Rena Protocol White Paper

Verifiable confidential data exchange for market integrity and private AI

Published by Renaissance Foundation

Date: 2026-08-26

Abstract

Renaissance Foundation coordinates ecosystem development, grants, governance, and token distribution for the Rena Protocol. The protocol's confidential data infrastructure and products, including Insider Cash, are developed by Rena Labs.

Summary

This white paper is published by Renaissance Foundation, a Cayman Islands foundation company that coordinates ecosystem development, grants, governance, and token distribution for the Rena Protocol. The protocol's confidential data infrastructure and its products, including Insider Cash, are developed by Rena Labs.

Rena Labs develops verifiable confidential data infrastructure for AI products and market-integrity analytics. Its public materials describe Rena as a Trusted Execution Environment (TEE) data exchange room that enables confidential AI training and inference on private data. Rena Labs' product materials further describe Insider Cash as an integrity dashboard for abnormal token trading activity, TEE-processed market-making API data, KPI compliance, anomaly detection, CEX and DEX analytics, liquidity, spread, depth, volume, and market-maker performance.

The Rena Protocol is proposed as the network and economic coordination layer around this infrastructure. Its goal is to let data providers, token issuers, market makers, exchanges, funds, verifiers, analysts, developers, and AI agents collaborate around sensitive data without requiring raw confidential data to be exposed. The protocol is designed around verifiable confidential orchestration:

- Data is encrypted by the provider before transfer.
- Data is processed inside an attested TEE enclave.
- AI or analytics models run without exposing raw inputs.
- Outputs are returned or stored according to configured permissions.
- Selected actions and attestations can be logged on-chain with customizable transparency.

The proposed RENA token supports access, service settlement, governance signaling, and verified contribution incentives inside the Rena Protocol ecosystem. Its proposed initial supply is 1,000,000,000 RENA, with no additional minting currently planned. RENA is not designed as a stablecoin, asset-referenced token, e-money token, equity instrument, debt claim, collective investment interest, profit share, dividend right, or right to redemption against Renaissance Foundation, Rena Labs, or any affiliate. Holding RENA alone does not entitle a holder to revenue, profits, interest, assets, management rights in any legal entity, or any passive return.

The token model is utility-first:

- Product access: RENA can be used for Insider Cash scans, integrity dashboards, API calls, research reports, data-room sessions, and premium analytics features.
- Confidential compute settlement: RENA can settle TEE compute, model execution, attestation, and proof-publication fees.
- Future performance deposits: in later phases, approved third-party operators may be required to post a fixed commercial performance deposit, payable in fiat, stable-value assets, or RENA where permitted, to cover defined misconduct. This is not expected to be a Day 1 token utility.
- Verifier and challenge incentives: analysts, auditors, security researchers, and independent verifiers can earn incentives for useful and verified work.
- Governance signaling: time-locked or reputation-weighted RENA may be used to signal on limited protocol parameters, data schemas, attestation policy, grants, and ecosystem priorities.

- Contribution rewards: RENA may be distributed from an ecosystem allocation only for active, verifiable contributions. Rewards are not paid for mere holding.

Prospective holders should read this white paper as a whole and not rely on the summary alone. RENA may lose all value, may not be transferable, may have limited liquidity, and is not covered by deposit guarantee schemes or acquirer/holder compensation schemes. Purchasers are responsible for complying with laws applicable to them.

Contents

1. Introduction
2. Rena Labs and the Market-Integrity Problem
3. The Rena Protocol
4. Insider Cash
5. Technical Architecture
6. RENA Token Economic Design
7. RENA Token Utility
8. Token Supply and Distribution
9. Token Availability and Holder Restrictions
10. Governance
11. Roadmap
12. Rights and Obligations of Holders
13. Risks
14. Environmental Considerations
15. Appendices

1. Introduction

Digital markets increasingly depend on private data. Market makers hold orderbook, spread, inventory, and execution data. Exchanges hold trade and liquidity information. Token teams need to know whether market-making commitments are being honored. Funds and traders need reliable signals about market integrity. AI builders need private datasets for training and inference. Yet the parties with the most useful data often cannot expose raw information because it is proprietary, commercially sensitive, regulated, or security-critical.

This creates a coordination failure. The market wants transparency, but transparency can conflict with confidentiality. Token issuers want evidence of liquidity quality, but market makers cannot simply publish all raw trading data. Analysts want to detect abnormal activity, but the underlying data may be fragmented across centralized exchanges, decentralized venues, market makers, token teams, and data providers. AI agents can produce useful analysis, but they need access to datasets that owners often cannot port or share.

Rena Labs addresses this problem through verifiable confidential computation. The public Rena Labs website describes Rena as a TEE data exchange room that unlocks liquidity for proprietary data with privacy and compliance built in. The website also describes a flow in

which data is encrypted by the provider, transferred into a verifiable TEE enclave, processed by an AI model without exposing raw data, and then returned or stored securely with selected on-chain logs.

The Rena Protocol extends this model into a tokenized coordination layer. The protocol is intended to support secure data exchange rooms, AI execution on sensitive data, market-integrity analytics, operator accountability, verifier incentives, and ecosystem governance. The RENA token is designed to support the operational use of this protocol, not to provide a claim on Renaissance Foundation, Rena Labs, or any other legal entity.

This white paper is intended to serve two purposes:

- Product and technical explanation: It describes Rena's architecture, use cases, and token utility in a form understandable by exchanges, ecosystem partners, market participants, and sophisticated users.
- Public token disclosure: It summarizes the proposed token design, utility categories, allocation, holder rights, limitations, roadmap, and principal risks.

The structure is intentionally conservative and utility-focused. It follows a technical-whitepaper format suitable for public ecosystem materials.

2. Rena Labs and the Market-Integrity Problem

2.1 Rena Labs

Renaissance Foundation coordinates ecosystem development, grants, governance, and token distribution for the Rena Protocol. Rena Labs develops the protocol's confidential data infrastructure and products, including Insider Cash.

Public Rena Labs materials describe Rena as a confidential data infrastructure company. Rena's website states that it unlocks trustless AI on private data that users could not otherwise access, port, or share. It describes Rena as a TEE data exchange room for proprietary data, confidential AI training, and confidential inference.

Rena Labs' public-facing products include at least:

- Insider Cash: a market-integrity dashboard for abnormal token trading activity, powered by live, TEE-processed market-making API data.
- Addys: a proactive meeting agent described by Rena Labs' website as listening, extracting what needs to happen, and helping complete follow-up work.

This white paper focuses on the Rena Protocol and the market-integrity and confidential-data-exchange use cases reflected by Insider Cash.

2.2 The market-integrity gap

Crypto markets are highly transparent at the settlement layer but often opaque at the market-structure layer. On-chain trades are visible, but centralized exchange orderbooks, market-maker inventory, spread commitments, depth, venue-by-venue execution quality, and API data can remain private. This asymmetry affects multiple stakeholders:

- Token teams need to understand whether market makers are satisfying liquidity, spread, depth, and volume expectations.
- Market makers need to protect proprietary trading methods and client-specific execution data.
- Exchanges need to preserve confidential orderbook and user information.
- Funds and traders need reliable market-health signals.
- Regulators and industry bodies increasingly expect stronger controls against manipulation, insider activity, abusive trading patterns, and misleading liquidity.
- Retail users are often the least able to distinguish organic market activity from engineered or abnormal activity.

The result is a trust problem. If token teams ask for raw data, counterparties may refuse. If counterparties only provide summaries, token teams may not trust them. If public dashboards use incomplete data, analysts may draw the wrong conclusions. A secure computation layer can reduce this conflict by letting sensitive data be processed under verifiable rules while only approved outputs are revealed.

2.3 Why TEEs are useful here

A Trusted Execution Environment is a protected execution context that can run code and process data while limiting access by the surrounding system. TEEs can support remote attestation, allowing external parties to verify that a specific program is running in an expected environment. TEEs are not perfect and do not remove all security risk, but they are useful for workflows where parties want to compute over private data without exposing raw inputs.

For Rena Labs, TEE-based design supports four core goals:

- Confidentiality: raw market-making and proprietary data can remain hidden from parties that do not have permission to see it.
- Verifiability: participants can verify that an approved computation was executed in an attested environment.
- Automation: AI models and analytics can run over sensitive datasets in a repeatable and auditable way.
- Selective transparency: outputs, proofs, logs, and attestations can be published without publishing the underlying confidential data.

2.4 Market-integrity use cases

Rena's market-integrity stack can support a range of use cases:

- Liquidity compliance: measuring whether venue-specific liquidity commitments are met.
- Spread and depth monitoring: measuring whether spreads and orderbook depth remain within agreed ranges.
- Volume quality analysis: distinguishing healthy activity from suspicious wash-like or self-referential patterns.
- Market-maker performance analytics: comparing committed service levels against observed performance.

- Abnormal activity detection: using models to identify trading anomalies, sudden liquidity withdrawals, suspicious order placement, or coordinated behavior.
- Token-health dashboards: giving project teams, funds, and traders a concise view of market quality.
- Confidential research reports: producing market-integrity reports without exposing raw proprietary data.
- Data-provider monetization: allowing participants with proprietary data to provide useful outputs without surrendering the data itself.

3. The Rena Protocol

3.1 Protocol objective

The Rena Protocol is proposed as a coordination layer for private-data AI and market-integrity analytics. Its objective is to allow independent participants to contribute data, compute, verification, models, and analysis under common rules. The protocol should support:

- Secure data exchange rooms.
- Confidential AI inference and training workflows.
- Market-integrity analytics.
- Data-provider and compute-provider accountability.
- Attestation and proof publication.
- Incentives for useful verified work.
- Governance over protocol parameters and standards.

3.2 Network participants

The protocol is expected to involve the following participant types:

Participant	Role	Examples of protocol interaction
Data providers	Supply data into a data exchange room under defined permissions	Market makers, exchanges, token teams, research partners
Data consumers	Request analytics, reports, or AI outputs	Token teams, funds, traders, analysts, ecosystem partners
TEE operators	Run approved jobs in attested environments	Confidential compute providers, infrastructure operators
Model providers	Provide analytics models or AI agents	Rena Labs, independent developers, research partners
Verifiers	Validate outputs, anomalies, attestations, or disputes	Auditors, analysts, security researchers, community verifiers
Token holders	Use services, contribute, or signal governance preferences	Users, ecosystem participants, contributors
Foundation	Coordinates early development and grants	Renaissance Foundation

3.3 Protocol design principles

Rena's economic and technical design should follow five principles:

- Confidentiality by default: raw data should remain private unless the provider has explicitly authorized disclosure.
- Verifiability without over-disclosure: participants should be able to verify that the right computation was performed without seeing data they are not authorized to see.
- Utility over speculation: token mechanics should be tied to access, settlement, governance signaling, and verified contribution rather than passive value expectations.
- Compliance-aware design: identity, sanctions, jurisdiction, KYC, AML, data protection, and market-abuse controls should be embedded where required.
- Incremental decentralization: early versions may use curated participants and permissioned controls; decentralization should expand only when security, legal, and operational standards are ready.

3.4 Relationship to Insider Cash

Insider Cash is the first flagship market-integrity product built on Rena Labs' confidential data infrastructure. It is not the entire protocol. Rather, Insider Cash is an application layer that demonstrates how the protocol can transform private market data into useful insights while protecting raw inputs.

The token model should therefore avoid overfitting to a single product. RENA should be usable across the broader Rena Protocol ecosystem, while Insider Cash provides the clearest near-term utility:

- Paying for scans, dashboards, and reports.
- Accessing premium analytics tiers.
- Funding data-room compute jobs.
- Introducing commercial performance deposits for approved third-party operators in later phases, if needed.
- Incentivizing anomaly verifiers.
- Coordinating governance around market-integrity standards.

4. Insider Cash

4.1 Product description

The Insider Cash website describes the product as unlocking token analysis from a user's own trading activity through an AI agent. It presents the value proposition as easy-to-use transparency that reduces insider activity and improves token sustainability. Public product pages describe an all-in-one integrity dashboard with real-time insights across centralized and decentralized exchanges, a unified view of market-maker performance, spread, depth, and volume tracking, and machine-learning assisted anomaly detection.

Rena Labs' website describes Insider Cash as an integrity dashboard revealing abnormal token trading activity, powered by live, TEE-processed market-making API data. It is designed for founders, traders, and funds seeking transparency into market-maker behavior and token health.

4.2 Product modules

Insider Cash is expected to include the following modules:

Module	Purpose	Example outputs
Market health dashboard	Summarize token market quality across venues	Liquidity score, spread score, depth score, volume score
Market-maker performance	Compare commitments against observed execution	KPI compliance, spread/depth adherence, venue coverage
CEX and DEX aggregation	Combine centralized and decentralized market data	Venue comparison, market fragmentation, liquidity concentration
Anomaly detection	Identify abnormal trading or liquidity behavior	Suspicious bursts, sharp liquidity removal, unusual inventory patterns
Confidential data room	Process sensitive inputs without exposing raw data	Attested computation result, permissioned report, audit log
Reporting layer	Convert analytics into shareable insight	Monthly transparency reports, project team reports, research notes

4.3 Data privacy posture

Insider Cash should be positioned as privacy-preserving market transparency. This distinction is important. The product does not require every participant to publish raw data. Instead, it lets approved computations run over private data and publishes outputs according to configured permissions.

The public-facing explanation should be simple:

- The market needs more truth.
- Raw trading data is sensitive.
- Rena lets useful analytics be produced without exposing the raw data.
- Attestation and logs increase confidence in the process.

4.4 Commercial users

The product can serve:

- Token teams seeking market-maker accountability.
- Market makers seeking privacy-preserving proof of performance.
- Exchanges seeking better analytics without over-disclosing confidential data.
- Funds seeking token-health and venue-quality signals.
- Research partners publishing market-integrity analysis.

- AI agents that need controlled access to private financial data.

5. Technical Architecture

5.1 Architecture overview

The Rena Protocol can be represented as five layers:

16. Data ingestion layer: connectors ingest market data, API data, orderbook snapshots, trade events, wallet data, or other permissioned datasets.
17. Confidential execution layer: approved jobs run in attested TEE environments.
18. Analytics and AI layer: models convert raw inputs into scores, alerts, reports, predictions, or research outputs.
19. Verification and attestation layer: attestations, job manifests, hashes, logs, and dispute evidence support accountability.
20. Settlement and coordination layer: RENA supports access, service fees, contribution rewards, and governance signaling.

5.2 Data exchange room lifecycle

The expected data exchange room flow is:

21. Room creation: a data provider or requester creates a room with permissions, model choices, data types, and output rules.
22. Provider encryption: the provider encrypts data client-side or through an approved secure connector.
23. Attestation: the TEE operator provides attestation evidence for the code and environment.
24. Job execution: the approved AI or analytics job processes the data inside the enclave.
25. Output control: outputs are filtered, aggregated, or redacted according to room policy.
26. Proof and log publication: hashes, job metadata, attestations, and selected outputs may be logged on-chain.
27. Settlement: fees, rewards, attestations, and dispute outcomes are handled according to protocol rules.

5.3 Attestation registry

The protocol should maintain an attestation registry that records:

- Approved enclave measurements.
- Approved job manifests.
- Model and code hashes.
- Operator identity or pseudonymous operator identifiers.
- Policy version and schema version.
- Timestamped job execution metadata.
- Output hash or report hash.
- Dispute status, if any.

The registry should avoid placing confidential raw data on-chain. On-chain records should be limited to hashes, attestations, permission references, state transitions, and other metadata that does not reveal sensitive content.

5.4 Data minimization and selective disclosure

Rena Labs should implement data minimization as a core design rule. A computation should access only the data necessary for the approved purpose, and outputs should reveal only the minimum information required for the use case. For market-integrity dashboards, this may mean publishing scores, ranges, alerts, or redacted explanations rather than raw order-level data.

5.5 Security controls

The protocol should include:

- TEE attestation verification.
- Secure connector validation.
- Encryption in transit and at rest.
- Role-based access controls.
- Key management standards.
- Job manifest allowlists.
- Independent security audits for smart contracts and critical off-chain components.
- Incident response procedures.
- Vulnerability disclosure and bug bounty processes.
- Monitoring for availability, abnormal operator behavior, and data leakage.

5.6 Limitations of TEEs

TEE systems have known risks. Vulnerabilities can arise from side-channel attacks, vendor defects, misconfiguration, compromised key management, flawed attestation verification, malicious operators, or bugs in the code running inside the enclave. Rena Labs should not market TEEs as absolute privacy guarantees. The correct position is that TEEs are one component in a defense-in-depth architecture.

6. RENA Token Economic Design

6.1 Token classification

The proposed RENA token is intended to be a utility token for the Rena Protocol ecosystem. It is not designed to maintain a stable value by referencing a fiat currency, commodity, crypto-asset, basket of assets, or any other reference value. It is not redeemable at par, and no holder has a claim against Renaissance Foundation, Rena Labs, or any affiliate for redemption.

6.2 Proposed token parameters

Field	Parameter
Token name	Rena
Ticker	RENA
Token type	Utility token
Initial standard	ERC-20 or compatible EVM token
Initial network	EVM-compatible network; final network will be announced before launch
Decimals	18
Proposed initial total supply	1,000,000,000 RENA
Minting policy	All initial tokens are expected to be created at genesis. No additional minting is currently planned. Any future supply increase would be subject to the conditions described in Section 8.1.
Burning policy	None. No burn, buyback, repurchase, or supply-reduction mechanism is implemented, announced, or planned.
Redemption	No redemption right or holder redemption claim
Rights in Renaissance Foundation or Rena Labs	None
Profit or revenue share	None
Governance	Limited protocol signaling only; no legal-entity control
Transfer restrictions	Jurisdiction, sanctions, KYC/AML, and platform restrictions may apply

6.3 Economic design objectives

The token design has four objectives:

- Create a clear medium for access and settlement across Rena services.
- Create operational accountability through transparent service rules, verification, and future commercial performance deposits where appropriate.
- Reward active contributions that improve protocol utility and safety.
- Coordinate protocol-level decisions without granting legal-entity ownership or financial rights.

The design avoids passive-yield language. Rewards require work, usage, verification, or contribution. Governance is limited to protocol parameters. Any future performance deposit mechanism should be a commercial risk-control tool rather than a yield, staking, or token-demand mechanism.

6.4 Core economic components

The Rena Protocol's proposed economy has four components:

- Service settlement: users pay for protocol services, data-room sessions, analytics, scans, reports, and API calls.
- Operational accountability: service providers may be subject to published service standards, verification, dispute processes, and, in later phases, fixed commercial performance deposits.
- Contribution rewards: ecosystem allocations reward useful verified work.
- Governance signaling: holders can signal preferences on protocol configuration.

6.5 Settlement model

Let service category s have quantity q_s and fee f_s denominated in USD-equivalent terms for user clarity. If the token price at settlement is P_t, the RENA settlement amount for that service is:

```
RENA_s,t = q_s * f_s / P_t
```

Where permitted, users may pay in fiat or stable-value assets through approved payment processors, and the protocol or service provider may convert the payment into RENA for settlement. This is an onboarding convenience only. RENA is not backed by fiat, not redeemable for fiat, and not designed to maintain a stable value.

6.6 Future performance deposit model

Performance deposits are not expected to be a Day 1 token utility. If third-party operators, data providers, or other high-trust service participants are onboarded in later phases, the Rena Protocol may introduce fixed commercial performance deposits to support accountability.

Any such deposit should be denominated in a stable unit of account and may be paid in fiat, stable-value assets, or RENA where legally and operationally permitted. A participant should not be required to acquire RENA merely to participate. Deposit size should be set by role category or service tier and should not increase permitted job volume, task allocation, selection probability, rewards, fee entitlement, or any other earning capacity.

Performance deposits do not pay interest, rewards, fee share, inflation, or any other return. Holding a deposit longer does not produce any return, and posting a larger amount does not provide any economic advantage. The sole purpose of a deposit is to create a responsibility reserve for specific operational misconduct.

Deposits may be reduced or forfeited only for defined misconduct, such as fraudulent data submission, intentional manipulation of market-integrity outputs, unauthorized disclosure in breach of an applicable policy or agreement, or other material breach specified in published terms. Downtime, service-level credits, model-quality issues, and ordinary commercial disputes should be handled primarily through service agreements, support procedures, or dispute resolution rather than automatic token penalties.

If a deposit is reduced or forfeited, the deducted amount should be handled through a transparent waterfall. First, it may compensate identifiable counterparties for proven losses caused by the misconduct, limited to actual loss. Second, any remaining amount should be transferred to a segregated Security Reserve used only for security audits, incident response, and affected-user compensation. Deducted amounts should not be burned, distributed to

token holders, transferred to a general treasury or operating account, or paid to challengers as a percentage of the deducted amount. Verified investigation costs may be reimbursed only under published caps.

6.7 Contribution reward model

Contribution rewards are designed to compensate active work. They are not paid for passive holding. A contribution score can be defined as:

```
C_i,t = a * A_i,t + b * V_i,t + c * Q_i,t - d * R_i,t
```

Where:

- A_i,t is verified activity, such as useful reports, validated alerts, or resolved challenges.
- V_i,t is validation quality, such as successful fraud proofs or accepted anomaly labels.
- Q_i,t is quality score, such as peer validation or accuracy.
- R_i,t is risk adjustment, such as disputes, false positives, or rejected work.
- a, b, c, and d are governance-controlled weights.

Rewards are distributed only from pre-allocated ecosystem pools and only for qualifying activity. Reward eligibility may require KYC, sanctions screening, jurisdiction screening, minimum quality thresholds, and anti-Sybil checks.

6.8 Fee handling

Protocol service fees are consideration for services rendered and are received by the party providing the relevant service. Fees are not pooled, are not allocated among token holders, and do not accrue to holders by virtue of holding. No portion of protocol service fees is distributed to token holders, used to acquire tokens on the open market, or applied to reduce token supply.

Any fee allocation, reserve policy, or service-provider payment flow must be disclosed before implementation. Fees should not be described as dividends, profit distributions, interest, or passive income to token holders.

6.9 Non-security characterization

The RENA token is designed for consumptive and operational use:

- Users need RENA or RENA-denominated credits to access services.
- Future approved operators or providers may be subject to commercial performance deposits, but these deposits should not be required for general holders and should not generate yield or increase earning capacity.
- Verifiers and contributors can earn RENA for active, verified work.
- Governance participants use RENA only to signal on protocol parameters.

RENA does not represent equity, debt, a legal claim on assets, a right to profits, a right to revenue, a right to dividends, a right to interest, or a share in any legal entity. No person should purchase RENA with an expectation of profit from the efforts of Renaissance Foundation, Rena Labs, or any other person.

7. RENA Token Utility

7.1 Utility overview

RENA has five proposed utility categories, with one future operational control that may be introduced for approved third-party service participants:

Utility	User need	Token function
Product access	Use Insider Cash and Rena data-room services	Pay for scans, dashboards, reports, API calls, and subscriptions
Confidential compute settlement	Run TEE jobs and AI inference	Pay compute, attestation, proof, and model-execution fees
Verification and challenge	Improve accuracy and detect misconduct	Earn rewards for active verified work; anti-spam deposits may apply under published rules
Governance signaling	Coordinate protocol policy	Vote or signal on limited protocol parameters
Ecosystem contribution	Grow data, models, integrations, and research	Earn incentives from allocated pools for accepted contributions

7.2 Utility 1: Product access

RENA can be used to access Rena ecosystem services. Examples include:

- Insider Cash token scans.
- Market-health dashboards.
- Premium anomaly detection.
- Market-maker KPI reports.
- Confidential data-room sessions.
- API calls.
- Attested AI inference jobs.
- Custom research outputs.

Enterprise users may require invoices, fiat pricing, or stable-value payment options. The protocol may support such payment methods for user convenience, while service settlement can remain RENA-denominated.

7.3 Utility 2: Confidential compute settlement

Rena's infrastructure involves compute costs, attestation costs, model execution, storage, and reporting. RENA can serve as the settlement asset for:

- TEE job execution.
- Attestation verification.
- Output hashing and proof publication.
- Model provider fees.

- Data-room policy enforcement.
- Secure storage or retrieval.
- Report publication.

This creates a direct link between token use and protocol activity.

7.4 Future operational control: performance deposits

Future third-party data providers, connector operators, TEE operators, or model providers may be required to post fixed commercial performance deposits (as a guarantee of service standards and reliability) before participating in high-trust workflows. These deposits are not expected to be a Day 1 token utility and should be available in fiat, stable-value assets, or RENA where permitted.

Deposits are intended to support accountability for defined misconduct, such as fraudulent data submission, intentional manipulation of market-integrity outputs, unauthorized disclosure in breach of policy or agreement, or other material breach specified in published terms.

Deposits are refundable if the participant satisfies applicable requirements. Deposits do not generate interest, rewards, fees, inflation, or any other return. Posting a deposit does not increase task allocation, throughput, selection probability, fee entitlement, rewards, or earning capacity. Deposits are not available to general holders for the purpose of earning returns.

This mechanism is distinct from staking or proof-of-stake. It does not create a return for locking tokens, cannot be delegated to or by third parties, and is limited to approved operational roles under published commercial terms.

7.5 Utility 3: Verification and challenge

Market-integrity analytics require verification. RENA can coordinate verification by allowing:

- Analysts to flag suspected false positives or false negatives.
- Verifiers to validate anomalies.
- Security researchers to report vulnerabilities.
- Participants to challenge false attestations or bad outputs.
- Verifiers to earn rewards for accurate work.

Challenge systems should require anti-spam protections. A participant who submits a challenge may need to post a small anti-spam deposit, which can be returned if the challenge is valid or reduced if the challenge is frivolous or malicious. Any reimbursement for verifiers or challengers should be limited to verified costs under published caps and should not be paid as a percentage of a forfeited amount.

7.6 Utility 4: Governance signaling

RENA may support limited governance signaling. Governance should be scoped to protocol matters, such as:

- Fee categories and maximum rates.
- Future performance deposit categories.

- Deposit reduction or forfeiture conditions.
- Data schema standards.
- Attestation requirements.
- Approved TEE operator criteria.
- Ecosystem grants.
- Research bounty categories.
- Dispute process parameters.
- Product-specific access tiers.

Governance does not give holders control over Renaissance Foundation, treasury assets of any legal entity, employment decisions, corporate budgets, or distributions.

7.7 Utility 5: Ecosystem contribution

RENA can incentivize contributions that make the network more useful:

- New data connectors.
- New analytics models.
- New anomaly labels.
- Market-integrity reports.
- Security audits and vulnerability reports.
- Documentation and developer tools.
- Exchange integrations.
- AI agent integrations.
- Research partnerships.

Rewards should be rule-based, capped, and tied to verifiable work. The protocol should avoid open-ended promises.

8. Token Supply and Distribution

8.1 Proposed supply

The proposed initial total supply is 1,000,000,000 RENA, with all tokens expected to be created at genesis and allocated as set out below. No additional minting is currently planned. Any future proposal to increase supply would be a change to the current token model and would require separate legal and technical assessment, applicable approvals, and an updated white paper before implementation. Any final change to allocation, unlocks, token standard, network, or token contract should be reflected in an updated white paper before TGE or public distribution.

8.2 Proposed allocation

Category	Allocation	Tokens
Team	20.0%	200,000,000
Early Purchaser	17.0%	170,000,000

Advisor	3.0%	30,000,000
Treasury, Ecosystem & Liquidity	60.0%	600,000,000
Total	100.0%	1,000,000,000

The combined 60.0% allocation supports treasury needs, ecosystem development, and liquidity. Its internal breakdown will be determined as the project develops and disclosed before the relevant distribution or deployment.

8.3 Token release policy

The release policy should support long-term alignment:

- No Team, Early Purchaser, or Advisor tokens are scheduled to unlock at TGE.
- Ecosystem incentives, including any community onboarding or airdrop-style programs, should be distributed only for verified work, programmatic eligibility, or disclosed campaign rules.
- Treasury movements should be transparent where legally, commercially, and security-wise appropriate.
- Any material change should be reflected in an updated white paper and website disclosure.

8.4 Airdrop and ecosystem distribution principles

A portion of the combined Treasury, Ecosystem, and Liquidity allocation is intended for community airdrop and onboarding programs. Eligibility is designed around useful participation rather than passive speculation. Potential categories may include:

- Early product users.
- Verified data-room participants.
- Insider Cash beta testers.
- Useful anomaly verifiers.
- Security researchers.
- Developer contributors.
- Research partners.
- Community members who completed non-trivial tasks.

The size of the reserved portion, eligibility criteria, campaign timing, and claim mechanics will be published in a separate distribution release before any claim window opens.

Any airdrop includes anti-Sybil checks, sanctions screening, and jurisdiction restrictions, and is subject to published campaign terms. Airdrops are not described as an investment opportunity.

9. Token Availability and Holder Restrictions

9.1 Launch and availability status

RENA availability will be announced through official Renaissance Foundation channels. Any public distribution, exchange availability, claim process, pricing method, accepted currencies, eligibility rules, allocation limits, and restricted jurisdictions will be published before the relevant program begins.

9.2 Reasons for token availability

The reasons for making RENA available may include:

- Expanding access to Rena products and services.
- Enabling token-based settlement for data rooms and confidential compute.
- Supporting future operator accountability mechanisms where appropriate.
- Incentivizing early contributors and ecosystem growth.
- Providing liquidity needed for token utility.
- Supporting exchange and partner integrations.

9.3 Use of proceeds

If funds or crypto-assets are collected, proceeds are expected to be used for:

- Product development.
- TEE infrastructure and security.
- Smart contract development and audits.
- Data partnerships.
- Exchange, ecosystem, and market-integrity integrations.
- Legal, operational, and compliance operations.
- Research grants and verifier programs.
- Operational reserves.

No proceeds should be described as creating a right to profits or distributions for token holders.

9.4 Holder restrictions

Participation may be restricted for:

- Sanctioned persons or entities.
- Jurisdictions subject to comprehensive sanctions.
- Persons who fail KYC, AML, sanctions, or risk screening where required.
- Persons in jurisdictions where the offer, sale, holding, or use of RENA would require registration, licensing, authorization, or other steps not completed by the relevant responsible entity.
- Restricted insiders during lock-up or blackout periods.
- Persons attempting to manipulate airdrop, rewards, or governance systems.

9.5 Publication and website placement

The official project website may include high-level token utility and a link to the white paper. Detailed token distribution and availability information can be placed in the white paper and updated through modified white papers when necessary. The website should avoid promotional language that could imply profit, investment returns, guaranteed appreciation, or foundation-backed redemption.

10. Governance

10.1 Governance scope

RENA governance should be limited to protocol operations. Governance can include:

- Protocol fee schedules.
- Future performance deposit categories.
- Deposit reduction or forfeiture conditions.
- Approved data schemas.
- TEE attestation standards.
- Verifier onboarding criteria.
- Grant categories.
- Reward weights.
- Dispute resolution parameters.
- Privacy and transparency settings.

Governance should not include:

- Control of Renaissance Foundation or any related legal entity.
- Rights to appoint directors of a legal entity.
- Rights to dividends or liquidation proceeds.
- Rights to require treasury distributions.
- Rights to redeem tokens against Renaissance Foundation or any related legal entity.

10.2 Suggested governance phases

Phase	Governance model	Rationale
Phase 1: Launch	Foundation-led with published policies and limited community signaling	Security, compliance, and product stability
Phase 2: Controlled expansion	Token-holder signaling for selected parameters; committees for security and data standards	Gradual decentralization
Phase 3: Mature protocol	Broader on-chain governance for non-corporate protocol parameters	Increased transparency and ecosystem ownership

10.3 Governance risk controls

Governance should include:

- Proposal thresholds.
- Quorum requirements.
- Time delays for major changes.
- Emergency pause for security incidents.
- Conflict-of-interest disclosures.
- Exclusion of sanctioned or restricted participants.
- Clear separation between protocol votes and corporate decisions.

11. Roadmap

This roadmap describes the current expected development path for the Rena Protocol ecosystem.

Phase 0: Existing foundation

- Rena Labs develops TEE data exchange room infrastructure.
- Insider Cash public website and app entry point are live.
- Rena Labs public materials describe confidential AI training, inference, TEE attestation, and on-chain logging.
- Rena Labs publicly announces market-integrity partnerships and research ambitions.

Phase 1: Ecosystem announcement and registration

- Announce initial ecosystem partners.
- Complete product registration flow for early users.
- Prepare public token utility materials.
- Publish the public white paper and related token information.
- Prepare token terms, privacy, risk, and compliance materials.

Phase 2: Insider Cash beta and data-room pilots

- Expand Insider Cash scans and dashboards.
- Onboard early token teams, market makers, and research partners.
- Test TEE data exchange room workflows.
- Run private reports and transparency report pilots.
- Establish data-provider and verifier operating standards.

Phase 3: Token utility launch

- Deploy token contract after security audit and launch readiness checks.
- Enable product access and service settlement.
- Launch selected contribution programs.

- Design future performance deposit policies for approved third-party participants, if needed.
- Publish final token address, allocation, lock-up, and vesting disclosures.

Phase 4: Broader protocol expansion

- Expand data connectors and supported venues.
- Introduce governance signaling.
- Launch third-party model and analytics developer programs.
- Publish recurring market-integrity reports with selected partners.
- Improve environmental and operational reporting.

Phase 5: Mature confidential AI data network

- Support multiple categories of private-data AI beyond market integrity.
- Enable broader data-provider marketplace functionality.
- Expand decentralized verification.
- Increase transparency around protocol metrics, security, and governance.

12. Rights and Obligations of Holders

12.1 Holder rights

Subject to published network rules, holders may have the ability to:

- Use RENA to access Rena ecosystem services.
- Pay for data-room, compute, API, analytics, and reporting fees.
- Participate in approved operational roles subject to published requirements, which may include future commercial performance deposits.
- Receive RENA for active, verified contribution if eligible.
- Signal preferences on limited protocol parameters.
- Transfer RENA where legally and technically permitted.

12.2 No corporate or financial rights

Holding RENA does not provide:

- Equity in Renaissance Foundation or any affiliate.
- Debt claim against any entity.
- Dividend, revenue share, interest, or profit participation.
- Liquidation preference.
- Redemption right.
- Right to repayment of principal.
- Ownership of data, models, TEE infrastructure, dashboards, intellectual property, or treasury assets.
- Voting rights in any company.

12.3 Holder obligations

Holders are responsible for:

- Complying with applicable law.
- Paying taxes.
- Maintaining wallet security.
- Understanding transfer restrictions.
- Not using RENA or Rena services for unlawful activity.
- Not attempting to manipulate airdrops, rewards, data-room outputs, markets, governance, or verification systems.

13. Risks

13.1 Token value and liquidity risk

RENA may lose some or all of its value. There is no guarantee that RENA will be listed, remain listed, or have an active market. Even if trading occurs, liquidity may be limited and prices may be volatile.

13.2 Regulatory risk

The regulatory treatment of crypto-assets continues to evolve. Authorities may classify RENA or related activities differently from the intended utility-token classification. This could restrict offering, trading, transfer, use, marketing, or platform access.

13.3 Legal and regulatory implementation risk

Crypto-asset rules vary by jurisdiction and continue to evolve. A launch, distribution, listing, or marketing campaign may require additional disclosures, registrations, platform checks, eligibility controls, or timing changes.

13.4 Securities and financial-instrument risk

Even if RENA is designed as a utility token, regulators or courts may determine that the token or associated activities are securities, financial instruments, or regulated products in one or more jurisdictions. This may affect token availability, transferability, product access, or marketing in affected jurisdictions.

13.5 Product adoption risk

The utility of RENA depends on adoption of Rena products and protocol services. If Insider Cash, data exchange rooms, confidential AI workflows, or other Rena products fail to achieve adoption, demand for RENA utility may be limited.

13.6 TEE and confidentiality risk

TEEs can fail. Vulnerabilities, side-channel attacks, vendor issues, misconfiguration, compromised keys, malicious operators, or flawed code may expose data or produce unreliable results. Rena Labs should use defense-in-depth controls and should not represent TEEs as absolute guarantees.

13.7 Data quality risk

Market-integrity outputs depend on input quality. Incorrect, incomplete, delayed, manipulated, or biased data can lead to inaccurate reports, false positives, false negatives, or misleading scores.

13.8 Model risk

AI models and anomaly-detection systems can make errors. They may overfit, under-detect, misclassify market behavior, or produce outputs that users misunderstand. Rena Labs should provide model limitations and validation processes.

13.9 Market-abuse and manipulation risk

Participants may attempt to manipulate dashboards, token markets, reward programs, governance, or data feeds. Rena Labs and the Rena Protocol should implement surveillance, rate limits, anomaly detection, independent validation, clear service standards, and future performance deposit controls where appropriate.

13.10 Smart contract risk

Smart contracts can contain bugs or vulnerabilities. Audits reduce but do not eliminate risk. Exploits may result in loss of tokens, incorrect rewards, failed settlement flows, deposit disputes, or governance disruption.

13.11 Operational risk

The protocol may suffer downtime, failed integrations, data-provider outages, exchange API changes, inaccurate connectors, delayed reports, or infrastructure failures.

13.12 Cybersecurity risk

Wallet compromise, phishing, private-key loss, cloud compromise, endpoint compromise, or insider threats may affect holders, operators, or Rena services.

13.13 Data protection and privacy risk

Rena Labs' services may involve personal data or commercially sensitive data. Data protection laws such as GDPR may apply. The protocol must define controller/processor roles, data retention, data-subject rights, cross-border transfers, lawful bases, and security measures where relevant.

13.14 Tax risk

Token acquisitions, sales, rewards, airdrops, payments, and transfers may have tax consequences. Each participant is responsible for tax advice and reporting.

13.15 Governance risk

Governance may be concentrated, captured, inactive, or misaligned. Early governance may be foundation-led. Governance processes may change over time.

13.16 Counterparty risk

The Rena Protocol may depend on exchanges, market makers, data providers, cloud providers, TEE vendors, auditors, payment processors, and other counterparties. Their failure may affect services.

13.17 Legal entity and corporate risk

Foundation, token issuing, and service-provider structures may evolve over time. Changes in legal structure may affect rights, obligations, compliance, and disclosures.

14. Environmental Considerations

14.1 Overview

The RENA token is expected to be deployed on an EVM-compatible proof-of-stake network rather than a proof-of-work network. The environmental impact of token transfers should therefore primarily arise from the selected network's validator infrastructure, TEE compute workloads, cloud storage, AI inference, data transfer, and operational infrastructure.

Renaissance Foundation should publish environmental information that is reasonable for the final selected network and infrastructure stack, using available data from Rena Labs, infrastructure providers, and network-level sources.

14.2 Environmental impact categories

Category	Disclosure
Consensus mechanism	Expected proof-of-stake or equivalent
Energy consumption	To be estimated using selected network and infrastructure providers
Renewable energy share	To be requested from infrastructure providers where available
GHG emissions	To be estimated using recognized methodology where required
TEE compute impact	AI inference and confidential compute workloads consume energy; workload metrics to be tracked
Hardware impact	TEE and cloud infrastructure depend on specialized hardware with embodied carbon and supply-chain impacts

Mitigation measures	Efficient batching, workload optimization, cloud-region selection, renewable-energy provider preference, monitoring

15. Appendices

Appendix A: Legal Characteristics of RENA

RENA is intended to have the following legal characteristics:

- Utility token for access, settlement, governance signaling, and verified contribution.
- Not an asset-referenced token.
- Not an e-money token.
- Not designed to maintain a stable value.
- No redemption right against Renaissance Foundation or any affiliate.
- No claim on reserve assets.
- No equity, debt, revenue share, dividend, interest, or liquidation right.
- No passive yield.
- No staking, no buyback, and no burn mechanism.
- No ownership of Renaissance Foundation, protocol treasury, data, models, reports, or infrastructure.
- Transferability subject to legal, technical, jurisdictional, and platform restrictions.

Appendix B: Airdrop Eligibility and Compliance

Any airdrop is discretionary and may be changed, delayed, canceled, or restricted. Eligibility criteria, the claim period, and its duration will be announced with the campaign terms before any claim window opens. Eligibility may consider:

- Product usage.
- Verified contribution.
- Developer participation.
- Security research.
- Research participation.
- Community engagement.
- Anti-Sybil score.
- Jurisdiction and sanctions screening.
- KYC or risk checks where required.

Airdrops are not available to prohibited persons or jurisdictions. Airdrop communications do not promise value, liquidity, appreciation, or listing.