VibeCheck Product and Token Utility Whitepaper

Website and token project inspection on Solana

Version 1.0 September 2026

VibeCheck analyzes public technical and media signals to estimate whether websites and project assets were created or assisted by AI. This paper defines the product, its scoring principles, the CA Inspector, and the utility assigned to the $VIBE token.

Product documentation and utility disclosure

Executive Overview

VibeCheck is a public signal inspection product for websites and Solana token projects. It combines deterministic builder fingerprints, technology indicators, public metadata, and AI media estimates into evidence based reports. The product is designed to show why a result was reached. It does not claim to prove who created a website or image.

The platform has two core inspection surfaces. The Website Scanner accepts a public URL and estimates whether the site was created or assisted by AI. The CA Inspector accepts a Solana contract address, reads public token metadata, evaluates the token image and linked X profile picture for AI generation signals, and runs a website vibe check when metadata includes a site.

The $VIBE token provides access to premium Website Scanner reports. The current launch configuration exchanges 1,000,000 $VIBE for 10 premium scan credits. One premium scan consumes one credit. Each connected wallet may also use one basic Website Scan per rolling 24 hour period. CA Inspector is free at launch and consumes no scan credits.

Product surface	Input	Primary output	Current access
Website Scanner	Public URL	AI likelihood, possible builder, technology signals, evidence and limitations	One basic scan per wallet every 24 hours or one premium credit
CA Inspector	Solana contract address	Token metadata, token and X image AI signals, linked website vibe check	Free at launch and no scan credits used
Premium Scan Pack	$VIBE payment	Ten premium Website Scanner credits	1,000,000 $VIBE at launch

Status and Scope

This paper documents confirmed product mechanics discussed for VibeCheck and marks undisclosed token parameters as not yet published. It does not invent a total supply, allocation schedule, vesting plan, mint address, legal entity, or treasury control structure. Those items require separate publication before they can be treated as official.

Important Notice

This whitepaper is product documentation. It is not investment advice, a promise of token value, a security audit, or an offer to sell financial instruments. AI and builder classifications are estimates based on observable public signals. Users must perform their own technical, legal, and financial review.

Contents

1 Product Purpose and Principles

2 Product Overview

3 Website Scanner

4 CA Inspector

5 Detection and Scoring Methodology

6 System Architecture

7 Security and Abuse Controls

8 Access and Scan Credits

9 VIBE Token Utility

10 Token Parameters and Treasury Controls

11 Privacy and Responsible Use

12 Risks and Limitations

13 Roadmap

14 Success Measures

15 Conclusion

Appendix A Report Data Model

Appendix B Launch Parameter Registry

Appendix C Glossary

1 Product Purpose and Principles

Product Purpose

Modern websites often combine human design, generated code, site builders, AI written copy, and later manual edits. Once deployed, the public site usually does not preserve a complete development history. Crypto project review adds another problem: token metadata, project imagery, social identity, and website implementation often live in separate places. VibeCheck brings those public signals into a single inspection workflow.

VibeCheck is intended to answer a narrow question responsibly: what observable signals suggest that AI or an AI enabled builder contributed to this website or project asset? The answer is presented with evidence, confidence, and limitations. It is not a binary declaration of human or machine authorship.

Design Principles

Principle	Meaning in the product
Evidence before verdicts	Reports identify the signals behind a classification instead of returning an unsupported score.
Deterministic signals first	Explicit metadata, builder fingerprints, asset paths, and bundle evidence receive more weight than visual style or language patterns.
Public data scope	Scans use public pages, public token metadata, and public linked media. VibeCheck does not require access to private repositories or accounts.
Uncertainty stays visible	Low confidence and missing evidence are shown directly. No evidence is not treated as proof of human authorship.
Utility before speculation	$VIBE is tied to premium scan access. The product makes no promise about market price or financial return.

Intended Users

- Developers and agencies comparing implementation patterns across public websites.
- Founders and researchers studying adoption of AI enabled website builders.
- Crypto users reviewing the public identity of a Solana token project before making their own decision.
- Project teams that want an explainable report about the signals visible in their public assets.

Non Goals

VibeCheck is not a vulnerability scanner, smart contract audit, fraud detector, identity verification service, or investment rating. It does not guarantee that a project is safe, legitimate, original, or profitable.

2 Product Overview

The product uses a common inspection pipeline. Inputs are validated, public content is collected within strict limits, specialized engines extract signals, and a scoring layer produces an explainable report. Website Scanner and CA Inspector share this pipeline but use different inputs and access rules.

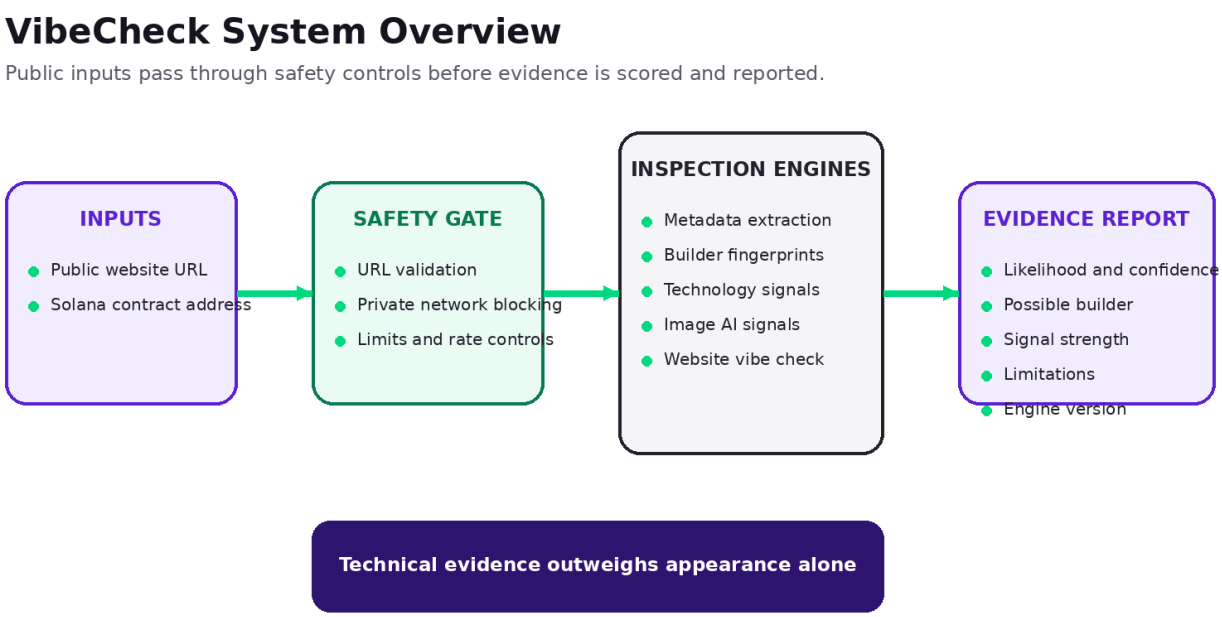


Figure 1 VibeCheck accepts public inputs, applies safety controls, and produces an evidence based report

Report Structure

- Input and scan type, including the normalized URL or contract address.
- AI likelihood and confidence when the scan supports those fields.
- Possible builder, framework, hosting, and technology indicators.
- Evidence items with a plain language explanation and a strength rating.
- Limitations, missing sources, scan timestamp, and engine version.

Result Language

Classification	Use
Confirmed builder signature	Reserved for explicit and verifiable builder metadata or an equivalent direct marker.
Likely AI assisted	Used when several strong signals point in the same direction.
Possibly AI assisted	Used when signals exist but are incomplete, weak, or mixed.
Insufficient evidence	Used when the public site does not provide enough reliable information for a meaningful classification.

3 Website Scanner

Basic Scan

A Basic Scan accepts a public HTTP or HTTPS URL and analyzes the homepage. Each connected wallet receives one Basic Scan during each rolling 24 hour period. The report includes a basic AI likelihood estimate, a possible builder, detected technologies, the strongest evidence items, and limitations.

Premium Scan

A Premium Scan uses one scan credit and performs a deeper inspection. The intended launch configuration analyzes the homepage and up to four additional pages on the same origin, subject to availability and safety limits. It expands builder fingerprinting, technology detection, visual analysis, and evidence coverage.

Capability	Basic scan	Premium scan
Page coverage	Homepage	Homepage plus up to four same origin pages
Builder detection	Core fingerprints	Expanded fingerprints and cross page evidence
Technology analysis	Primary framework indicators	Broader framework, hosting, and asset analysis
Evidence	Strongest signals	Full evidence list with strength labels
Report	On screen summary	Detailed shareable and downloadable report
Cost	One free allowance per wallet every 24 hours	One premium scan credit

Website Signals

- Generator metadata, public builder badges, and explicit platform markers.
- HTML comments, script and stylesheet paths, asset domains, and bundle strings.
- Framework, hosting, deployment, and structured data indicators.
- Repeated component, layout, and copy patterns used as supporting evidence only.
- Image provenance or media indicators when the public asset provides usable data.

Website Scanner Limits

A public deployment can hide or remove its original source, generator metadata, repository history, and build process. A human can use AI for only part of a site, and an AI generated starting point can be heavily rewritten. The Website Scanner therefore estimates likelihood from the available evidence and never labels a site definitively human made.

4 CA Inspector

CA Inspector accepts a public Solana contract address and builds a project level report from the public information associated with that address. At launch, the feature is free and does not consume Website Scanner credits.

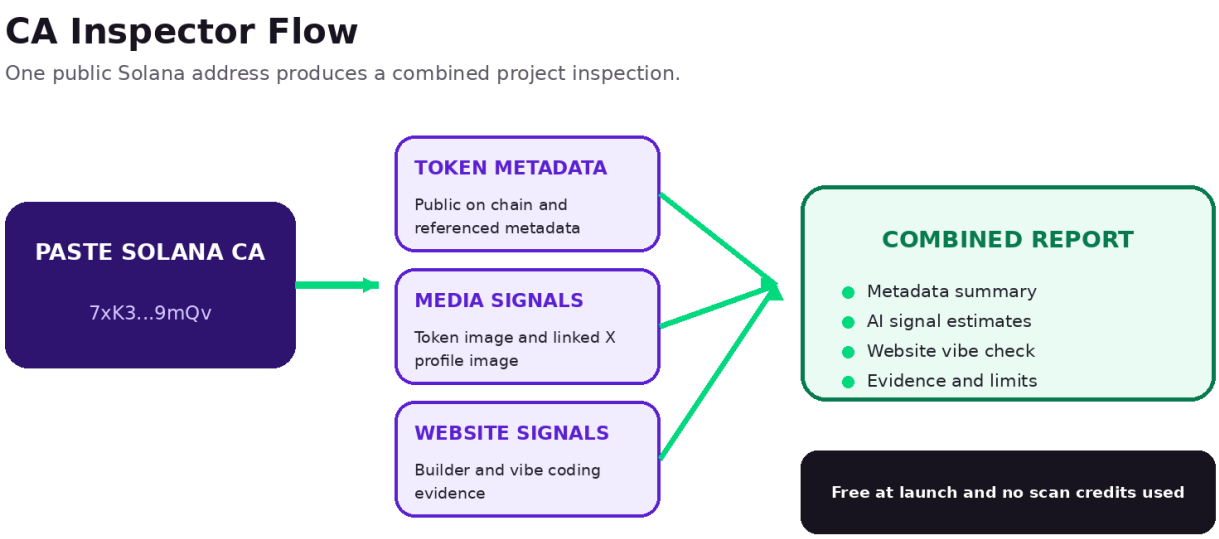


Figure 2 CA Inspector combines token metadata, media signals, and the linked website into one report

Inspection Steps

1. Validate the submitted Solana address and request public on chain token metadata.
2. Retrieve referenced public metadata when it is available and safe to access.
3. Evaluate the token image for signals associated with AI generated imagery.
4. Evaluate the linked X profile picture when a public image is available.
5. Run a Website Scanner inspection when the metadata includes a public website.
6. Combine the results with source availability, confidence, evidence, and limitations.

CA Inspector Output

- Token name, symbol, public metadata fields, and referenced links when available.
- AI generation signal estimates for the token image and linked X profile picture.
- Website builder and vibe coding signals for the linked public site.
- A record of missing, inaccessible, or invalid sources so the report does not imply complete coverage.

CA Inspector Boundaries

CA Inspector does not audit token code, liquidity, holder concentration, transfer restrictions, authorities, or trading risk unless those capabilities are separately implemented and disclosed. A favorable media or website result is not evidence that a token is safe.

5 Detection and Scoring Methodology

Evidence Hierarchy

Evidence level	Examples	Typical weight
Direct	Explicit generator metadata, public builder badge, verifiable platform marker	Highest

Evidence level	Examples	Typical weight
Technical	Asset domains, bundle strings, script paths, framework and deployment fingerprints	High
Corroborating	Repeated component patterns, layout structure, media metadata	Medium
Heuristic	Visual style, generic copy patterns, model based aesthetic estimates	Low

A high score should require either direct evidence or several independent technical signals. Heuristic appearance alone should not produce a high confidence result. Conflicting signals lower confidence and appear in the limitations section.

Scoring Process

1. Normalize the input and collect permitted public sources.
2. Run deterministic fingerprint rules and record every matched rule.
3. Run supporting media or pattern classifiers where applicable.
4. Apply source reliability, signal strength, and conflict adjustments.
5. Map the combined result to a likelihood range and confidence label.
6. Generate a report that lists evidence and limitations beside the result.

Calibration and Versioning

The scoring engine should be versioned. Each release should be tested against known builder examples, manually created sites, mixed origin sites, and altered deployments. VibeCheck should track false positive disputes, false negatives found through verified provenance, and accuracy changes when builder signatures evolve. Public reports should record the engine version so results can be interpreted in context.

Corrections

Site and project owners should be able to submit provenance evidence or report an incorrect association. Corrections should update the fingerprint registry only after review. The product should preserve a distinction between user supplied claims and independently verified evidence.

6 System Architecture

Application Components

Component	Responsibility	Trust boundary
Web client	Collect URLs or contract addresses, connect a wallet, and display reports	Untrusted client input
Server functions	Validate requests, fetch public sources, orchestrate engines, and enforce limits	Primary validation boundary
Fingerprint registry	Store versioned builder, framework, and hosting signatures	Curated rules only

Component	Responsibility	Trust boundary
Media analyzer	Estimate AI generation signals for permitted public images	Probabilistic output
Scoring engine	Combine evidence, conflicts, and source reliability	Versioned decision logic
Database	Store scan records, credit balances, purchases, and rule versions	Row level access controls
Solana verifier	Read metadata and verify premium token transfers	Server side RPC verification

Scan Lifecycle

1. Receive an authenticated or rate limited request.
2. Normalize and validate the URL or contract address.
3. Apply network safety checks before every fetch and redirect.
4. Collect public content within time, size, and page limits.
5. Run extraction and analysis engines.
6. Create a versioned report and charge a credit only when the premium scan is accepted for processing under the published policy.

Operational Reliability

The production service should use structured logs, request identifiers, scan status transitions, retry limits, and explicit failure messages. A partial result must identify which sources failed. The service should not convert a missing source into a negative finding.

7 Security and Abuse Controls

URL Fetching Controls

- Allow only public HTTP and HTTPS targets.
- Block loopback, private, link local, and other non public IPv4 and IPv6 ranges.
- Reject embedded credentials, unsupported protocols, and disallowed ports.
- Resolve and revalidate every redirect destination before continuing.
- Use strict redirect, time, response size, and page count limits.
- Apply rate limits by wallet, account, IP risk signals, and service capacity.

Wallet and Payment Controls

Premium credits must be issued only after server side verification of the Solana transaction. Verification should confirm transaction finality, the official $VIBE mint, the treasury destination, the paying wallet, the transferred raw amount after token decimals, and the uniqueness of the transaction signature. Credit issuance and purchase recording should be atomic to prevent double crediting.

Application and Data Controls

- Keep API credentials and RPC keys in server side secret storage.
- Treat the browser as untrusted and repeat critical authorization checks on the server.
- Use row level policies so users can access only their own private scan and purchase records.
- Expose only selected fields when a user creates a public share link.
- Record rule and engine versions to support incident review and reproducibility.

Abuse Considerations

The service must discourage bulk scraping, harassment, and attempts to scan internal systems. Rate limits, blocked target classes, source caps, and account controls protect both the service and third party sites. Public reports should describe technical evidence without accusing an owner of deception or misconduct.

8 Access and Scan Credits

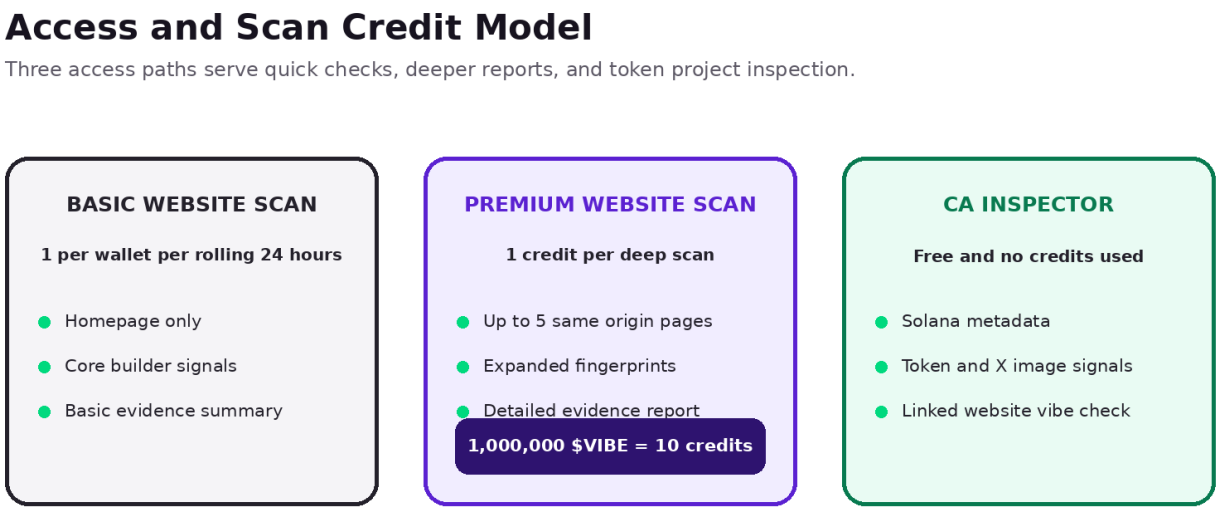


Figure 3 VibeCheck uses separate access rules for basic scans, premium scans, and CA Inspector

Basic Website Access

Each connected wallet receives one Basic Website Scan per rolling 24 hour period. Wallet based limits reduce casual abuse but do not eliminate multi wallet behavior. Additional risk controls may be used when necessary, provided they are applied consistently and disclosed in the product terms.

Premium Credits

The launch scan pack contains 10 premium credits for 1,000,000 $VIBE. A premium scan consumes one credit. Credits represent service access and do not represent ownership, revenue share, or a claim on treasury assets. The product should display the exact token amount, number of credits, and receiving address before a wallet signs a payment.

CA Inspector Access

CA Inspector is free at launch and does not consume scan credits. Its rate limits may differ from Website Scanner limits because it depends on public Solana and linked metadata sources. Any future pricing change should be announced before it takes effect.

Credit Policy

- Credits should be deducted through a single server controlled transaction.
- A failed scan should follow a published refund or restoration policy based on when processing failed.
- Purchased credits should not expire unless an expiration rule is disclosed before purchase.
- Pricing changes should not reduce credits already recorded in a user account.

9 VIBE Token Utility

Current Utility

$VIBE is the access token for premium VibeCheck scans. Its defined launch utility is limited and concrete: users may transfer the published amount of $VIBE to receive premium scan credits. The token does not provide equity, ownership, profit rights, guaranteed access to future products, or governance rights unless a later specification explicitly adds those rights.

Utility Lifecycle

1. The user connects a supported Solana wallet.
2. The application shows the official mint, treasury destination, token amount, and credits to be issued.
3. The user approves the transfer in the wallet.
4. The server verifies the finalized transaction and rejects a reused signature.
5. The database records the purchase and adds 10 premium scan credits atomically.
6. The user spends one credit for each completed premium Website Scan under the published credit policy.

What the Utility Does Not Promise

Product demand may create demand for service access, but VibeCheck makes no statement that token value will increase. The whitepaper does not define price support, yield, dividends, buybacks, burns, staking returns, or revenue sharing. Those mechanisms should not be inferred from the scan credit model.

Pricing Changes

The 1,000,000 $VIBE scan pack is a launch configuration. Token price volatility and service costs may require later adjustment. Any change should be versioned, announced in advance, displayed before payment, and applied prospectively.

10 Token Parameters and Treasury Controls

Published and Unpublished Parameters

Parameter	Current disclosure
Network	Solana
Ticker	$VIBE
Launch utility	Premium Website Scanner credits
Launch scan pack	1,000,000 $VIBE for 10 premium credits
Token mint address	Not yet published in the source material for this whitepaper
Total supply	Not yet published
Allocation	Not yet published
Vesting and lockups	Not yet published
Treasury address	Not yet published
Treasury signer policy	Not yet published

Parameter	Current disclosure
Burn or buyback policy	None specified
Token governance rights	None specified

Required Treasury Disclosures

Before broad token based access is promoted, VibeCheck should publish the official mint address, treasury address, signer structure, authority status, and policy for tokens received through scan packs. If treasury funds support hosting, model inference, development, audits, liquidity, or other activities, the policy should distinguish those uses and explain the approval process.

Change Management

The operator currently controls product and pricing parameters. Token ownership does not imply a vote. Material changes to scan pricing, credit quantities, report scope, treasury routing, or token rights should receive a dated specification update and an effective date. Existing credits should remain valid under the terms shown when they were issued unless the user agrees otherwise.

11 Privacy and Responsible Use

Data Scope

VibeCheck is designed for public data. Website scans should fetch only public pages. CA Inspector should use public Solana metadata and public linked images or sites. The product should not request private keys, seed phrases, website credentials, or access to private repositories.

Data Minimization

A production deployment may need to store the normalized input, result, evidence, timestamps, engine version, wallet address for allowances, credit balance, and transaction signature for purchase verification. The service should avoid retaining raw fetched content longer than operationally necessary and should publish a retention and deletion policy.

Responsible Result Presentation

- Describe results as likelihoods and signals rather than accusations.
- Show the strongest contrary evidence and missing sources when relevant.
- Provide a correction channel for site and project owners.
- Do not rank projects by safety or investment quality without a separately defined and validated methodology.
- Prevent public share pages from exposing private account, wallet, or purchase information beyond what the user deliberately shares.

Third Party Services

Some reports depend on Solana RPC providers, website hosts, public X images, and other external services. Their availability, terms, and response formats can change. VibeCheck should identify unavailable sources rather than silently substituting a conclusion.

12 Risks and Limitations

Risk	Effect	Mitigation
False positive or false negative	A site or image may be classified incorrectly	Use evidence tiers, confidence labels, test sets, and correction review
Fingerprint drift	Builder updates can invalidate rules	Version the registry and monitor known examples
Spoofing	A site can copy or remove fingerprints	Require independent signals and lower confidence when evidence conflicts
Incomplete metadata	CA Inspector may miss links or images	Report missing sources and avoid completeness claims
Third party outage	RPC, website, or image access may fail	Use timeouts, controlled retries, partial reports, and source status
Token volatility	The fiat value of a scan pack can change	Publish pricing changes and show the exact amount before signing
Treasury or wallet failure	Payments or funds may be lost or misrouted	Publish official addresses, use secure signing, and verify transactions server side
Regulatory change	Token access or marketing may face new obligations	Obtain jurisdiction specific legal review and update product terms
Reputational misuse	Reports may be presented as proof of fraud or authorship	Use cautious language, disclaimers, evidence visibility, and correction channels

Detection Is Not Provenance

Reliable provenance normally requires signed metadata, source history, repository access, builder attestations, or other first party evidence. VibeCheck usually sees the public output instead. Its reports should help users investigate, not replace provenance.

CA Inspector Is Not Due Diligence

CA Inspector does not determine whether a token contract is safe, whether liquidity can be withdrawn, whether holders are concentrated, or whether a project team is genuine. Users who trade tokens need separate contract, market, ownership, and legal review.

13 Roadmap

Current Product Scope

- Public Website Scanner with one basic allowance per connected wallet every 24 hours.
- Premium Website Scanner credits purchased with $VIBE under the launch scan pack configuration.
- CA Inspector for public Solana metadata, token and X image AI signals, and linked website vibe checks.

Near Term Priorities

- Expand and version the builder fingerprint registry.
- Publish calibration results and improve confidence explanations.
- Add scan provenance fields, engine versions, and source availability summaries.
- Implement owner correction and evidence submission workflows.
- Publish treasury, token parameter, privacy, and failed scan credit policies.

Later Product Options

- Historical report comparison to show how a public project changes over time.
- API access for developers and research teams.
- Community submitted fingerprints with review, versioning, and abuse controls.
- Additional project metadata modules only after their scope and limitations are documented.

The roadmap intentionally does not assign delivery dates. Features should be announced as committed only after the required data sources, security review, and operating capacity are confirmed.

14 Success Measures

Area	Measures
Detection quality	Verified false positives, verified false negatives, confidence calibration, evidence coverage
Report usefulness	Completion rate, repeat use, shared reports, correction rate, user comprehension
Reliability	Scan success rate, source failure rate, latency, queue time, uptime
Security	Blocked unsafe URL attempts, payment replay rejection, abuse rate, incident count
Token utility	Premium pack purchases, credit utilization, premium repeat rate, payment verification success
Responsible use	Correction response time, disputed report resolution, privacy requests, policy compliance

VibeCheck should publish targets only after a baseline period produces enough data to set meaningful thresholds. A high scan count alone is not a quality measure. Accuracy, evidence coverage, reliability, and correction handling matter more.

15 Conclusion

VibeCheck provides an explainable inspection layer for public websites and Solana token project assets. The Website Scanner looks for builder, technology, and AI assistance signals. CA Inspector connects public token metadata, project imagery, and the linked website in one report. Both products keep uncertainty visible and avoid treating appearance as proof.

$VIBE has a defined product role through premium Website Scanner credits. The launch configuration offers 10 premium credits for 1,000,000 $VIBE, while CA Inspector remains free and consumes no credits. This utility does not imply investment rights or future value.

The next disclosure obligations are concrete: publish the official mint and treasury details, define supply and allocation, document failed scan credit handling, release methodology benchmarks, and maintain a correction process. Completing those items will make the product and token model easier to evaluate on their actual operation.

Appendix A Report Data Model

Field	Description
input	Normalized public URL or Solana contract address
scan type	Basic website, premium website, or CA Inspector
timestamp	Time the scan was accepted or completed
engine version	Version of the fingerprint and scoring logic
likelihood	AI assistance estimate when supported by the scan
confidence	Low, medium, or high confidence label
possible builder	Builder or platform suggested by public evidence
technologies	Detected frameworks, hosting, and public technology indicators
evidence	Signal, explanation, source, and strength for each finding
limitations	Missing sources, conflicts, and reasons the result may be incomplete
sources queried	Public pages, metadata, and media sources attempted
credit charge	Whether the scan used a premium credit

Appendix B Launch Parameter Registry

Parameter	Launch value	Change rule
Basic Website Scan allowance	1 per connected wallet per rolling 24 hours	Prospective notice

Parameter	Launch value	Change rule
Premium scan pack price	1,000,000 $VIBE	Prospective notice and checkout display
Premium credits per pack	10	Prospective notice and checkout display
Premium credit use	1 credit per premium scan	Prospective notice
Premium page coverage	Homepage plus up to four same origin pages	May vary with source availability and safety limits
CA Inspector price	Free	Prospective notice
CA Inspector credit use	No scan credits	Prospective notice

Appendix C Glossary

Term	Definition
AI assistance signal	An observable feature associated with AI generated or AI assisted content. It is not proof of origin.
Builder fingerprint	A public technical marker associated with a website builder, framework, hosting platform, or deployment process.
CA	Contract address. In this paper it refers to a public Solana token address submitted to CA Inspector.
Confidence	The system's estimate of how strongly and consistently the available evidence supports a classification.
Evidence strength	A direct, technical, corroborating, or heuristic rating assigned to an individual signal.
Premium scan credit	A service access unit consumed by one premium Website Scanner report.
Rolling 24 hour period	A 24 hour interval measured from the wallet's prior free scan, rather than a calendar day reset.
Vibe coded	Informal product language for a website built or substantially assisted through prompt driven or AI enabled development tools.