resilience Posture

The production system favors operational simplicity over architectural maximalism. Critical paths use managed leader election for the transactional ledger, redundant worker pools for background operations, and idempotent event handlers so that retries do not double-credit. The objective is not to eliminate every single-box dependency on day one, but to keep application logic observable, recoverable, and inspectable end-to-end. The protocol's settlement authority lives on chain regardless of the application layer's availability at any given moment — treasury balances are checkable from any synced BSC node.

15.3 Gas Efficiency

WES avoids writing every impression or micro-credit to the blockchain. The system computes high-frequency events off-chain and records them in durable ledgers. On-chain transactions occur only at meaningful settlement points:

- Token purchases and verified contribution records.
- Staking deposits and staking reward settlement.
- User claims and withdrawals.

- Vesting releases.
- Treasury-controlled batch operations.
- Buyback, burn, and other treasury flows.

This approach reduces gas cost, keeps the user experience responsive, and preserves on-chain finality where it actually matters.

16. Security Model

16.1 Wallet Authentication

WES login is based on message signing. The server issues a nonce, the wallet signs it, and the backend verifies the recovered address. JWT sessions carry role, hierarchy level, wallet address, and staking gate data.

16.2 Role-Based Access Control

WES uses numeric hierarchy levels rather than only string roles. This keeps permission checks consistent across the entire application surface — front-end controls, content rendering, and the protocol API layer all evaluate the same numeric authority.

Level	Role	Typical authority
99	Admin	Full administration, treasury services, system operations
90	BOD	Approval, revenue, member, and management surfaces
70	Agency	Campaign creation and campaign management
50	Venue Owner	Own venue visibility and limited venue management
40	Agent	Venue onboarding and operational assistance
20	Installer	Limited install/update duties
5	Regular Member	Public user actions, staking, rewards, lucky draw

The frontend may hide controls, but the backend remains the source of truth for authorization.

16.3 Treasury Safety

The Treasury Safe is a Gnosis Safe v1.3.0 multisig with a 2-of-3 threshold. It owns the WESToken contract and holds critical on-chain authority. Treasury signers are separated from web-app Admin and BOD login identities so a compromise of the web admin surface does not automatically grant fund-movement authority.

16.4 On-Chain Verification

Sale contribution records are confirmed only after backend verification of the BNB or USDT transaction on BNB Smart Chain. Verification checks transaction existence, success status, sender, receiver, token contract, amount, chain ID, and minimum confirmations.

16.5 Smart Contract Hardening

The contract suite is built on industry-standard security patterns:

- Two-step ownership transfer to prevent accidental key loss.
- Emergency pause capability on token operations.
- Role-based permissions for sensitive contract actions, with each role separable from token ownership.
- Safe ERC-20 transfer handling that surfaces failures explicitly rather than silently.
- Time-locked vesting contracts for all non-public-sale allocations.
- Multisig ownership over treasury authority.

17. Governance and Operations

WES governance is operationally split into three layers:

1. Product and account governance through Admin and BOD roles.
2. Treasury governance through multisig-controlled Safes.
3. Protocol execution through deployed contracts and keeper identities.

Admin and BOD can manage users, campaigns, locations, and operational approvals. Treasury movement requires multisig approval. Automation accounts may submit or execute specific operations, but they are not Safe owners and cannot drain principal.

18. Roadmap

Phase status reflects state as of this whitepaper revision. Items are labeled **DONE** (shipped to production), **IN PROGRESS** (partially shipped or actively under development), and **PLANNED** (next-phase scope, not yet started).

18.1 Phase 1: Core Infrastructure

- **DONE** — Production backend stack live with resilient routing, redundant workers, and idempotent event handling.
- **DONE** — Wallet authentication via EIP-191 nonce signing and JWT sessions.
- **DONE** — Venue registry, captive portal, role-aware dashboards, RBAC by hierarchy level.

- **DONE** — WESToken, WESStaking, WESClaim, TokenVestingTeam, and TokenVestingHardware contracts deployed on BNB Smart Chain mainnet.
- **DONE** — Treasury Safe, BOD Safe, and Hardware Safe established as Gnosis Safe v1.3.0 multisigs (2-of-3) with three independent protocol signers.
- **DONE / READY** — Angel investor tier structure finalized (Tier 1/2/3, see Section 11.5). The three `TokenVestingAngelsTier` contracts are internally audited and testnet-verified end-to-end on BSC testnet; mainnet lazy deployment occurs on first angel commitment.

18.2 Phase 2: Public Sale and Staking

- **IN PROGRESS** — Three-round public sale (Strategy γ) infrastructure complete; R1 activation on admin "GO LIVE" trigger when product is ready.
- **DONE** — USDT and BNB purchase paths with on-chain transaction verification at three confirmations before confirmed accounting.
- **DONE** — Staking dashboard, staking listener, and reward-distribution worker.
- **DONE** — Revenue and earnings surfaces gated by Staking Success flag.
- **DONE** — Per-user HD deposit address with redundant watcher infrastructure and idempotent sweep-and-credit pipeline.
- **PLANNED** — PCS V3 liquidity pools (WES/USDT + WES/BNB) deploy Day 181, immediately after R3 close. Phase 0 liquidity-support window operates for 30 days post-launch (see Section 11.6).

18.3 Phase 3: Venue and Campaign Expansion

- **IN PROGRESS** — Venue onboarding flow with reverse provisioning (plug-and-adopt access points) and dual-SSID branding.
- **DONE** — Campaign targeting engine by venue category, city, and brand metadata.
- **DONE** — Creative hot-cold storage on edge object storage plus archive-to-replicated-storage pipeline.
- **IN PROGRESS** — AI-assisted multi-worker creative moderation followed by human review; full automation pending confidence-history baseline.
- **PLANNED** — Programmatic agent and installer workflows at fleet scale (10+ venues onboarded per agent per week).
- **PLANNED** — Richer advertiser analytics (per-venue, per-creative, per-city impression deltas).

18.4 Phase 4: Revenue Settlement and Growth Loops

- **DONE** — Epoch revenue distribution on closed UTC hour windows with atomic per-epoch writes.
- **DONE** — User withdrawal pipeline with admin approval, Treasury Safe 2-of-3 signing, automated on-chain broadcast, and automatic settlement reconciliation.
- **DONE** — Stuck-withdrawal monitor with graduated operator alerts (3 / 7 / 14 / 30 days).
- **IN PROGRESS** — Larger Lucky Draw rounds; prize pool scaling with Phase 2 / 3 marketing-skim ratios.
- **PLANNED** — Affiliate / referral leaderboard and rolled-up tree visualization for referrers.
- **PLANNED** — Public buyback-and-burn dashboard with batch history, burn ledger, and supply-reduction chart.

18.5 Phase 5: Ecosystem Maturity

- **PLANNED** — Native mobile application (iOS / Android) that issues a stable device identifier from the secure enclave. This delivers more reliable device-to-wallet binding for users across operating-system MAC randomization and app reinstalls, scaling anonymous reward accrual at high confidence.
- **PLANNED** — Centralized exchange listings once on-chain liquidity, daily trade volume, and verified user metrics meet listing tier criteria. Decentralized PancakeSwap pools remain the canonical price-discovery venue throughout.
- **PLANNED** — Enterprise advertiser tools: programmatic API access, multi-campaign budget rollups, branded campaign templates, and a self-serve agency onboarding flow.
- **PLANNED** — Governance evolution from BOD-multisig approval to a published proposal cadence with on-chain voting where the protocol benefits from formal decentralization. The Treasury Safe remains the source of fund-movement authority; voting governs protocol parameters such as marketing allocation ratios, burn-phase thresholds, ad-slot CPM weights, and venue brand taxonomies.
- **PLANNED** — Quarterly transparency reports covering revenue distribution, burn batches, treasury allocations, and active-venue / active-user metrics.
- **PLANNED** — Expanded venue categories and managed brand taxonomies covering regional verticals as the network grows beyond initial geographies.
- **PLANNED** — Additional integrations (loyalty programs, point-of-sale partners, on-ramp providers, identity layers) where they improve user, venue, or advertiser utility without compromising the protocol's core attribution invariants.

19. Risks

WES has real risks. Participants should understand them before interacting with the ecosystem.

19.1 Market Risk

The value of WES can fluctuate. Token price may be affected by liquidity, market demand, user adoption, regulatory conditions, and broader crypto market cycles.

19.2 Revenue Risk

Revenue depends on advertiser demand, campaign quality, venue coverage, user engagement, and operational execution. The revenue split describes allocation rules, not guaranteed revenue.

19.3 Smart Contract Risk

Although the contracts use standard security patterns, smart contracts can contain unknown vulnerabilities. On-chain operations are irreversible once executed.

19.4 Operational Risk

WES combines web infrastructure, WiFi hardware and controllers, edge services, databases, and blockchain RPC providers. Any of these layers can experience downtime, configuration

drift, rate limits, or external service outages.

19.5 Regulatory Risk

Digital assets, advertising, data privacy, rewards, and token sales may be regulated differently across jurisdictions. WES may need to adjust product availability, sale access, or reward mechanics to comply with applicable requirements.

19.6 Ad Fraud Risk

Even with the integrity controls described in Section 14, ad fraud is an evolving adversarial problem. Adversaries may discover new ways to generate billable impressions without delivering genuine attention. This can directly reduce advertiser ROI and indirectly affect venue revenue, user rewards, and treasury burn velocity. WES commits to publishing what it filters and at what fraction, but cannot guarantee fraud-free measurement at any point in time.

19.7 Privacy Enforcement Risk

WES processes device identifiers and hashed device fingerprints to attribute impressions and bind anonymous rewards. Jurisdictions with strict privacy regimes (GDPR, PDPA, equivalents) may require operational changes — consent flow adjustments, retention reductions, deletion workflows, or geographic restrictions on the reward mechanism. Adverse rulings could reduce the addressable venue or user base, or require redesign of the wallet-binding flow.

19.8 Key Compromise and Operational Security Risk

Treasury Safe signers, vesting destination Safes, and operational keeper EOAs together control on-chain fund movement and protocol execution. The protocol uses multisig discipline, identity separation between web admin and treasury, and key isolation on dedicated host boundaries to reduce concentration of authority. However, a sufficiently capable compromise of multiple signer hosts or a coerced key disclosure could allow unauthorized treasury action. Time-locked vesting contracts and immutable destinations limit the blast radius. Users should evaluate counterparty risk before staking or holding meaningful balances.

20. Conclusion

WES is built around a practical thesis: real-world WiFi attention can become a measurable digital economy when venues, users, advertisers, and token participants are connected through transparent accounting and Web3 settlement.

The project combines a working Ad-Tech operating model with a BEP-20 token, staking, revenue allocation, venue-level targeting, and multisig treasury controls. Its success depends on growing real venue supply, advertiser demand, reliable infrastructure, careful treasury governance, and disciplined product execution.

WES is not just a token attached to an idea. It is an attempt to build a real-world WiFi advertising network where the economic value of impressions is shared across the people and infrastructure that make those impressions possible.

Appendix A. Mainnet Contracts and Audit Status

All contracts and Safes below are deployed on BNB Smart Chain (chain ID 56) and are independently verifiable on any BSC block explorer. Audit status is reported as of this whitepaper's revision date; subsequent updates are reflected on the public dashboard.

Contract	Address	Network	Status	Audit
WESToken	`0xA90fdd27D893CE4D1EF5c33b89CC6dEf630663bC`	BSC mainnet	Deployed	Internal review
WESStaking	`0x9fBF1997e73b633d88848f2cB5C8845D845D7eA6`	BSC mainnet	Deployed	Internal review
WESClaim	`0x7970bE58D6dc84BE4dE22fd73B51C74FA1D4C6eB0f`	BSC mainnet	Deployed	Internal review
TokenVestingTeam	`0x11A6886d6aE204412DA18b4CdBcE1052829d49A0`	BSC mainnet	Deployed	Internal review
TokenVestingHardware	`0xB4564d3BbB9eF0cE0939915dbaFC7a73956bDEf0D`	BSC mainnet	Deployed	Internal review
TokenVestingAngelsTier 1/2/3	to be published at deploy time	BSC mainnet	Lazy deploy on first angel commitment	Internal review + testnet verified
Treasury Safe	`0xa79edf5f23a1358e652a9fd19c3c53165240bf8f`	BSC mainnet	Active (2-of-3)	n/a
BOD Safe	`0x8e97600c39bC8D013399DBfaB54fa2955E6702e0`	BSC mainnet	Active (2-of-3)	n/a
Hardware Safe	`0xAd8137dF75a15d890Fd40aEA8BDECA452d9d4dE5`	BSC mainnet	Active (2-of-3)	n/a

Audit programme. "Internal review" indicates that the contract has been reviewed by the engineering team using static analysis (Slither) and a unit-test harness, including time-warped lifecycle tests where applicable, plus end-to-end exercise on BSC testnet for the tier vesting family. **No third-party smart-contract audit has been completed as of this revision.** A third-party external audit by a recognised smart-contract auditing firm is planned and will be funded from treasury proceeds at the appropriate funding milestone; the audit report and any resulting fixes will be published as an addendum to this appendix once available.

Safe configuration. All three Safes are Gnosis Safe v1.3.0 multisigs with the same independent three-signer set and a 2-of-3 threshold. Lowering the threshold to 1-of-3 is forbidden by protocol policy; raising to 3-of-3 itself requires a 2-of-3 Safe transaction. Web-app administrative identities are distinct from on-chain Safe signers: a compromise of the web surface does not grant fund-movement authority, and vice versa.

Vesting immutability. Each vesting contract's destination addresses are baked into the constructor at deploy time and cannot be changed afterwards. `TokenVestingTeam` can only release WES to the BOD Safe; `TokenVestingHardware` can only release WES to the Hardware

Safe; each `TokenVestingAngelsTier` instance can only release to its registered beneficiary set.