PROVISIONAL PATENT APPLICATION

Title of the Invention:

System and Method for Behavior-Based Coordination and Access Control in Decentralized Operational Networks

Inventor:

Dmitry Romanenko

Correspondence Address:

Republic of Kazakhstan, Almaty city, Mamyr 1 microdistrict, building 11, apartment 14, email - iam.equinomix@gmail.com, +7 775 443 60 18

Date of Filing:

Entity Status: Micro Entity

2. Field of the Invention

This invention relates to systems and methods for coordinating the operational and financial behavior of participants in decentralized economic networks. Specifically, it pertains to architectures that continuously gather, assess, and act on execution traces derived from operational, behavioral, and financial data, in order to regulate access, forecast risk, and tokenize infrastructure and behavior through smart contracts and digital credentials. The invention contributes to sustainable development goals, particularly SDG 8 (“Promote sustained, inclusive and sustainable economic growth”), SDG 9 (“Build resilient infrastructure”), SDG 12 (“Ensure sustainable consumption and production patterns”), and SDG 16 (“Promote peaceful and inclusive societies through transparency and institutional trust”).

3. Background of the Invention

Legacy enterprise resource planning (ERP) frameworks rely on static contracts, fixed role hierarchies, and manual reporting. These limitations reduce system responsiveness and introduce structural risks. Operational deviations are not tracked in real time, and contract breaches often remain undetected—contributing to workplace instability and underperformance (SDG 8). Siloed behavioral scoring mechanisms lack dynamic feedback loops and are rarely integrated into resource access or contractual enforcement logic. This separation reduces institutional accountability and transparency (SDG 16), especially in contexts requiring real-time trust signals.

Further, tokenization models in decentralized ecosystems typically represent static asset references without capturing the behavioral, operational, and financial context behind asset usage. This omission leads to inefficiencies in asset allocation and increases idle time of capital resources (SDG 12), while weakening regulatory alignment and investor visibility (SDG 9).The present invention addresses these deficits by providing a protocol-based architecture that enables behavioral governance, institutional auditability, and trace-driven redistribution mechanisms aligned with key sustainable development goals (SDG 8, 9, 12, 16).

4. Summary of the Invention

The invention introduces an integrated architecture that governs participant behavior in decentralized networks through statistical execution modeling and protocol-based access control. ERP systems collect operational, financial, and behavioral data. Telemetry and fatigue modules add situational context. A statistical engine constructs time-windowed behavior trajectories and classifies them as normal or high-risk.

An adaptive coaching module issues operational recommendations and tracks user responsiveness. Execution patterns are evaluated over observation windows (e.g., 7 days for drivers, 30–90 days for operators) to assess learning responsiveness. A behavioral rating aggregates template conformity, feedback adoption speed, and KPI consistency.

Smart contracts regulate access to infrastructure, capital, and governance privileges based on this rating. Financial buffers mitigate execution volatility.

The system establishes a shared cooperation layer for institutional participants, enabling decentralized but auditable role delegation. Entities may include, but are not limited to, banks, inspection agents, insurance firms, regulatory authorities, ESG assessors, infrastructure operators, and behavioral auditors. For instance, a financial institution may outsource vehicle inspection to a certified agent under protocol rules, ensuring on-chain record verifiability, behavioral accountability, and collateral integrity. This structure reinforces institutional trust and expands access to coordinated public-private service ecosystems.

The system includes:

- **non-transferable tokenized credentials** representing execution history, used for access rights and institutional trust scoring;
- **composite NFTs** representing tokenized physical assets enriched with condition data, contractual terms, and behavioral footprint;
- All investment interactions involving composite NFTs must be executed via the system-native utility token to ensure trace integrity, yield routing, and institutional auditability. External tokens shall not be recognized for routing protocol-based investments or accessing behavioral trace repositories.
- a **utility token** for external financial circulation, staking, and liquidity;
- a **protocol layer** serving as execution engine for yield enforcement, trace-based redistribution, and institutional agreement compliance.

Key modules align with specific SDG targets:

- Fatigue Assessment → SDG 8.8 (“Protect labor rights and promote safe working environments”)
- Composite NFT Issuance → SDG 9.3 (“Increase access to financial services and markets”)
- Normality Corridor → SDG 12.2 (“Achieve sustainable management of resources”)

- On-chain control logic → SDG 16.6 (“Develop effective, accountable and transparent institutions”)

All actions are on-chain verifiable, enabling auditability, risk prediction, and ESG-compliant governance. (Contributes to SDG 8, 9, 12, 16)

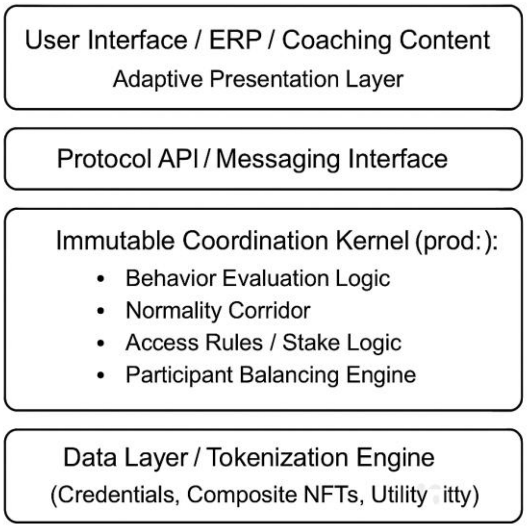
The system is designed for open-source implementation under a modular architecture. While the coordination kernel—comprising behavior evaluation logic, access control mechanisms, normality thresholds, and participant balancing rules—remains immutable and protected, external components such as user interfaces, ERP connectors, and localization modules may be freely adapted. This structure supports transparent and extensible deployments across domains and regions while preserving protocol compliance and integrity.

The invention addresses the structural gap between decentralized digital protocols (Web3) and the execution-based trust required in real-world economic environments. By modeling behavior trajectories from verifiable off-chain sources (ERP, telemetry, financial systems), and transforming them into protocol-governed access decisions, the system enables measurable and auditable coordination across physical and digital actors. This enables Web3 systems to interact with real-world execution in a statistically grounded and trust-preserving manner.
Additionally, operational roles—such as vehicle drivers, equipment operators, service providers, and other participants—execute recurring payments, including asset rental fees and system access charges, via the system-native utility token. These payments are on-chain recorded, contribute to execution trace, and serve as protocol-enforced contributions to the architectural rent mechanism. By embedding role-specific payments into the protocol, the system ensures

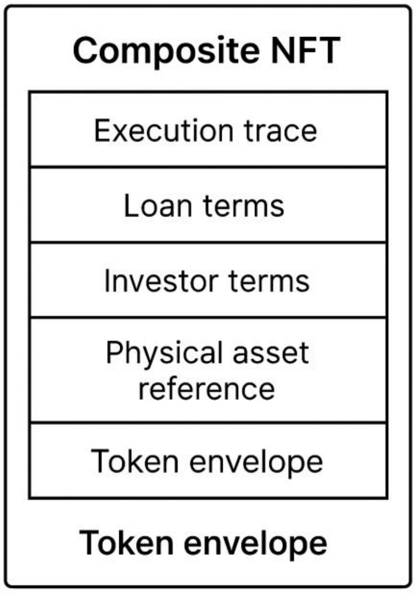
measurable participation, decentralized cost-sharing, and auditable compliance across all economic actors.

5. Brief Description of the Drawings

- **Figure 1** — Modular system architecture diagram illustrating behavioral flow: ERP → telemetry → normality corridor → coaching → behavioral rating → smart contract access control → financial buffers → composite NFT issuance → reputation layer → protocol meta-evaluation → shared cooperation layerModular system architecture diagram: ERP → telemetry → normality corridor → coaching → behavioral rating → access control via smart contracts → financial buffers →composite NFT issuance → protocol meta-evaluation


User Interface / ERP / Coaching Content
Adaptive Presentation Layer
Protocol API / Messaging Interface
Immutable Coordination Kernel (prod:):
• Behavior Evaluation Logic
• Normality Corridor
• Access Rules / Stake Logic
• Participant Balancing Engine
Data Layer / Tokenization Engine
(Credentials, Composite NFTs, Utility itty)

- **Figure 2** — schematic representation of a composite NFT structure including physical asset reference, loan terms, execution trace, and the token envelope. The figure illustrates how behavioral history and financial metadata are embedded into the tokenized digital asset for institutional-grade validation and protocol compliance.



6. Detailed Description (продолжение)

1. ERP Module Collects real-time operational, behavioral, and financial data from all participants. This includes income generation records, location metadata, schedule adherence, and peer interaction logs. The ERP layer acts as the root execution record across all roles (drivers, operators, investors). *(Supports SDG 9.1: "Develop quality, reliable infrastructure") and SDG 8.5: "Productive employment with real-time accountability")*

2. Telemetry Module Captures vehicular and mobile sensor data: GPS, CAN-bus, accelerometers, gyroscopes, and screen-based events. For low-instrumented participants or vehicles, the system applies comparative cohort analytics. *(Supports SDG 12.2: "Efficient resource use and asset utilization") and SDG 9.4: "Upgrade infrastructure for sustainability")*

3. Fatigue Assessment Module Evaluates driver wellness using smartphone-based sleep patterns, screen activity, and travel alignment. The resulting fatigue signal adjusts behavioral templates and protocol-level access policies. *(Supports SDG 8.8: "Protect labor rights and promote safe working environments")*

4. Normality Corridor Module Generates statistical behavior templates across configurable time windows (e.g., 24h, 7d, 30d) using IQR and z-score analysis. Template bounds adapt to variables such as time-of-day, seasonality, and traffic context. Deviations trigger classification into risk profiles, coaching recommendations, and compensation signaling. *(Supports SDG 12.2: "Reduce asset downtime via predictive usage analysis")*

5. Coaching Module Issues operational guidance based on deviation severity. Monitors implementation lag and trajectory correction to assess responsiveness. Observation windows are role-specific: 7 days (driver), 30–90 days (operator). Generates a behavioral adaptation index. *(Supports SDG 8.6: "Substantially reduce underperformance by enabling corrective feedback")*

6. Behavioral Rating Engine Computes participant score using weighted criteria: template conformity, feedback responsiveness, and KPI durability. Smart contracts consume this score to govern access privileges across infrastructure, capital, and governance roles. *(Supports SDG 16.6: "Develop transparent and accountable institutions")*

7. Smart Contract Access Layer Regulates access to infrastructure, token transfers, and governance privileges based on behavioral ratings and protocol-defined thresholds. Permissions adapt in real time according to performance. *(Supports SDG 16.6: "Develop effective, accountable and transparent institutions" and SDG 9.1: "Develop quality, reliable infrastructure")*

8. Financial Buffer Architecture Includes liquidity vaults, stabilization pools, and buyback logic triggered by deviation signals and asset-level failures. The buffer operates autonomously per role and asset category. *(Supports SDG 9.3: "Increase access to financial services" and SDG 12.2: "Ensure sustainable management of resources")*

9. Composite NFT Issuance Module Issues NFTs representing tokenized physical assets (e.g., vehicles). Metadata includes: — protocol-defined investor yield logic; — asset condition scores; — complete execution trace of participant interaction tied to income generation. The NFT functions as a composite object: physical reference + behavioral footprint + capital logic. *(Supports SDG 9.3: "Expand access to financial instruments" and SDG 12.2: "Reduce idle asset time"). **Application Example: Auto Loan Tokenization** NFTs may represent tokenized auto loan products. Metadata includes:*

– credit agreement terms (e.g., interest rate, duration);
– real-time Loan-to-Value (LTV) based on vehicle telemetry and condition data;
– borrower execution trace, including payment history and driving behavior.

Upon default or behavioral noncompliance, smart contracts may restrict vehicle re-registration or access to refinancing modules.

*(Supports SDG 8.10: “Expand access to financial services for SMEs” and SDG 9.3: “Increase institutional risk transparency”)

9a. Protocol-Payments from Operational Roles Operational participants—including, by way of example, vehicle drivers, equipment operators, and service agents—are required to execute system-level payments via the native utility token. These payments cover asset usage (e.g., rental fees), platform or ERP access charges, and any other service fees defined by deployment. All transactions are on-chain recorded, linked to execution trace and behavioral metrics, and contribute to architectural rent flows managed by the protocol.

10. Reputation and Credential Layer Execution history is tokenized as a **non-transferable credential token**, used for trust scoring, institutional validation, and stake verification. These tokens are non-fungible and restricted to internal system coordination. *(Supports SDG 16.6: “Promote transparent verification systems”) and SDG 8.5: “Ensure inclusive and performance-based access”)*

Application Example: Insurance Risk Scoring via Peer Matching**

Behavioral data collected via low-instrumented users (e.g., smartphone sensors) may be enriched and evaluated against professionally instrumented trajectories from fleet participants.

The system uses statistical peer matching to classify driving behavior, predict risk exposure, and generate underwriter-grade profiles.

Insurance providers may integrate this logic into dynamic premium structures (e.g., pay-as-you-drive policies), enabling cost-effective coverage personalization and improved actuarial accuracy.

*(Supports SDG 8.10: Financial access and affordability; SDG 16.6: Institutional transparency and accountability)

11. Protocol Core, Execution Engine and Meta-Evaluation Module

Serves as the autonomous execution engine, enforcing:

— behavioral-based access control;

— redistribution of funds upon trajectory deviation;

— enforcement of financial terms (e.g., 7.5% annualized yield on residual investment);

— institutional contract compliance without intermediaries;

— meta-evaluation of intervention outcomes and trajectory resilience.

The meta-evaluation module operates by continuously monitoring aggregated execution trajectories across all roles and observation windows. It calculates deviation clusters, improvement decay curves, and feedback absorption rates to assess systemic behavioral resilience.

Results are time-windowed and compared to prior baseline networks to identify structural fatigue, intervention efficacy, and risk propagation.

These meta-signals may be used to recalibrate access thresholds, redistribute incentives, or initiate audit requests automatically.

The process runs on-chain and may include predictive modules for systemic stress and failure probability.

(Supports SDG 16.6: Transparent and accountable institutional governance)

Yield and compensation logic are hardcoded at the protocol layer, independent of the tokenized asset class. *(Supports SDG 8.8, SDG 9.3, SDG 16.6)*

All system-compliant deployments are required to route yield, redistribution logic, and trace validation through the native utility token. The token serves as a mandatory gateway for investment execution, composite NFT verification, and access to protocol-wide meta-evaluation modules. Deployments that omit this integration shall be considered non-compliant and excluded from protocol-level auditability and institutional interoperability.

12. Secondary Market Module Enables asset or share transfer contingent upon behavioral compliance. Prior to execution, the system validates participant rating, execution trace, and tokenized credentials to ensure institutional-grade transfer conditions. *(Supports SDG 9.3: "Promote inclusive financial market participation" and SDG 16.6: "Enable audit-ready transactions")*

Open Modular Architecture and Coordination Kernel Integrity

The system architecture follows an open-source model, where external modules—such as ERP interfaces, local integrations, and coaching content—are designed for adaptation and localization.

However, the coordination kernel, including statistical behavior evaluation, normality corridor computation, access control logic, and participant balancing rules, is defined as immutable across deployments.

Deployments that modify the coordination kernel or omit integration with the native utility token shall be considered non-compliant and excluded from protocol-wide evaluation, access verification mechanisms, and institutional trust signaling. Only full protocol-compliant platforms may claim NFT trace validity, access meta-evaluation modules, and participate in system-level yield redistribution. This compliance structure preserves architectural rent across all compatible deployments and reinforces systemic transparency, traceability, and governance integrity.

This ensures cross-deployment integrity, interoperability, and resistance to manipulative modification. The protocol enforces execution-based access and fairness without relying on AI or opaque machine learning models. All coordination logic is deterministic and audit-ready. The design supports resource-sharing among multiple actors, including financiers, infrastructure providers, regulatory agents, and executors. Role-specific behaviors are evaluated uniformly through statistical norms, enabling decentralized cooperation without central arbiters. Local implementers may build interfaces, dashboards, or region-specific rule extensions, but may not alter the protected kernel logic without losing protocol compliance.

7. Claims

Claim 1. A system for coordinating operational and financial behavior of participants in decentralized economic networks, comprising: a. an ERP module configured to collect and store operational, financial, and behavioral data; b. a telemetry module configured to gather sensor data from mobile and vehicular sources; c. a normality corridor module configured to construct statistical behavior trajectories and flag deviations; d. a coaching module configured to issue executable recommendations and adapt feedback based on user response; e. a behavioral rating engine synthesizing behavior conformity, responsiveness, and KPI adherence; f. smart contracts evaluating this rating to regulate access to resources and capital; g. financial buffers triggered by volatility; h. a reputation layer issuing tokenized execution credentials; i. all actions and control decisions being on-chain verifiable. *(Supports SDG 8, 9, 12, 16)*

Claim 2. The system of claim 1, further comprising a fatigue assessment module configured to analyze mobile device screen activity and accelerometry to evaluate a driver's rest quality and integrate such evaluation into the behavioral profile. *(Supports SDG 8.8: "Protect labor rights and promote safe working environments")*

Claim 3. The system of claim 1, wherein the normality corridor module primarily operates using statistical analysis of peer cohort data, and may incorporate explainable machine learning models—such as logistic regression or interpretable boosting frameworks (e.g., XGBoost with SHAP)—when aligned with auditability and transparency requirements.

Claim 4. The system of claim 1, wherein the non-transferable tokenized credential instruments represent behavioral reputation markers or asset-linked records with embedded execution trace data used by financial institutions to validate collateral risk status in real time, consistent with Basel III compliance frameworks.

These instruments may also represent tokenized credit-based financial products, including auto loans, whereby embedded execution trace includes:

a) repayment history;

b) asset usage signals derived from telemetry;

c) behavioral compliance indicators affecting dynamic interest and risk rating.

(Supports SDG 9.3, SDG 8.10, SDG 16.6)

Claim 5. The system of claim 1, wherein the protocol core is configured to redistribute operational control or funds between participants when deviations from the normality corridor persist and threaten systemic buffers, without manual intervention.

Claim 6. The system of claim 1, wherein the smart contracts dynamically adapt fund distribution logic based on execution quality and system stability parameters, rather than predetermined fixed shares.

Claim 7. The system of claim 1, further including fiat-to-token and token-to-fiat gateways for seamless exchange between fiat currency and system tokens.

Claim 8. The system of claim 1, further including a stake/priority module configured to determine participant access levels based on stake amount and behavioral profile.

Claim 9. The system of claim 1, further including a behavioral scoring module configured to generate reliability scores based on execution history and adherence to the normality corridor.

Claim 10. The system of claim 1, further including a KYC/AML layer configured to ensure compliance with customer identification and anti-money laundering regulations. (Supports SDG 16.5: "Reduce corruption through transparent identity verification")

Claim 11. A method for coordinating operational and financial behavior of participants in decentralized economic networks, comprising the steps of: a. collecting operational, financial, and behavioral data via an ERP module; b. collecting telemetry data from vehicles and mobile devices to evaluate behavior and performance; c. dynamically calculating a statistical behavior corridor using IQR or z-score methods with contextual adjustments; d. issuing executable recommendations upon deviation, and adapting feedback based on observed participant response; e. aggregating learning responsiveness and KPI adherence into a behavioral rating; f. granting or revoking access via smart contracts based on this rating; g. issuing composite NFTs embedding asset data, investor terms, condition signals, and execution history. *(Supports SDG 8.8, SDG 9.3, SDG 12.2)*

Claim 12. The system of claim 1, wherein behavior assessment of a participant operating without professional-grade sensors is enhanced via comparative analytics derived from peer vehicles equipped with full-scale telemetric instrumentation.

Claim 13. The system of claim 1, wherein the normality corridor module constructs statistical behavior trajectories from time-windowed execution data, categorizes patterns associated with contract fulfillment as normal, and flags trajectories correlated with contract breach or operational instability as risky, enabling pre-emptive coaching or access limitation.

Claim 14. The system of claim 1, wherein the coaching module receives deviation signals and execution trajectory data from the normality corridor module, issues behavioral recommendations to participants, evaluates learning responsiveness through observed implementation lag and trajectory adjustment, and dynamically modifies recommendation frequency and structure accordingly.

Claim 15. The system of claim 14, wherein the coaching module monitors participant behavior over defined observation windows—comprising 7 days for drivers and 30 to 90 days for operators—compares post-recommendation execution trajectories to pre-recommendation baselines, and adjusts learning parameters and recommendation frequency based on measured improvement.

Claim 16. The system of claim 1, wherein the normality corridor module operates continuously, updates behavior templates in real time using sliding execution windows, and adjusts statistical thresholds based on contextual variables including time of day, seasonal factors, and systemic conditions.

Claim 17. The system of claim 1, wherein the normality corridor module performs predictive analytics by correlating current and historical execution data to estimate the probability of future contract breach, asset misuse, or safety violations, and transmits risk scores to downstream modules for proactive intervention.

Claim 18. The system of claim 1, wherein access to system resources and capital is regulated by smart contracts that evaluate a participant's behavioral rating, the rating being calculated from execution templates, coaching responsiveness, and sustained KPI performance, and wherein access is granted or revoked based on protocol-defined minimum threshold scores.

Claim 19. The system of claim 1, wherein the reputation layer comprises non-fungible tokens representing tokenized physical assets, each token embedding metadata including contractual investor reward terms, real-time asset condition metrics, and a historical execution trace of participant interactions, thereby forming a composite digital asset consisting of both the object and its behavioral footprint.

Claim 20. The system of claim 1, wherein the protocol core includes a meta-evaluation module configured to assess system-wide effectiveness by analyzing changes in aggregate participant execution trajectories over time and measuring the impact of behavioral interventions on the probability of successful contract fulfillment.

Claim 21.

The system of claim 1, wherein behavioral patterns are analyzed using statistical methods, including but not limited to interquartile range and z-score modeling, using statistical methods including interquartile range and z-score modeling, and optionally integrating explainable machine learning techniques compatible with institutional audit and compliance standards.

Claim 22.

The system of claim 1, wherein execution traces from low-instrumented users are enriched and evaluated via comparative analytics against professional-grade telemetry records from fleet-operated vehicles.

Claim 23.

The system of claim 1, wherein access to infrastructure or capital is granted or revoked based on a statistically derived behavioral rating calculated from execution templates and performance deviation metrics.

Claim 24.

The system of claim 1, wherein composite non-fungible tokens embed behavioral execution traces that serve as validation logic for resale, refinancing, or collateral reassessment.

Claim 25.

The system of claim 1, wherein fatigue signals derived from mobile device usage patterns dynamically modulate protocol-level access thresholds and infrastructure availability.

Claim 26.

The system wherein behavioral profiling is performed using only statistical models based on time-windowed excluding the use of non-transparent or non-interpretable AI models, and permitting explainable machine learning techniques such as SHAP-interpretable classifiers or statistical regressions, subject to institutional auditability.

Claim 27.

The system wherein behavioral metrics from low-sensor devices are mapped to high-fidelity peer traces to create predictive risk profiles.

Claim 28.

The system wherein non-transferable credential tokens encode execution history, including behavioral responses to fatigue, deviation coaching, and contractual compliance.

Claim 29.

A coordination protocol wherein the core logic comprising behavioral evaluation, normality corridor computation, access control rules, and participant balancing mechanisms is immutable across all protocol-compliant deployments, while external interface modules may be adapted.

Claim 30.

The coordination logic of claim 29, wherein behavior evaluation is performed using deterministic statistical functions and, where appropriate, explainable machine learning models—including interpretable boosting algorithms, logistic regression, or SHAP-weighted classification—provided all models support on-chain auditability and institutional compliance.

Claim 31.

The protocol of claim 29, implemented in an open-source architecture, wherein any modification of the coordination kernel results in loss of compliance status and protocol recognition.

Claim 32.

The system of claim 29, wherein participants include, but are not limited to, financiers, infrastructure operators, resource users, regulatory agents, and execution agents, all of whom are evaluated under uniform behavioral metrics.

Claim 33.

A coordination protocol as in claim 29, wherein a system usage fee is embedded into the transaction flow, calculated as a percentage of the value transacted within the protocol, and automatically routed to a designated protocol treasury or architect wallet.

Claim 34.

The protocol of claim 29, wherein access to aggregated behavioral datasets, including but not limited to execution templates, driving patterns, risk classifications, and responsiveness metrics, is subject to a data access fee collected by the protocol and routed to a designated treasury or governing entity.

Claim 35.

The system of claim 29, wherein derivative or white-label deployments of the coordination protocol are subject to sublicensing terms defined by the protocol owner, including but not limited to interface branding, data synchronization rights, and integration conditions.

Claim 36.

The system of claim 1, further comprising a system-native utility token configured to support financial circulation, staking mechanisms, and external liquidity flows; wherein said token is required for trace-binding, composite NFT validation, and protocol compliance across all protocol-compliant deployments.

Claim 37.

The system of claim 36, wherein all deployments utilizing the coordination kernel shall be subject to architectural rent via predefined system usage and data access fees, automatically routed to the architect wallet, regardless of external interface customization or local token integration.

Claim 38.

The system of claim 1, wherein operational participants—including but not limited to vehicle drivers, equipment operators, service agents, and other actors—execute recurring payments—such as asset rental fees, system usage charges, and service fees—via the system-native utility token, said payments being on-chain recorded, trace-linked, and contributing to behavioral rating, access governance, and architectural rent redistribution governed by the protocol.

Claim 39.

The system of claim 1, wherein behavior modeling may include explainable machine learning algorithms—such as gradient boosting models with SHAP interpretation, logistic regression classifiers, or decision tree-based scoring—selected for compatibility with protocol-level transparency, institutional auditability, and SDG-aligned governance.

Abstract

A system and method for governing operational and financial behavior in decentralized networks using statistical modeling and protocol-based access control. Time-windowed execution trajectories are built from ERP, telemetry, fatigue, and financial data, with contextual template

updates and deviation-triggered coaching. Behavioral ratings derived from conformity and responsiveness regulate infrastructure and capital access via smart contracts.

Execution history is tokenized into non-transferable credentials, while composite NFTs represent physical assets enriched with condition signals and behavioral trace. A system-native utility token enables circulation, staking, liquidity, and is required for trace-binding and institutional auditability.

A meta-evaluation layer assesses systemic resilience. All modules operate on-chain, enabling auditability, SDG alignment (8, 9, 12, 16), and compliance with institutional frameworks. Composite NFTs may encode tokenized debt instruments combining repayment, condition, and behavior—reducing default risk, improving credit scoring, and expanding access to asset-backed lending. (Aligned with SDG 8.10 and SDG 9.3)