MASTR

ONCHAIN INVESTIGATIONS, WEB3 KNOWLEDGE & PROTECTION

ANTI-SCAM | ANTI-LIES | ANTI-FRAUD

RESEARCH | DETECTION | DEBUNKING | WEB3 KNOWLEDGE

MASTR ECOSYSTEM DOCUMENT

GREENPAPER

SECURITY INFRASTRUCTURE FOR A TRUST-ABUSED MARKET

Independent onchain intelligence, responsible security research, practical protection tools, knowledge and an economic layer built to fund evidence rather than manufacture certainty.

VERSION 1.0

28 AUGUST 2026 | MASTRLABS.COM

00 / DOCUMENT CONTROL

Status, purpose and reading rules

The GREENPAPER replaces the 2024 Whitepaper as the primary public description of the MASTR ecosystem. It preserves the original mission while separating deployed systems, selective programmes, private development, historical concepts and future work.

Field	Current record
Document	MASTR GREENPAPER
Version	1.0
Publication date	28 August 2026
Owner	MASTR
Public domain	mastrlabs.com
Supersedes	MASTR Whitepaper V5 dated 24 November 2024
Review trigger	Material product, token, legal, security or programme-status change

Status language

A serious ecosystem document must distinguish reality from intention. Every major MASTR component therefore carries a status label. These labels are operational controls, not marketing decoration.

Label	Meaning
LIVE	Publicly available production product or service.
ACTIVE	Work is currently performed and can be scoped or used.
SELECTIVE	Available only after review, acceptance or defined conditions.
PUBLIC REGISTER	Published record that can be inspected; not a guarantee of future safety.
IN DEVELOPMENT	Implemented or being built, but not represented as a completed public release.
PRIVATE ALPHA	Internal or invited testing. No public availability or reliance claim.
FRAMEWORK	A documented model that is not an active binding service.
HISTORICAL	A former plan or allocation preserved for transparency, not current terms.

CONTROL RULE

If this document conflicts with a current product release, binding product terms, a verified onchain record or a later official MASTR notice, the more specific and more recent verified source takes precedence. Screenshots, shortened addresses and third-party summaries are not authoritative.

01 / INTRODUCTION

Why a GREENPAPER

The original Whitepaper described an ambitious anti-scam ecosystem before most of its present products, methods and operating evidence existed. Two years later, the correct document is not a larger promise. It is a stricter account of what MASTR is, what it does, how it decides, where the token belongs and what remains unfinished.

The word GREENPAPER reflects the MASTR identity, but the change is substantive. Green is the colour of the brand and the signal for verified progress. It is not permission to disguise uncertainty. The document therefore treats evidence, status and boundaries as first-class architecture.

The 2024 foundation remains intact: protect users from fraud, preserve autonomy, build practical security tools, improve knowledge and create a durable role for $MASTR inside the ecosystem. What changes is the precision. Insurance is described as a framework until binding terms, reserves and claims administration exist. A badge is a point-in-time assessment, not a permanent safety certificate. Artificial intelligence accelerates collection but does not own conclusions. Security claims are tied to reproducible tests, explicit limits and independent retesting.

This paper is written for community members, users, technical reviewers, project teams, partners and counterparties. It is deliberately direct about the limits of MASTR because credibility is not created by claiming that every component is live. Credibility is created by publishing what can be verified and refusing to sell the gap between the two.

CORE THESIS

Crypto does not suffer from a shortage of opinions. It suffers from hidden incentives, unverifiable interfaces, concentrated control and marketing claims that outrun the systems beneath them. MASTR exists to force evidence back into that gap.

What this document does

- Defines the present MASTR ecosystem and the role of each component.
- Separates deployed capabilities from selective, development, framework and historical states.
- Documents the research, security, privacy and responsible-disclosure standards used by MASTR.
- Places $MASTR inside the ecosystem without pretending that ownership is a security verdict or guaranteed return.
- Preserves the 2024 allocation model as project history while refusing to mislabel it as current onchain tokenomics.
- Sets measurable conditions for future products, badge reassessment and any protection programme.

Contents

02 / EXECUTIVE SUMMARY

MASTR in one page

MASTR is an independent Web3 security ecosystem built around onchain investigations, external security assessments, scam prevention, public knowledge, practical applications and a token layer intended to align participation with useful work.

30,000+	8,000+	3	1
PUBLIC COMMUNITY	TOKEN CHECKS	APP WORLDS	SECURITY STANDARD
Public audience built without paid KOL distribution.	Historical lifetime checks through August 2026.	Community app, MASTRpass and classified MASTRful.	Evidence, scope, disclosure and retesting.

The ecosystem is organised in 4 connected layers. The intelligence layer investigates wallets, supply, authority, interfaces, signatures and operational trust. The verification layer turns findings into scoped assessments, badges, registers and remediation decisions. The product layer delivers access through AskMASTR, the live mobile community app, MASTRpass, MASTRful and MASTR Knowledge. The economic layer gives $MASTR a role in access, participation and long-term alignment without allowing token ownership to purchase a positive conclusion.

The central operating rule is simple: a finding must survive scrutiny. MASTR records the affected boundary, the test method, the evidence, the impact, the limits and the remediation required. A Critical or High issue remains open until the underlying control changes and an independent retest closes the original and adjacent paths.

MASTR does not sell paid certainty. A project may pay for a defined investigation, but payment buys the work and agreed outputs. It cannot buy a clean report, a badge, silence or immunity from public warning when user protection requires disclosure. The same separation applies to $MASTR. The token can align participation with the ecosystem, but it does not govern the truth of a security result.

Current ecosystem snapshot

Component	Status	Function
MASTR Security	ACTIVE	External assessments, bug-bounty research, responsible disclosure and retesting.
Onchain Intelligence	ACTIVE	Wallet networks, authority, supply, treasury and money-flow analysis.
AskMASTR	LIVE / EVOLVING	Accessible token checks, Web3 answers and risk intelligence.
$MASTR community app	LIVE	Android and iOS community, learning, alerts, token checks, wallet and reward functions.
MASTRpass	IN DEVELOPMENT	Offline encrypted vault and local security toolkit across 4 platform tracks.
MASTRful	PRIVATE ALPHA	Classified product research. No public feature or utility commitment.
MASTR Knowledge	ONGOING	Structured public security knowledge and research method.
MASTR Badge	SELECTIVE	Point-in-time human review signal with reassessment and withdrawal conditions.
Verified Projects	PUBLIC REGISTER	Published project records, links, contracts and review context.
MASTR Insurance	FRAMEWORK	Historical protection model; not an active regulated insurance policy.
$MASTR	LIVE ECOSYSTEM TOKEN	Solana-based economic alignment layer; not a security guarantee.

03 / EVOLUTION

From the 2024 Whitepaper to the 2026 operating model

The original document is preserved as the project's historical starting point. The GREENPAPER retains the mission and ecosystem identity while correcting claims that were too broad, too early or no longer accurate.

2024 statement or concept	2026 treatment
App as a single centre of the ecosystem	Expanded into a portfolio: live community apps, AskMASTR, MASTRpass, MASTRful and MASTR Knowledge.
Badge as a symbol of trust	Defined as a scoped, dated and revocable point-in-time assessment, never a guarantee.
Insurance as an available safety net	Reclassified as a framework until legal entity, reserves, binding terms, limits and claims administration are published.
AI predicts fraud and provides real-time monitoring	AI assists collection and triage. Human review owns conclusions; live monitoring is claimed only where a specific product actually performs it.
HSM, MFA and E2EE as platform-wide controls	Applied only to products where architecture and verification support the claim. MASTRpass is documented separately from the networked community app.
Base and Solana integration	Current $MASTR economic layer is documented on Solana. Other chains are research targets or supported data profiles, not proof of token deployment.
12-person team allocation	Kept only inside the archived 2024 distribution model. Current governance is described by actual decision rights, not an unverified headcount.
Influencer partnerships as a growth strategy	Replaced by an explicit no-paid-shill rule and organic evidence-led distribution.
Fixed future roadmap dates	Replaced by release gates, measurable readiness conditions and status-led updates.

PRESERVED FOUNDATION

The anti-scam mission, educational purpose, Badge concept, protection ambition, app ecosystem and $MASTR utility thesis remain part of MASTR. The GREENPAPER strengthens them by removing false certainty and making each claim testable.

Why the correction matters

Security language is cheap when it is not tied to a boundary. A project can say 'audited' while an upgrade key can replace the code, say 'non-custodial' while a backend can construct unsafe transactions, or say 'private' while telemetry records sensitive behaviour. The same failure can happen in a whitepaper: broad labels create an impression that the evidence does not support. MASTR cannot criticise that behaviour elsewhere and repeat it in its own documentation.

This document therefore treats accuracy as part of the product. Where a capability is implemented, the paper states the scope and limit. Where it is planned, it states the gate. Where a former plan remains useful as history, it is archived rather than erased. This is harder than hype and far more valuable.

04 / PROBLEM LANDSCAPE

The market's failure is structural

Scams are not an isolated category of bad token. They are the visible result of broken incentives, weak engineering, concentrated authority, social manipulation and users being asked to trust interfaces they cannot verify.

A modern Web3 attack often crosses several layers. A public account manufactures urgency. A website renders untrusted content inside a trusted interface. A wallet request hides the affected account or authority. A backend expands one request into hundreds of expensive operations. An upgrade key remains capable of replacing the rules after an audit. None of these failures is solved by checking a contract name or displaying a green badge.

MASTR divides the problem into 6 risk domains so that evidence can be collected against the actual boundary.

Risk domain	Typical failure	Required evidence
Influence and narrative	Paid promotion, undisclosed allocation, insider positioning, fake consensus.	Funding, timing, wallet links, disclosures and repeated behaviour.
Onchain control	Mutable programmes, single upgrade authority, treasury concentration, privileged routes.	Deployed state, authorities, multisig thresholds, upgrade history and simulations.
Wallet and signing	Blind signatures, weak account binding, unsafe transaction construction, key exposure.	Exact message or transaction, affected account, signer scope and reproducible path.
Application and API	Auth failures, unsafe rendering, exposed secrets, amplification, CORS and session errors.	Requests, responses, code paths, environment boundaries and controlled proof.
Token and market structure	Supply concentration, bundled holders, liquidity control, wash activity and exit design.	Holder clusters, funding sources, liquidity ownership and flow history.
Operational and supply chain	Weak deployment controls, unsigned builds, compromised dependencies and domain exposure.	Build provenance, signing, DNS, CI/CD boundaries and privileged access design.

The verification gap

Retail users are routinely shown a simplified surface while the decisive control lives elsewhere. A decentralised interface may depend on a central sequencer. A verified token may retain freeze or mint authority. A reviewed contract may be replaceable by one key. A non-custodial app may still decide what the wallet sees and signs. A KOL may disclose a partnership but not the timing, price, side agreement or exit. MASTR's work begins where the marketing sentence ends.

DESIGN REQUIREMENT

Protection must combine technical inspection, onchain context, human incentive analysis and clear communication. Any one of these without the others leaves a predictable blind spot.

05 / MISSION

Vision, mission and non-negotiable principles

MASTR exists to make exploitation harder, evidence easier to access and security claims more expensive to fake.

Vision

A crypto ecosystem in which users can inspect the real controls behind a claim before they connect, sign, invest or amplify it. MASTR does not promise a market without loss. It works toward a market where avoidable loss is not normalised by opacity, paid influence and weak engineering.

Mission

Build an independent security and knowledge ecosystem that combines human-led investigations, reproducible technical evidence, responsible disclosure, practical applications and a sustainable economic layer. Every component should reduce the distance between what users are told and what the system can actually do.

Operating principles

Principle	Operational meaning
Evidence before trust	Claims are tested against contracts, wallets, code, interfaces, permissions and history.
Human accountability	Automation can collect and rank. A human owns impact, limits and the final conclusion.
No paid verdicts	Commercial work never purchases a clean outcome, badge, silence or public endorsement.
Responsible disclosure	Exploitable details remain private while reasonable remediation is possible.
Retest before closure	A promise, screenshot or changed label is not remediation. The original path must fail after the control change.
Status over theatre	Live, selective, development, framework and historical states remain visibly distinct.
Minimum necessary data	Products should collect, retain and expose only what their function requires.
No fake decentralisation	Central operators, keys, validators, sequencers and fallback controls are documented plainly.
No KOL machinery	MASTR does not rent credibility from paid shillers or disguise distribution as conviction.
Challenge is allowed	Findings, methods and limits should be clear enough for another reviewer to dispute and reproduce.

Preserving autonomy without protecting incompetence

The original mission linked security with financial autonomy and resistance to unnecessary central control. That remains valid, but autonomy is not a defence for undisclosed privilege, unsafe code or deliberately misleading interfaces. Decentralisation language cannot excuse a single upgrade key, and freedom language cannot excuse retail extraction. MASTR protects the right to participate by exposing the control that participation actually depends on.

06 / ARCHITECTURE

One mission, 4 connected layers

The MASTR ecosystem is not a collection of unrelated apps around a token. It is a security system in which intelligence, verification, products and economic alignment serve separate functions and constrain one another.

INTELLIGENCE

Onchain investigations | Security research | Threat detection

VERIFICATION

Human review | MASTR Badge | Verified register | Retesting

PRODUCTS

AskMASTR | Community apps | MASTRpass | MASTRful | Knowledge

ECONOMIC ALIGNMENT

$MASTR utility | Product access | Participation | Long-term funding

Layer 1: intelligence

MASTR Security and Onchain Intelligence inspect application behaviour, wallet and signing flows, smart-contract control, supply, liquidity, infrastructure, claims and incentives to produce a defensible evidence base.

Layer 2: verification

Findings enter a dated and scoped decision system: report, severity, disclosure, remediation, retest, badge, register or public warning. Status can expire, be suspended or be withdrawn.

Layer 3: products and access

AskMASTR, the community app, MASTRpass, MASTRful and MASTR Knowledge translate research into protection, learning and workflow. Each retains its own status, data model and trust boundary.

Layer 4: economic alignment

$MASTR aligns participation, product access, ecosystem activity and long-term funding. It cannot override the intelligence layer, change a finding or purchase a positive decision.

ARCHITECTURE RULE

The economic layer supports the security system. It does not sit above it.

07 / INTELLIGENCE

Onchain investigations and adversarial research

MASTR investigates the control behind the claim: who can change the rules, who funded the wallets, where the supply is concentrated, what the interface asks users to approve and which failure path can move real value.

Onchain analysis

Holder concentration, wallet clustering and common funding sources.

Deployer history, programme upgrade authority, mint and freeze authority, treasury control and multisig design.

Liquidity creation, ownership, lock or burn status, migration paths and abnormal withdrawal patterns.

Privileged instructions, parameter changes, operator actions and relationships between public claims and deployed state.

Money flows connecting insiders, promoters, market makers, treasury wallets and exit liquidity.

Application and product analysis

Wallet connection, transaction construction, signature binding, trusted rendering and consent boundaries.

Web, API, authentication, sessions, CORS, security headers, DNS, TLS, email posture and exposed secrets.

Backend amplification, unsafe input handling, insecure defaults, environment confusion and production/testnet separation.

Mobile packages, permissions, signing, embedded endpoints, data storage and build provenance where scope permits.

Operational authority, dependency and deployment paths that can invalidate a narrow code audit.

Evidence levels

Label	Meaning	Use
CONFIRMED	Reproduced live, decoded from current state, proven by controlled simulation or directly visible in deployed artefacts.	Can support a firm finding within stated scope.
INFERRED	Strongly supported by confirmed architecture but dependent on an unavailable implementation detail.	Supports risk analysis with explicit qualification.
OPEN	Cannot be resolved without source, privileged access, internal logs or a dedicated stateful test environment.	Remains a question or required verification step.

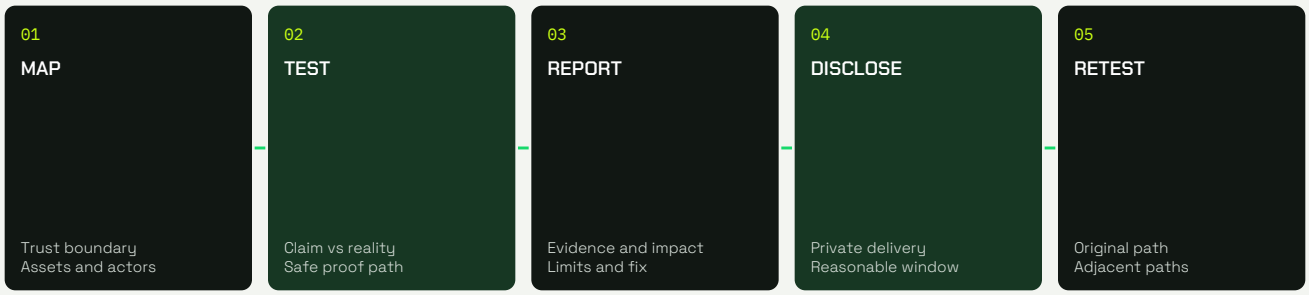
RESEARCH LIMIT

An external assessment can establish serious risk, but it cannot prove the absence of hidden code, compromised infrastructure or privileged behaviour outside the inspected surface. Reports state that limit instead of hiding it.

08 / SECURITY STANDARD

Assessment, disclosure and remediation

A finding is useful only if another competent reviewer can understand the boundary, reproduce the evidence and determine whether the control changed.



Required finding structure

1. Identify the affected asset, user, account, wallet, contract, service or trust boundary.
2. State the exact preconditions and the least privilege required to reproduce the issue.
3. Provide reproducible evidence, a safe proof of concept or a controlled simulation.
4. Describe realistic impact without inflating worst-case speculation into confirmed loss.
5. Separate confirmed facts, strong inference and unresolved questions.
6. Name the root cause and the control that must change.
7. Retest the original path and equivalent paths after remediation.

Severity and release gates

Severity	Typical meaning	Closure standard
CRITICAL	Direct or near-direct path to systemic asset loss, key compromise, arbitrary privileged action or catastrophic trust failure.	Root cause removed, production path closed, adjacent systems checked and independent retest documented.
HIGH	Material loss, account or authority compromise, unsafe signing, broad exploitation or major control failure.	Same retest standard as Critical. Interface warnings alone are insufficient.
MEDIUM	Meaningful weakness requiring conditions, chaining or limited scope, but still capable of harming users or reliability.	Fix verified against the stated scenario and regression risk.
LOW	Limited impact, hardening gap or localised weakness.	Change verified where practical; remaining acceptance documented.
OBSERVATION	Assurance limit, architectural concern or improvement without a confirmed exploitable path.	Decision and rationale recorded.

NO VULNERABILITY THEATRE

MASTR does not perform reckless production exploitation, move real funds, create avoidable service load or disclose weaponised detail for engagement. Safe evidence is stronger than a dramatic screenshot.

09 / ASKMASTR

Fast checks with visible limits

AskMASTR is the accessible intelligence entry point: a Telegram AI agent and token-scanner experience that helps users collect warning signals, ask Web3 questions and decide when deeper human review is justified.

AskMASTR reduces the cost of a first look. Automated checks can surface contract metadata, holder or liquidity concerns, suspicious configuration, common scam patterns and relevant context. They are useful because many users otherwise act with no structured review at all.

The scanner does not convert uncertain data into certainty. Chain data can be incomplete, token standards differ, labels are wrong, proxy and upgrade paths complicate interpretation and a clean automated result cannot prove honest operators. The system therefore belongs upstream of a human conclusion, not in place of one.

Decision layers

Layer	Purpose	Output
Automated collection	Retrieve structured token, wallet, contract and public-source signals.	Machine-readable facts and flags.
Rule and model triage	Prioritise abnormal patterns, missing controls and known attack indicators.	Risk hypotheses, not verdicts.
Human Coin Check	Review context, incentives, control and contradictory evidence.	Focused human assessment.
Deep Project Check	Expand into multi-source investigation and documented decision.	Branded evidence report and risk register.

Design commitments

- Show confidence and missing data rather than only a single score.
- Keep automated flags traceable to their underlying input where possible.
- Do not describe absence of a detected signal as proof of safety.
- Escalate authority, signing, wallet-cluster and insider questions to human review.
- Separate educational content from financial instruction.
- Measure whether a check changes user behaviour, not only how many checks are run.

[illegible]	[illegible]	[illegible]
HISTORICAL CHECKS	TELEGRAM ENTRY	FINAL ACCOUNTABILITY
Lifetime public figure through August 2026.	Official @askmastrbot access point.	Models assist; reviewers conclude.

10 / LIVE APPLICATION

The $MASTR community app

The official Android and iOS app is the connected community product. It combines token and scam checks, security information, learning, conversations, wallet interaction and server-controlled rewards. It is operationally separate from MASTRpass.

Capability	Current role	Boundary
Token and scam checks	Inspect tokens and warning signals before independent action.	Informational; cannot prove safety or replace due diligence.
Security, learning and alerts	Deliver warnings, educational context and push notifications.	Networked content can become stale and must cite current evidence.
Chat and conversations	Community exchange, questions and project context.	User-generated content is not a MASTR verdict.
Solana wallet connection	Mobile Wallet Adapter for supported wallet and reward flows.	Wallet shows and authorises final transaction; every request must be inspected.
Daily rewards	Mining or reward-claim routines under server-side rules.	Eligibility and reward state are not decentralised guarantees.
MASTR badges	Visible participation and achievement features.	In-app achievements must not be confused with project security verification.
Human Coin Checks	Route users from automated information to manual review.	Scope and output must be agreed before reliance.

Product separation

$MASTR APP IS NOT MASTRPASS

The community app is a connected product with accounts, messaging, purchases, subscriptions and service data. MASTRpass is an offline encrypted vault with no MASTR account, cloud, backend or telemetry. Neither product should inherit the other's claims.

Historical operating snapshot

Public records through August 2026 describe approximately 1,000 cumulative app downloads, approximately 400 active users, more than 8,000 lifetime token checks and 11 paying subscribers. These figures are dated operating snapshots, not live counters or promises of future activity.

Privacy boundary

The networked app may process account, messaging, device, diagnostic, purchase and subscription data required for its functions and uses platform or cloud service providers. Users must never submit private keys, seed phrases, passwords or financial credentials. The offline-vault privacy model cannot be used to describe this product.

11 / MASTRPASS

Offline vault, explicit threat model

MASTRpass is being built as a local encrypted vault for passwords, recovery phrases, TOTP, recovery codes, secure notes and encrypted attachments, with local inspection and recovery tools. It is not a wallet and does not sign or broadcast blockchain transactions.

The product is deliberately separated from MASTR services. It requires no MASTR account or $MASTR holding and is designed without a backend, cloud, telemetry, ads, trackers, WebView or recovery backdoor. Android builds do not request the INTERNET permission. Current Windows provenance records describe no network API and an AppContainer profile without capabilities.

Security model

Control	Design
Key derivation	Argon2id for password-based derivation.
Vault encryption	XChaCha20-Poly1305 authenticated encryption.
Key mixing	HKDF-SHA-256.
Companion store	AES-256-GCM where the platform design requires a separate protected store.
Access	Master password plus recovery key for portable manual access; optional biometrics or Windows Hello after local enrolment.
Core	Shared Rust cryptography core with compatible encrypted vault and bundle formats.
Data location	Local private app area; encrypted export only on deliberate user action.
Recovery	No support bypass. Loss of required credentials can make the vault unrecoverable.

Capability groups

Organisation: folders, tags, favourites, expiry dates, trash, versions, search, filters and batch actions.

Migration: structured imports with masked preview, duplicate detection and completion reporting before data is written.

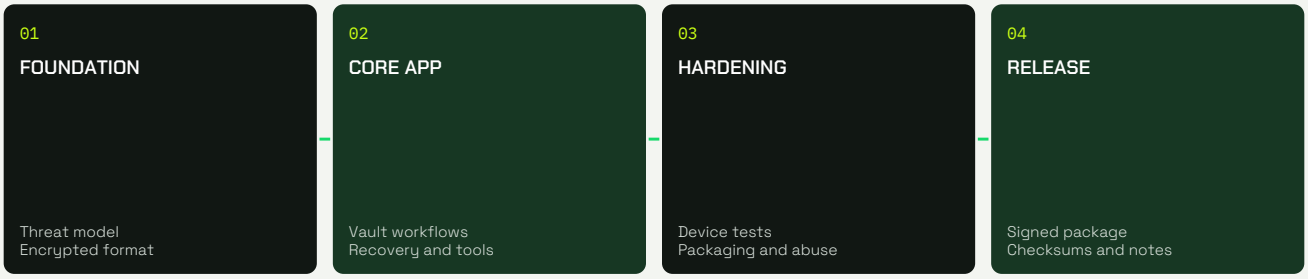
Backup: encrypted exports, integrity checks, guided recovery tests and multiple local backup generations.

Security Center: local detection of weak, reused, similar or old passwords, missing recovery data and overdue backups.

Offline inspection: URL, QR, Unicode, Punycode, IP, wallet-address, selected transaction, hash, signature, certificate, JWT and file analysis with explicit limits.

Platform tracks: Android / Solana Seeker, iOS / iPadOS, Windows and macOS with feature and release-stage differences.

Release model



Platform	Public status	Current engineering stage
Android / Solana Seeker	COMING SOON	Device and security validation; no INTERNET permission.
iOS / iPadOS	COMING SOON	Native implementation and platform integration.
Windows	COMING SOON	Security hardening, recovery testing and release packaging.
macOS	COMING SOON	Foundation planning and shared-core integration.

CURRENT LIMIT

MASTRpass remains pre-release and has not completed an independent external audit. Alpha and Security Beta builds must never be the only backup or the sole protection for high-value wallets. Local encryption reduces specific risks; it does not make a compromised device trustworthy.

Threats MASTRpass can reduce

Plaintext screenshots, unencrypted note files and uncontrolled cloud copies.

Password reuse, missing recovery information and forgotten backup testing.

Accidental exposure through clipboard, screen capture and weak local organisation.

Some structural risks in URLs, QR codes, addresses, signatures and files that can be inspected offline.

Threats it cannot eliminate

Compromised operating systems, malicious keyboards, physical coercion and unknown platform exploits.

Loss of all encrypted backups or loss of the master password and recovery key.

Current onchain state, revocation data, reputation or malware intelligence when the tool is offline.

Bad investment decisions, malicious smart contracts or signatures authorised outside the vault.

12 / MASTRFUL

Private alpha without public theatre

MASTRful is a classified MASTR Labs application in private alpha. Its existence is acknowledged; its product details, release date and economic role are not committed in this GREENPAPER.

The correct treatment of an unreleased product is restraint. Internal builds prove that engineering activity exists, but they do not create a public feature promise, a security claim or a $MASTR utility. Until MASTR publishes a product specification and release path, MASTRful remains outside the live ecosystem contract.

Publication gates

1. Define the user problem and publish what data the product processes.
2. Document its trust boundary, permissions, storage model and network behaviour.
3. Separate implemented features from concepts and future ideas.
4. Complete platform testing, package verification, signing and release provenance.
5. Publish security limits, privacy terms and a vulnerability-reporting route.
6. Define whether any $MASTR access or participation role exists. No implied utility is created before that decision is public.

STATUS

PRIVATE ALPHA. No public availability. No promised release date. No token utility attached. No security or privacy claim beyond evidence published with a future release.

Why secrecy and transparency can coexist

A team can keep product strategy private without misleading users. The line is simple: do not solicit reliance, capital, sensitive data or promotional certainty for features that have not been published and verified. MASTRful can remain classified while the ecosystem remains honest about its status.

13 / KNOWLEDGE

MASTR Knowledge turns incidents into prevention

Warnings disappear quickly in social feeds. MASTR Knowledge converts investigations, recurring failure patterns and security practice into structured material that users can revisit before the next incident.

The knowledge layer is not generic crypto education. Its purpose is to expose the incentive and control failures that ordinary tutorials skip: why KOL promotion creates negative selection, how upgrade authority changes an audit conclusion, how wallet prompts hide authority, how fake support accounts exploit urgency and why a tokenised claim may not be legally enforceable.

Knowledge domains

Domain	Questions answered
Wallet security	What is being signed, which account is affected, what authority is granted and how can it be revoked?
Tokens and memecoins	Who controls supply and liquidity, how are top wallets related and who becomes exit liquidity?
DeFi and protocols	Which operator, oracle, sequencer, upgrade key or backend still determines the outcome?
Exchanges and counterparties	What custody, withdrawal, listing, solvency and legal-enforcement risks remain?
KOL incentives	What was paid, allocated, timed, undisclosed or sold into followers?
Scams and social engineering	Which urgency, impersonation, domain, approval or recovery pattern is being exploited?
Responsible disclosure	How can evidence be collected and reported without creating avoidable harm?
MASTR method	How are evidence levels, severity, scope, limits, remediation and retesting documented?

Education standard

- Explain mechanisms and consequences, not only labels.
- Use concrete examples while avoiding live exploit detail that creates unnecessary risk.
- Date facts that can change and distinguish historical evidence from current state.
- Link users to the primary contract, policy, code, transaction or official statement where possible.
- Make uncertainty visible and correct material errors publicly.
- Measure comprehension and safer behaviour, not only impressions.

14 / VERIFICATION

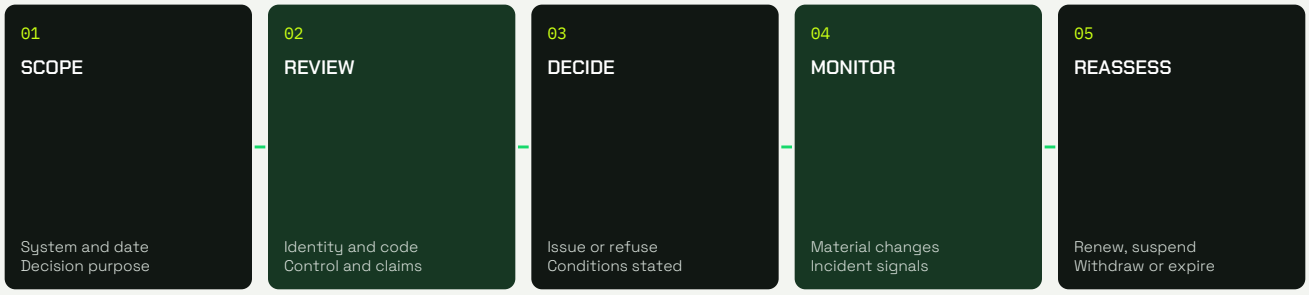
MASTR Badge and Verified Projects

The MASTR Badge is a selective human review signal tied to a defined scope, reviewed state and decision date. It is not a lifetime certificate, insurance guarantee or investment endorsement.

Assessment dimensions

Dimension	Minimum review questions
Ownership and identity	Who controls official channels, deployers, repositories, domains and responsible contacts?
Technical and onchain	What can contracts, authorities, treasuries, mints, interfaces and privileged operators do?
Market structure	How concentrated are supply and liquidity, how are major wallets related and what exit risks exist?
Claim verification	Do public promises match deployed permissions, delivered products and operating evidence?
Operational security	How are privileged actions, upgrades, keys, releases and incidents controlled?
Remediation	Were material findings fixed at the root and independently retested?

Badge lifecycle



Withdrawal triggers

- Material contract, authority, liquidity, treasury, team or product change outside the reviewed state.
- New Critical or High finding that remains unresolved.
- False or materially incomplete information supplied during review.
- Loss of access to responsible contacts or required reassessment evidence.
- Misuse of the Badge as a guarantee, insurance policy or blanket endorsement.

COMMERCIAL SEPARATION

A project may pay for the defined review effort. Payment never guarantees acceptance, badge issuance, renewal or a positive public statement.

Verified Projects register

The public register exists so users can inspect which project was reviewed, when, against what scope and through which official links and contracts. Six project entries were publicly listed as of the document date. Their presence is a record of MASTR publication, not a direction to buy or an assurance that the present state remains unchanged.

Published entry	Ticker	Status treatment
Popdog	$POPDOG	Published register entry; point-in-time context required.
Catown Kimono	$COK	Published register entry; point-in-time context required.
Odin	$ODIN	Published register entry; point-in-time context required.
Lou	$LOU	Published register entry; point-in-time context required.
JFK	$JFK	Published register entry; point-in-time context required.
Free Ross Now	$FRN	Published register entry; point-in-time context required.

USER RULE

Always verify the current register entry, official destination, full contract address, chain and date before interacting. Logos, tickers and old screenshots are easy to copy.

What the Badge cannot prove

That every future code, key, team, liquidity or treasury change will be safe.

That a token price will rise, remain liquid or avoid manipulation.

That undisclosed infrastructure, insider agreements or future compromises do not exist.

That the project complies with every jurisdiction or that every holder can enforce a legal claim.

That users can stop verifying transactions, permissions and official channels.

15 / $MASTR

The economic layer belongs inside the security system

$MASTR is the Solana-based ecosystem token intended to align access, participation, product activity and long-term support for the MASTR mission. It is not a security verdict and does not give holders the right to alter findings.

Reference	Value
Network	Solana
Published mint reference	96sQs3ooHRAsVuonoyoErynmqRVcdo9sAdUd32RWhvVq
Launch history	Project launch in November 2024; archived Whitepaper dated 24 November 2024.
Role	Economic alignment across MASTR products, access, participation and longer-term protection design.
Not a role	A safety guarantee, ownership of research conclusions, legal claim on revenue, insurance policy or promise of return.

Utility principles

Utility area	Permitted direction	Required condition
Security access	Token-linked access or benefits for checks, reports, education or protection features.	Current product terms define the actual benefit.
Participation	App activity, learning, community contribution or defined reward routines.	Rules, eligibility and server or onchain control are disclosed.
Ecosystem alignment	Products and services reinforce one security mission instead of isolated speculation.	Revenue and access decisions cannot change findings.
Protection eligibility	The historical framework used continuous holdings as one possible eligibility input.	No current coverage until binding programme terms exist.
Governance	Consultation or future voting can be designed for non-security decisions.	Token holders cannot vote a vulnerability away or purchase a badge.

Static-address risk

Contract addresses are a common substitution target. The full 44-character Solana mint is reproduced here as a dated reference, but users must still compare it against the current official MASTR link route and an independent explorer. Any shortened, ellipsised or malformed address is invalid for transaction use.

NO IMPLIED RETURN

Token utility is a use model, not a promise that demand, price, liquidity or access will increase. Market outcomes remain exposed to volatility, concentration, platform risk, regulation and execution.

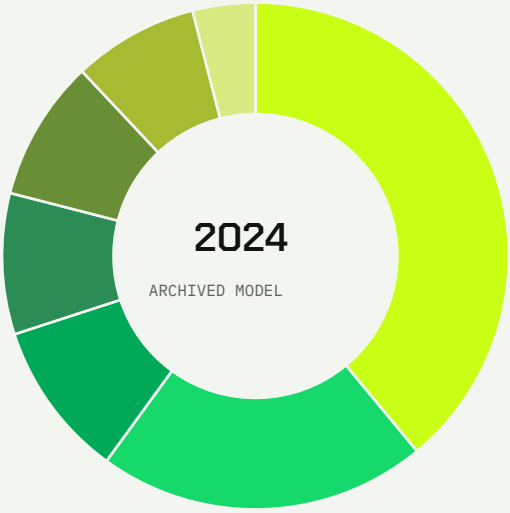
16 / TOKEN HISTORY

Archived 2024 distribution model

The allocation below is preserved because deleting old promises is not transparency. It describes the plan published in the 2024 Whitepaper. It is not presented as current wallet distribution, circulating supply, treasury balance, vesting state or a new offer.

STATUS

HISTORICAL MODEL. Current onchain data and later official records take precedence. No reader should treat the chart as today's circulating distribution.



39% Presale
21% Liquidity
10% Team
9% Marketing
9% App development
8% CEX listing
4% Airdrop

Allocation	Share	2024 stated purpose
Presale	39%	Early distribution; unsold tokens were described as locked for the planned insurance pool.
Liquidity	21%	Trading liquidity and market access.
Team	10%	Long-term team incentive under the former model.
Marketing	9%	Project awareness and community growth.
App development	9%	Mobile-app development and upgrades.
CEX listing	8%	Potential centralised-exchange listing activity.
Airdrop	4%	Promotional distribution and engagement.

What must be published for current tokenomics

Current supply, decimals, mint and freeze authority status.

Circulating methodology and wallet-level allocation mapping.

Treasury, team, liquidity, rewards and development balances.

Vesting, lock, multisig and authority controls with verifiable addresses.

Material transfers, burns, migrations or reclassifications since the 2024 model, with a dated reconciliation of every difference between plan and onchain state.

17 / ECONOMIC MODEL

Fund useful work without selling the conclusion

MASTR requires sustainable revenue for research, infrastructure, product development, testing and public knowledge. The economic model must finance that work while preventing the payer from controlling the result.

Current and intended revenue categories

Category	Examples	Conflict control
Fixed-scope intelligence	Token Risk Snapshot, Deep Project Check, Counterparty Intelligence and monitoring.	Scope and outputs agreed; positive conclusion not for sale.
Security programmes	Attack-surface review, wallet and signing security, full Web3 product assessment and remediation retest.	Severity and release decision remain reviewer-controlled.
App purchases and subscriptions	Platform-managed purchases for networked community features.	Product terms and data boundary remain separate from investigations.
Token-linked utility	Access, participation or benefits defined in current products.	No retroactive utility and no security result controlled by holdings.
Voluntary support	Community donations supporting independent work and development.	Creates no entitlement to returns, features, priority verdicts or silence.
Future protection fees	Premium or service fee only if a lawful, funded programme becomes active.	Reserves, claims administration, exclusions and legal responsibility published first.

Economic separation of duties

HARD RULE

Payment can change the amount of work performed. It cannot change the evidence found or the conclusion reached.

Use-of-funds priorities

Security research time, test infrastructure and reproducible evidence tooling.

MASTRpass hardening, platform validation, audit preparation, signing and release provenance.

AskMASTR signal quality, source traceability and human-review capacity.

Knowledge, translation, accessibility, legal, privacy and programme design required before any protection framework can become active.

18 / PROTECTION FRAMEWORK

MASTR Insurance remains a framework

The 2024 Whitepaper proposed rug-pull protection for eligible investments in MASTR-badged projects. That concept remains part of the long-term ecosystem vision, but it is not an active regulated insurance policy or guaranteed coverage.

Historical design

1. Only projects holding a valid MASTR Badge were intended to qualify.
2. Continuous $MASTR holdings from investment to claim were intended to form one coverage input.
3. The maximum basis was linked to the minimum eligible holding maintained during the relevant period.
4. Normal price decline, trading loss and events outside a defined rug-pull trigger were excluded.
5. The historical process described notification within 30 days, wallet-ownership verification and a case assessment.

Activation prerequisites

Requirement	Why it is mandatory
Responsible legal entity	Users must know who owes the obligation and which law governs it.
Regulatory analysis	Insurance, guarantee and protection products can require authorisation or specific structure.
Published reserves	Coverage without funded and verifiable capacity is marketing, not protection.
Binding terms	Trigger, eligible loss, limits, exclusions, valuation time and evidence must be unambiguous.
Claims administration	Independent intake, investigation, conflict handling, decision and appeal process.
Fraud controls	Wallet ownership, duplicate claims, collusion, manipulation and staged incidents must be addressed.
Risk concentration limits	One event, operator or correlated project cannot exhaust the pool without disclosed limits.
Audit and reporting	Reserve, claim and control reporting must be inspectable over time.

CURRENT PUBLIC STATUS

FRAMEWORK. Do not treat MASTR Insurance as active coverage until current binding terms, coverage limits, reserves, claims administration and the responsible entity are expressly published.

Why the Badge alone is insufficient

A security review reduces information asymmetry at a point in time. It cannot guarantee future behaviour, market liquidity, operator honesty or absence of compromise. A lawful protection product requires financial capacity and enforceable rules in addition to technical review. The GREENPAPER refuses to collapse those separate obligations into one logo.

19 / GOVERNANCE

Operator-led, evidence-constrained decision making

MASTR is not presented as a DAO. Current decisions are operator-led, with public methods, documented conflicts and security conclusions constrained by evidence rather than token voting.

Decision	Current authority	Constraint
Research conclusion	Assigned MASTR reviewer	Evidence, scope, reproducibility, limits and peer challenge.
Severity	MASTR Security	Demonstrated impact and realistic preconditions; not commercial preference.
Disclosure timing	MASTR Security with affected team input	User protection, remediation opportunity and exploitability.
Badge issue or withdrawal	MASTR review authority	Published scope, unresolved material findings and change state.
Product release	Product owner	Release gates, testing, signing, privacy and security limits.
Token utility	MASTR ecosystem owner	Published rules, product reality, legal review and conflict separation.
Knowledge correction	MASTR editorial owner	Source evidence, date and transparent material correction.
Future community consultation	Defined per proposal	Cannot override facts, security findings or legal duties.

Conflict controls

Record payment, token exposure, prior relationship and material personal interest before an assessment decision.

Do not assign a positive-verdict obligation to commercial scope.

Separate app engagement badges from project security verification.

Require another review where a conflict could reasonably alter severity or public status.

Publish material methodology changes and keep historical status records accessible.

Prevent $MASTR holders, clients, partners or community majorities from voting a technical fact into existence.

GOVERNANCE PRINCIPLE

Community input can help choose priorities. It cannot decide whether a private key was exposed, an authority is centralised or a signature is unsafe.

20 / SECURITY AND PRIVACY

Different products, different trust boundaries

The strongest privacy claim in one product must never be copied across the ecosystem. MASTRpass is offline. The community app is networked. AskMASTR depends on data sources and a messaging platform. Research engagements can contain confidential evidence. Each boundary requires its own controls.

Surface	Primary data	Core controls
MASTRpass	Local secrets, vault metadata, encrypted attachments and deliberate exports.	No account, backend, cloud, telemetry or Android INTERNET permission; authenticated encryption; local lock and recovery design.
Community app	Account, messaging, device, purchase, subscription and service data.	Platform authentication, access control, provider agreements, retention, deletion and secure wallet-consent flows.
AskMASTR	User questions, token identifiers, public chain and source data.	Minimum necessary retention, source separation, model limits and no submission of secrets.
Security research	Technical evidence, affected systems, contacts, PoCs and remediation records.	Need-to-know access, encrypted storage, private disclosure, redaction and controlled release.
Public register	Project identity, links, contracts, scope and status.	Full-address verification, dated entries, change records and withdrawal process.

Engineering baseline

Inventory every account, key, service, permission, data flow and third party before claiming a security boundary.

Use least privilege, multi-party control and documented emergency paths for material production authority.

Bind signatures and transactions to the affected account, chain, action and user-visible intent.

Treat HTML, token metadata, project content, remote configuration and model output as untrusted input.

Publish build provenance, hashes and owner-controlled signatures for security-sensitive releases.

Separate test, staging and production identifiers, endpoints, keys and user expectations.

Design logs and diagnostics so they help investigate incidents without becoming a second secret store.

Remove root causes, test adjacent paths and retain the evidence required for an honest closure decision.

Key management

Any key capable of upgrading code, moving treasury funds, rotating privileged state, changing verification records or signing releases is part of the security model. Such keys require an owner, purpose, storage design, rotation plan, recovery path, monitoring and ideally multi-party control. An undocumented single key can invalidate pages of decentralisation claims.

21 / AI AND DATA

Automation accelerates evidence; it does not own truth

MASTR uses automation and AI to collect, structure, compare and explain information. Human review remains responsible for impact, context, uncertainty and any conclusion that can materially affect users or projects.

Permitted uses

Extract structured indicators from public documents, transactions, contracts and interfaces.

Cluster related evidence and identify contradictions requiring human review.

Translate technical mechanisms into accessible language without changing the underlying fact.

Generate investigation checklists, regression cases and draft report structure for reviewer validation.

Prioritise tokens or systems for deeper review based on transparent signals.

Prohibited substitutions

Do not label a project safe because a model returned a high score.

Do not convert missing data into a clean result.

Do not invent team identity, legal rights, audit results, partnerships or current contract state.

Do not upload private keys, seed phrases, confidential PoCs or unredacted client evidence into an unapproved model service.

Do not let model confidence replace reproducibility or onchain verification.

Human decision record

Question	Required record
What did automation produce?	Inputs, source date, relevant model or rule version and output used.
What did the reviewer verify?	Primary evidence, reproduction result and contradictory information.
What remains uncertain?	Unavailable data, inference and conditions that would change the conclusion.
Who owns the conclusion?	Named MASTR function or reviewer responsible for the final assessment.
How can it be corrected?	Challenge route, evidence threshold and material-correction record.

AI STANDARD

A model can help find the evidence. It cannot be the evidence.

22 / INDEPENDENCE

Community, distribution and anti-shill policy

MASTR built its public reach through investigations, warnings and practical work rather than paid KOL distribution. That choice limits artificial growth but protects the credibility the ecosystem depends on.

30,000+	Millions	0	31
PUBLIC COMMUNITY	ORGANIC IMPRESSIONS	PAID VERDICTS	SUBSCRIBERS
Historical public audience figure.	Accumulated reach without a rented shill network.	Commercial scope never includes a clean conclusion.	Dated August 2026 product snapshot.

The anti-shill policy

No paid promotion disguised as an independent security conclusion.

No badge issued as sponsored decoration.

No casino promotion or memecoin call group presented as community building.

No undisclosed token allocation, affiliate interest or exit position behind a recommendation.

No suppression of a material risk to protect a partner, payer or holder.

No copying another researcher's finding without clear attribution and independent verification.

Why independence still needs funding

Research, testing, infrastructure, legal work and application development cost time and money. Pretending otherwise creates hidden sponsors. MASTR's answer is not to avoid revenue; it is to expose the terms. Fixed-scope work, subscriptions, product access, token utility and voluntary support can fund the mission when the payer cannot purchase the outcome.

DISTRIBUTION RULE

MASTR would rather publish a difficult result to a smaller audience than buy a larger audience by becoming dependent on the people it may need to investigate.

23 / PROOF OF WORK

Evidence of delivery without exploiting open findings

Recent security work is described by scope and output while exploitable detail and affected names remain private until disclosure is safe, authorised or necessary to protect users.

Engagement	Documented output	Release status
DeFi protocol deep retest	17 retained findings across authority concentration, network-state representation, backend amplification and user trust boundaries.	Private responsible disclosure; verification withheld while Critical and High blockers remain.
Trading platform assessment	38-page report with 3 High, 2 Medium and 5 assurance observations covering agent-enabled production risk.	Private responsible disclosure; public release on hold pending remediation and independent verification.
Web, API and domain assessment	8 issues: 3 High, 3 Medium and 2 Low across web, API, CMS, transport and email-security exposure.	Private responsible disclosure; no claim of confirmed compromise.

Why names remain private

A vulnerability report is not content inventory. Publishing an affected product before the team can fix a reproducible path can convert research into an attack guide. MASTR therefore separates proof of work from weaponised disclosure. Scope, evidence quality and release decision can be stated without revealing the target or the exploit path.

When public warning becomes justified

- The issue presents a material and current user risk.
- The affected party has received sufficient evidence and a reasonable opportunity to respond.
- Silence, denial or superficial changes leave the demonstrated path open.
- Disclosure can reduce harm without unnecessarily increasing exploitability.
- Legal, factual and attribution risks have been reviewed.

RELEASE DECISION

No unresolved vulnerability is used as engagement bait. No team receives indefinite secrecy while users remain exposed. The decision is made against harm, evidence and remediation reality.

24 / ROADMAP

Progress by evidence, not invented deadlines

The roadmap records what has been established and what must become true next. Future work is gated by security, legal, product and operational readiness rather than calendar theatre.

Period	Established direction	Evidence or current treatment
April-November 2024	Foundation, platform concept and $MASTR launch.	Historical project formation and original ecosystem document.
Late 2024	App, Badge, knowledge, reward and protection concepts.	Core ecosystem identity preserved; several claims reclassified by present status.
2025	Mobile adoption, token checks, community and product iteration.	Historical app and scanner metrics demonstrate productive use.
2026	MASTRlabs security positioning, external assessments, onchain investigations, new website and product portfolio.	Active security work, public knowledge, live apps and documented private development.
Current build phase	MASTRpass hardening across Android, Windows, iOS and macOS; AskMASTR signal quality; MASTRful private alpha.	Release-gated, not date-promised.
Next maturity phase	Signed releases, reproducible builds, external audit readiness, product-status reconciliation and current token transparency.	Requires published evidence before promotion.
Long-term protection phase	Potential lawful activation of a funded protection programme.	Requires entity, reserves, terms, claims operations and regulatory analysis.

Priority tracks

Track	Near-term objective	Exit gate
Security research	Standardise scope, evidence levels, remediation and retest records.	Reports remain reproducible across engagements.
MASTRpass	Complete hardening, recovery scenarios, packaging and platform validation.	Signed official release, hashes, notes, provenance and independent-audit plan.
AskMASTR	Improve traceability, confidence display and escalation to human review.	Measured reduction in false certainty and clearer source attribution.
Community app	Maintain reliable warnings, checks, conversations and wallet/reward boundaries.	Privacy, security and reward rules remain current and product-specific.
Badge and register	Publish scope, date, expiry and reassessment context consistently.	Every entry can be independently verified and withdrawn when stale.
$MASTR transparency	Reconcile archived allocation with current onchain state and controls.	Dated wallet-level transparency record.
Protection framework	Complete legal, reserve, claims and risk design.	No activation before all mandatory conditions are public.

25 / MEASUREMENT

Measure protection, not noise

Follower counts and scans show reach. They do not prove that users are safer. MASTR's measurement framework therefore separates activity, quality, remediation, product maturity and independence.

Objective	Metric	What good looks like
Research quality	Findings with reproducible evidence, clear limits and root-cause remediation.	High confirmation rate and low ambiguity after independent review.
Remediation	Critical and High findings closed after retest, not self-attestation.	Original and adjacent paths fail after control change.
Disclosure	Time to acknowledgement, remediation plan and verified closure.	Reasonable response without indefinite exposure.
Scanner utility	Checks leading to source review, human escalation or avoided unsafe interaction.	Behavioural value, not only request volume.
Knowledge	Completion, comprehension and correction rate.	Users can explain the mechanism and act on it.
MASTRpass	Recovery-test success, crash-free use, import fidelity and platform release gates.	Verified recovery and no silent data loss.
Badge integrity	Reassessments, expiries, suspensions and changes published on time.	No stale badge remains visually current.
Independence	Share of revenue with no control over conclusions; disclosed conflicts.	No payer-dependent verdicts or hidden promotional obligations.
Token transparency	Onchain reconciliation and authority disclosure currency.	Public records match current state.

Reporting cadence

Product status changes when release gates move, not when marketing needs content.

Material security findings remain tracked until verified closure or explicit risk acceptance.

Badge register entries show review and reassessment dates.

Historical metrics retain their date and are never displayed as live counters.

Token and protection records are updated when the underlying state materially changes.

METRIC RULE

A number without a date, denominator, method and consequence is decoration. MASTR metrics should help someone decide whether a control or product improved.

26 / RISK REGISTER

MASTR must apply its own standard to itself

The ecosystem carries technical, market, legal, operational and credibility risk. Naming these risks is not weakness. Hiding them would be.

Risk	Exposure	Primary mitigation
Key-person concentration	Independent operation can create bottlenecks and continuity risk.	Documented processes, protected records, scoped contributors and succession planning.
False-positive investigation	A wrong conclusion can harm users, teams and MASTR credibility.	Evidence levels, reproducibility, challenge route, correction record and legal review.
Retaliation and threats	Anti-scam and security work can trigger harassment or physical risk.	Undoxxed identity, minimum personal data, secure channels and controlled disclosure.
Unresolved vulnerabilities	Research detail can be abused before remediation.	Private disclosure, least-detail public reporting and release decision based on user harm.
MASTRpass defect	A vault bug can cause data loss or secret exposure.	Pre-release warnings, multiple backups, hardening, provenance, recovery tests and external audit before final trust claims.
App data exposure	Networked account and messaging data can be breached or mishandled.	Data minimisation, provider controls, access review, deletion and incident response.
Token volatility and concentration	Price, liquidity or holder structure can undermine utility and trust.	No return promises, onchain transparency, honest liquidity and authority disclosure.
Badge staleness	A project changes after review while the badge remains visible.	Expiry, monitoring, material-change duty, suspension and public register updates.
Protection insolvency	Future claims can exceed reserves or trigger correlated loss.	No activation without reserves, limits, concentration model, claims operations and audit.
AI error	Models hallucinate, omit context or amplify bias.	Human ownership, source traceability, confidence display and prohibition on model-only verdicts.
Commercial capture	A large payer influences priority or conclusion.	Scope-result separation, conflict disclosure and reviewer-controlled decisions.
Brand impersonation	Fake accounts, copied logos and malicious links exploit MASTR credibility.	Official link hub, full-address checks, signed releases and repeated user verification guidance.

27 / LEGAL BOUNDARY

Clear limits before capital or secrets

MASTR provides security research, risk intelligence, tools, education and ecosystem products. None of these removes a user's duty to verify, and none should be described as a regulated service without the legal structure that makes that statement true.

No financial advice

Research, token checks, badges, verified-project records, app content and this GREENPAPER are informational. They do not instruct a person to buy, sell or hold an asset and cannot eliminate smart-contract, market, custody, liquidity, counterparty or legal-enforcement risk.

No active insurance claim

The MASTR Insurance concept is a framework. Until current binding terms identify the responsible entity, reserve capacity, coverage, exclusions, claims process and governing law, no user should rely on it as active insurance, a guarantee or reimbursement obligation.

Product-specific privacy

MASTRpass and the networked community app have different data models. The applicable privacy notice and terms for the specific product govern data processing. Users must not send private keys, seed phrases, vaults or recovery keys to support, AskMASTR or security-reporting channels.

Intellectual property and fair challenge

MASTR owns its original reports, brand and product material subject to applicable rights. Factual criticism, independent verification and responsible challenge are necessary to security. Copyright must not be used to prevent good-faith discussion of a public claim or verified technical fact.

Jurisdiction and change

Laws, regulatory classifications and product terms can change. Each commercial engagement, app purchase, token interaction, badge review and future protection programme requires current terms. A 2024 governing-law sentence cannot be assumed to govern a 2026 product unless current binding terms say so.

USER RESPONSIBILITY

Verify the domain, full address, package name, hash, signature, requested permission and wallet action. Never trust a copied logo, shortened contract or unsolicited support message.

28 / COMMITMENTS

What MASTR commits to defend

The ecosystem will change. These operating commitments define the standard against which that change should be judged.

1. MASTR will not sell a positive security conclusion, badge or silence.
2. Material findings will distinguish confirmed fact, inference and unresolved questions.
3. Critical and High issues will not be called fixed until the relevant control changes and the fix is independently retested.
4. Open vulnerabilities will not be used as reckless engagement content.
5. Historical plans will be preserved as history and not quietly relabelled as current delivery.
6. Product status will remain explicit: live, active, selective, development, private alpha, framework or historical.
7. The offline privacy model of MASTRpass will not be falsely applied to connected MASTR products.
8. AI will assist research but will not be presented as the sole basis of a material verdict.
9. $MASTR ownership will not purchase authority over evidence or security decisions.
10. A future protection programme will not be activated without legal responsibility, reserves, binding rules and claims operations.
11. Material errors will be corrected with a dated record rather than hidden.
12. Official links, addresses and release artefacts will be published in forms users can verify independently.

MASTR STANDARD

ANTI-SCAM | ANTI-LIES | ANTI-FRAUD is not a slogan that applies only to other projects. It is the obligation to document MASTR with the same hostility toward weak claims, hidden incentives and false certainty.

Truth over hype

The value of MASTR is not that it can promise safety. The value is that it can make risk harder to hide, evidence easier to inspect and remediation harder to fake.

29 / FAQ

Clear answers to predictable questions

Question	Answer
What is MASTR?	An independent Web3 security ecosystem combining onchain investigations, external assessments, scam prevention, knowledge, apps and the $MASTR economic layer.
Is $MASTR a guarantee that a project is safe?	No. The token aligns ecosystem participation and utility. It does not certify projects or remove investment risk.
Can a project buy a positive report or badge?	No. A project can pay for defined work and outputs. Payment cannot determine the conclusion, badge decision or release status.
What does the MASTR Badge mean?	A dated, scoped and revocable point-in-time review signal. It is not permanent and is not a guarantee against loss.
Is MASTR Insurance active?	No. The GREENPAPER documents the historical framework. Binding terms, reserves, claims administration and the responsible entity are required before any activation.
Is MASTRpass the same as the community app?	No. The community app is connected and account-based. MASTRpass is an offline local vault with no MASTR account, backend, cloud or telemetry.
Does MASTRpass replace a hardware wallet?	No. It stores encrypted secrets and offers local inspection tools. It does not sign or broadcast transactions and should never be the only recovery copy.
Has MASTRpass been externally audited?	Not as of this document. It remains pre-release, and users must not rely on an alpha or beta as sole protection for high-value secrets.
What is MASTRful?	A classified MASTR Labs product in private alpha. No public feature list, release date or token utility is committed here.
Does AskMASTR provide financial advice?	No. It provides information and risk signals. Automated output can be incomplete and should be escalated to human review when the decision is material.
Who governs security findings?	The responsible MASTR reviewer or security function, constrained by evidence, scope, conflict controls and reproducibility. Token voting cannot change a technical fact.
How should the token mint be verified?	Compare the complete Solana address against the current official MASTR route and an independent explorer. Never use a shortened, ellipsised or malformed address.

30 / REFERENCES

Source basis, glossary and change record

This GREENPAPER is based on public MASTR records, the archived 2024 Whitepaper, current product pages, official brand assets and dated internal build provenance available at the document date.

Primary MASTR sources

Source	Use in this document
MASTR Whitepaper V5, 24 November 2024	Historical mission, ecosystem concepts, allocation model, former roadmap and protection design.
mastrlabs.com	Current security positioning, ecosystem status, services, Badge, register, token role and public metrics.
mastrapps.com	Live community-app capabilities, MASTRpass architecture, platform status, product separation and MASTRful public status.
askmastr.xyz	Archived Whitepaper and full official Solana token-route reference.
Official MASTR brand-asset record, effective 26 August 2026	Logo, banner, researcher identity image, colours and official brand language.
MASTRpass build provenance through 28 August 2026	Dated evidence of Android and Windows development builds, package identity and network-permission posture.
MASTR security assessment records, August 2026	Method, evidence levels, scope limits, finding counts and remediation standard.

Official destinations

Purpose	Destination
Ecosystem and research	https://mastrlabs.com
Official app portfolio	https://mastrapps.com
Main public account	https://x.com/MastrXYZ
Research and security account	https://x.com/MASTRlabs
Official link hub	https://linktr.ee/askmastr.xyz
AskMASTR portal	https://askmastr.xyz

Glossary

Term	Meaning
Authority	A key, role, account or process capable of changing privileged state.
Trust boundary	The point where control, data, authority or user reliance passes between actors or systems.
Point-in-time assessment	A review of a defined system state and scope at a stated date.
Retest	Independent verification that the original and adjacent paths no longer reproduce after remediation.
Responsible disclosure	Private delivery of exploitable findings with evidence and a reasonable remediation opportunity.
Build provenance	Evidence connecting release artefacts to source, toolchain, package identity and hashes.
Framework	A documented design that is not yet an active binding product or service.

Change record

Version	Date	Change
1.0	28 August 2026	First GREENPAPER. Replaced V5 with status-led architecture, current products, stricter security model, token history, governance, risks and legal boundaries.

Copyright

THE STANDARD

EVIDENCE BEFORE TRUST.

ONCHAIN INVESTIGATIONS, WEB3 KNOWLEDGE & PROTECTION

MASTRLABS.COM | X.COM/MASTRXYZ | VERSION 1.0