CYBER-PHYSICAL AUTONOMOUS COMMERCE

Machine-to-machine infrastructure, spatial proof and physical settlement protocol

CPAC

Document status	Version	Date	Scope
Technical proposal	1.1	September 2026	Protocol, economics and roadmap

READING NOTE

This document describes a proposed protocol architecture and illustrative economic model. Parameters remain subject to implementation testing, security review, governance approval and applicable law.

Institutional whitepaper | Prepared for technical, strategic and diligence review

Executive summary

Autonomous software is beginning to transact with the physical world. An AI agent may need to buy charging time, request a delivery, rent edge compute, or procure a sensor reading without a human approving each event. Existing infrastructure generally separates machine identity, payment, telemetry and service accountability across different systems. That separation creates friction exactly where machine commerce requires speed, low-value settlement and measurable service quality.

Cyber-Physical Autonomous Commerce (CPAC) is a proposed protocol stack for machine-to-machine commerce. It is designed to connect autonomous agents with physical service providers through three coordinated layers: CPAC-Node for hardware identity and presence attestations; CPAC-Pay for low-friction micro-tariff settlement; and CPAC-Proof for telemetry-backed service verification and automated economic remedies.

> **CORE THESIS**
> The machine economy needs a settlement and assurance layer that treats physical service delivery as a verifiable economic event, not merely as an off-chain API response.

The protocol does not require CPAC to manufacture hardware or replace every underlying blockchain. Its intended role is a coordination and settlement layer that can integrate with existing devices, chains and marketplaces while providing a common standard for identity, payment authorization, physical evidence and SLA closeout.

The native CPAC token is proposed as a utility asset for hardware collateral, protocol fees, slashing and governance. The current model fixes total supply at 1,000,000,000 tokens and assumes 25.0% circulating at TGE. All token and financial figures in this paper are design assumptions, not forecasts of market value or investment returns.

At a glance

Dimension	Current design position
Problem addressed	Trust, latency and accountability in autonomous purchases of physical services
Protocol layers	CPAC-Node, CPAC-Pay and CPAC-Proof
Primary users	Autonomous agents, machine operators, infrastructure providers and integrators
Settlement model	Off-chain micro-streaming with batched on-chain settlement
Assurance model	Device identity, presence evidence, telemetry and collateralized remedies
Token supply	1,000,000,000 CPAC; fixed cap in the current proposal
Launch posture	Phased testnet and security validation before production-scale deployment

Contents

This document map is intentionally static for reliable viewing across Word, LibreOffice and PDF readers. The section headings are also formatted as navigable Heading 1 and Heading 2 styles.

The opportunity: autonomous commerce enters the physical world

The transition from digital agents to physical execution changes the requirements of commerce. A software agent can complete a digital exchange with a signed message and a ledger state transition. A physical service introduces additional questions: Is the machine authentic? Is it where it claims to be? Did it perform the promised service? Can a buyer obtain a remedy without relying on a centralized operator?

CPAC frames this transition as a three-stage evolution:

1. **Pure digital financialization.** Agents operate in digital markets, trading tokens, managing liquidity and calling smart contracts.
2. **Human-directed physical infrastructure.** DePIN-style networks coordinate hardware such as GPUs, storage, connectivity and sensors, but demand and service selection remain primarily human-mediated.
3. **Autonomous machine commerce.** Agents become direct buyers and service coordinators, purchasing physical capacity in real time under explicit price, location, performance and settlement constraints.

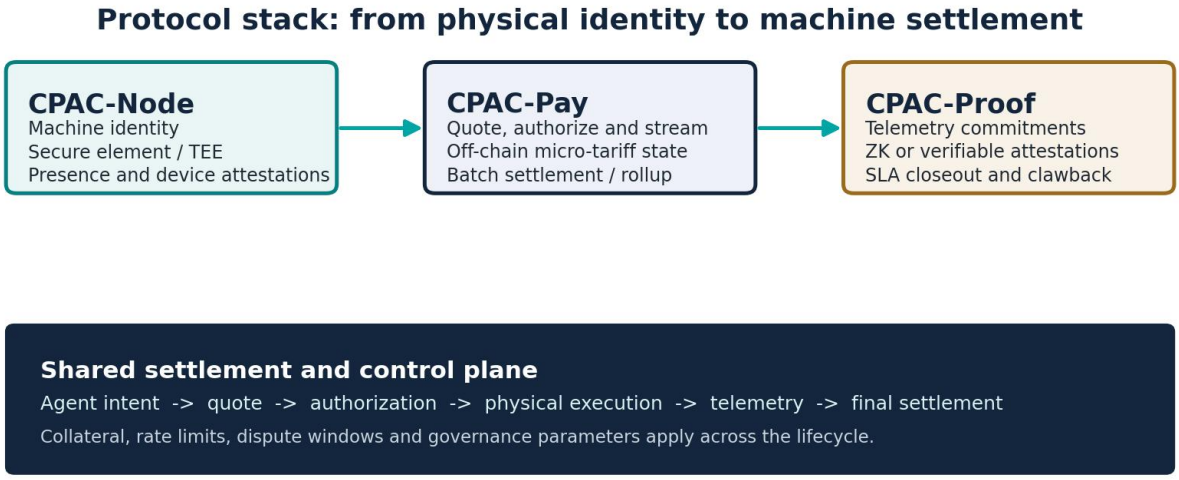

Figure 1. CPAC protocol stack: identity, settlement and physical proof are coordinated as one transaction lifecycle.

The M2M commerce trilemma

A machine economy cannot scale if identity, payment and service quality are resolved independently. CPAC focuses on three linked constraints:

Constraint	Why existing workflows struggle	CPAC design response
Machine identity and zero-trust risk	A buyer may not know whether a device is genuine, its position is authentic or its firmware remains within policy.	Secure-element or TEE-backed machine identity, signed attestations and presence evidence.
Micropayment friction and latency	Continuous services may involve sub-cent events and millisecond decisions that are uneconomic to settle one by one on a base chain.	Quota signatures, state channels and batched settlement to reduce per-event overhead.
Physical SLA enforcement	A failed delivery, degraded charging session or corrupted sensor feed needs an objective evidence path and an economic remedy.	Telemetry commitments, verification rules, collateral and automated clawback at closeout.

DESIGN BOUNDARY

CPAC is intended to coordinate and settle machine commerce. It does not make a blanket claim that cryptographic evidence can eliminate every physical-world uncertainty; sensor quality, oracle design, hardware compromise and jurisdictional enforcement remain material risks.

Protocol architecture

CPAC is organized as a modular stack so that identity, payment and physical assurance can evolve independently while remaining bound to one service lifecycle. The architecture is designed for integration with existing hardware and settlement environments, subject to adapter and security requirements.

Layer 1: CPAC-Node

CPAC-Node provides the identity and security substrate for participating hardware. Each registered device is expected to have a cryptographic root of trust, ideally through a Secure Element or Trusted Execution Environment. The registration record can include hardware class, firmware policy, operator authorization, service capabilities and revocation state.

- Chip-level machine identity: a device signs registration and service messages with a key anchored in hardware-backed protection.
- Proof of Physical Presence (PoPP): multiple evidence sources, such as RF triangulation, satellite telemetry and privacy-preserving location proofs, can be combined to make location spoofing more difficult.
- Lifecycle controls: registration, firmware changes, key rotation, maintenance windows and revocation are treated as explicit state transitions.

Layer 2: CPAC-Pay

CPAC-Pay is designed for continuous, low-value service consumption. Instead of writing one base-layer transaction for every second of charging, byte of bandwidth or unit of compute, an agent and provider can open a bounded micro-tariff state, exchange signed usage updates and settle the resulting net amount in batches.

- Micro-tariff state channels: the channel records authorized limits, pricing terms, service identifier and settlement conditions.
- Quota signatures: pre-allocated authorization reduces the need for a device to wait for a fresh base-layer confirmation before performing each micro-event.
- Batch settlement: validators or rollup infrastructure aggregate valid updates and commit the final state according to the protocol's settlement rules.

Layer 3: CPAC-Proof

CPAC-Proof connects service performance to evidence. A device or gateway commits to telemetry such as voltage, temperature, RPM, altitude, delivery milestones or bandwidth. The protocol can use zero-knowledge proofs where privacy is material, or other verifiable attestations where a simpler construction is more appropriate.

- Telemetry commitments: the service record preserves the minimum evidence needed for later verification without requiring all proprietary data to be public.
- SLA closeout: a service is closed only after the agreed evidence window and settlement conditions are satisfied.
- Automated remedies: where a breach is proven under the applicable rule, collateral can be deducted, payment adjusted or a claim routed to the physical indemnity vault.

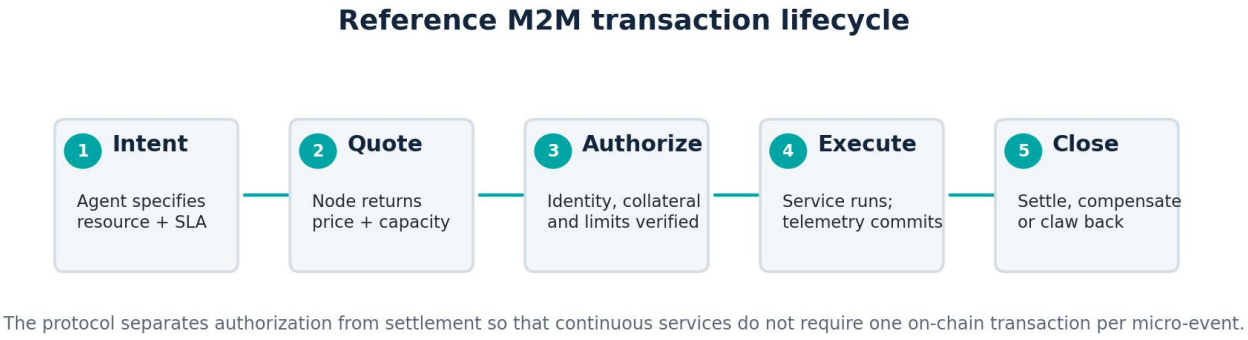

Figure 2. Reference transaction lifecycle from agent intent to final settlement or remedy.

Reference transaction model

The following sequence is a reference design rather than a final wire specification. Implementations may optimize message formats and batching, but should preserve the separation between intent, authorization, execution evidence and settlement finality.

Stage	Primary actor	Required state	Output
Intent	AI agent or orchestrator	Resource class, quantity, location, time window, budget and SLA terms	Signed service request
Quote	Machine operator / provider	Available capacity, tariff, collateral, identity and service policy	Signed quote and capacity reservation
Authorization	CPAC policy and settlement layer	Machine identity, operator permissions, limits, balance and risk parameters	Bound authorization and channel state
Execution	Physical machine	Authorized task, telemetry policy and heartbeat requirements	Usage updates and evidence commitments
Closeout	CPAC-Proof and settlement layer	Evidence window, SLA thresholds, dispute window and final amounts	Payment, refund, penalty or claim

Message binding and replay resistance

A production implementation should bind authorization and evidence to a unique service context. At minimum, signatures should cover the machine identity, service identifier, chain or domain separator, authorization nonce, tariff terms, relevant time or block window and the prior state commitment. This prevents a valid message from being detached from its original service or replayed in a different context.

The practical security objective is not merely to prove that a message was signed. It is to prove that the message was signed by the intended machine or operator, for the intended service, within the intended economic and temporal boundary.

> **IMPLEMENTATION PRINCIPLE**
> Every settlement outcome should be reproducible from the signed service state, the admissible evidence set and the published policy parameters. If a result cannot be independently reconstructed, it should not be treated as protocol finality.

Actuarial models and machine credit

Physical service quality is variable. CPAC therefore proposes a dynamic reputation and pricing layer that translates observed service behavior into transparent risk parameters. The model should be calibrated from real operating data and should never be treated as a substitute for hardware security, insurance capital or human incident response.

Physical Machine Score

For a registered machine, the illustrative Physical Machine Score is:

ILLUSTRATIVE MODEL

$$PMS_t = \mu1 \times U_{uptime} + \mu2 \times S_{SLA\text{-}pass} + \mu3 \times (1 - D_{telemetry\text{-}anomaly}) + \mu4 \times \ln(1 + Q_{staked})$$

The score is normalized to a 0-100 range. The parameter weights are governance and calibration variables, not fixed scientific constants. They should be accompanied by confidence intervals, data-quality flags and a mechanism for correcting unreliable or manipulated telemetry.

Variable	Meaning	Control consideration
U_{uptime}	Uptime ratio and operational response latency	Must distinguish planned maintenance from unexplained downtime.
$S_{SLA\text{-}pass}$	Historical success rate against committed service terms	Should be weighted by task value, recency and evidence quality.
$D_{telemetry\text{-}anomaly}$	Frequency of abnormal sensor variance	Requires anomaly definitions that are robust to normal operating conditions.
Q_{staked}	CPAC collateral posted by the hardware owner	Collateral improves economic alignment but cannot prove physical performance by itself.
$\mu1 \ldots \mu4$	Normalized model weights where $\Sigma\mu i = 1$	Published by policy and subject to governance, monitoring and review.

Dynamic physical tariff

The illustrative price function is:

ILLUSTRATIVE MODEL

$$Price_t = BaseFee + \theta1 \times Congestion_{spatial} + \theta2 \times (1 - PMS_t / 100) + RiskPremium_{slashing}$$

Under this design, a high-score machine in an uncongested location can approach the base fee, while a lower-score machine must compensate buyers for additional delivery risk. The model must include anti-manipulation controls: a provider should not be able to lower its risk premium through self-generated telemetry, circular usage or short-lived collateral deposits.

Insurance and remedy separation

Collateralized slashing and an indemnity vault serve different functions. Collateral is a direct economic bond posted by the provider. The vault is a pooled reserve for eligible physical incidents that exceed or fall outside a provider's bond, subject to policy. Neither mechanism guarantees full recovery in every event; coverage limits, exclusions, claims evidence and reserve sufficiency must be explicit.

Token utility and economic design

CPAC is designed around a utility token with four proposed functions: hardware collateral, protocol settlement fees, slashing and governance. The model should be implemented so that token price volatility does not silently change the real economic obligations of physical service providers. Where possible, service obligations and claim settlement should be denominated in stable units, while CPAC remains the protocol utility and governance asset.

Key parameters

Parameter	Current proposal
Token name	Cyber-Physical Autonomous Commerce
Ticker	$CPAC
Total supply	1,000,000,000 tokens; fixed cap in the current model
TGE initial circulating supply	250,000,000 tokens, or 25.0% of total supply
Primary utilities	Hardware collateral, M2M settlement fees, slashing and governance

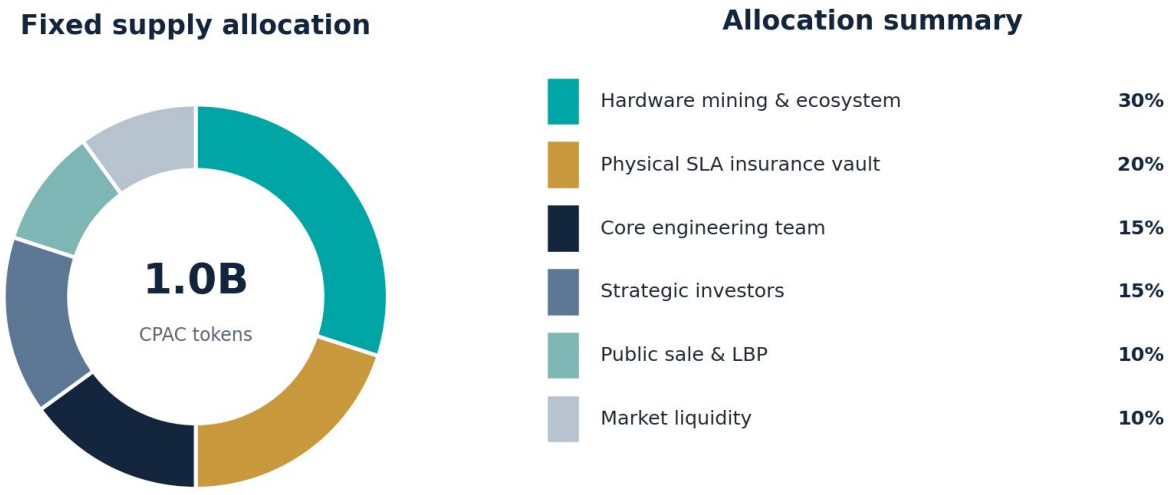

Figure 3. Proposed fixed-supply allocation. Percentages and vesting remain subject to final legal, technical and governance review.

Allocation and vesting

Pool	Category	Share	Amount	TGE	Cliff	Vesting / use
PUB	Public sale and LBP launch	10.0%	100,000,000	100,000,000	0 months	100% unlocked at TGE for market discovery.
ECO	Hardware mining and ecosystem	30.0%	300,000,000	50,000,000	0 months	50M for node activation; 250M emitted over 60 months against verified physical delivery.

Pool	Category	Share	Amount	TGE	Cliff	Vesting / use
LIQ	Exchange and market liquidity	10.0%	100,000,000	100,000,000	0 months	Locked into approved DEX/CEX pools to support M2M settlement liquidity.
INS	Physical SLA insurance vault	20.0%	200,000,000	0	3 months	Three-month cliff, then 48-month linear monthly vesting for eligible physical claims.
TEA	Core engineering team	15.0%	150,000,000	0	12 months	Twelve-month cliff, then 36-month linear monthly vesting.
INV	Strategic investors	15.0%	150,000,000	0	6 months	Six-month cliff, then 24-month linear monthly vesting.
Total	-	100.0%	1,000,000,000	250,000,000	-	Current design total.

ECONOMIC DISCLOSURE

Allocation percentages describe distribution, not value creation. Token utility, emissions, liquidity operations and vesting mechanics must be tested for concentration, sell pressure, governance capture and regulatory classification before launch.

Fee routing and deflationary mechanism

The current design proposes a 0.05% protocol fee on M2M settlement volume. The economic split is described as follows:

Use of protocol fee	Share	Intended function
Permanent burn	50%	Reduce supply through an auditable smart-contract burn mechanism.
CPAC-Proof indemnity vault	30%	Replenish reserves for eligible physical SLA events.
veCPAC governance stakers	20%	Compensate governance participants under approved policy.

The table above should be reconciled with any revenue forecast before publication. In particular, burn value depends on which fee streams are included, the actual settled volume and the CPAC token price at the time of execution.

Business model and illustrative operating scenarios

The protocol's potential revenue streams are linked to the lifecycle of physical machine commerce. They are presented as operating hypotheses, not guaranteed revenue or financial forecasts.

Revenue stream	Illustrative mechanism	Key driver
Machine registration	$10-$50 CPAC-equivalent fee for Machine-DID issuance and Secure Element provisioning	Number and class of registered machines
M2M settlement	0.05% protocol fee on settled machine-to-machine volume	Transaction volume, average service duration and netting efficiency
SLA underwriting	1.0% service surcharge for eligible higher-value tasks requiring risk coverage	Covered volume, claim frequency and reserve policy
Enterprise integrations	Commercial integration, validation or service fees where adopted	Deployment scope and support requirements

Illustrative operating scenarios

The following scenarios preserve the source model's adoption and volume assumptions. They are intended to show how protocol revenue scales with network activity; they are not a prediction of adoption, token price or profitability.

Scenario	Connected nodes	Annual M2M volume	Micropayment fee	SLA underwriting	Illustrative CPAC-directed value
Bootstrapping	10,000	$50,000,000	$25,000	$100,000	$62,500
Growth	500,000	$2,000,000,000	$1,000,000	$5,000,000	$3,000,000
Scale	10,000,000+	$50,000,000,000	$25,000,000	$100,000,000	$62,500,000

Forecast interpretation

The scenarios assume that connected physical nodes, settled volume and underwriting income grow together. Actual performance would depend on integration cycles, hardware reliability, regional regulation, customer acquisition, liquidity, claims experience and the share of volume that is economically suitable for CPAC settlement. Before institutional use, the model should include sensitivity cases for slower adoption, lower utilization, higher claims, fee compression and reserve losses.

Strategic positioning and integration thesis

CPAC is positioned as a specialized commerce and assurance layer rather than a general-purpose hardware network or a single-resource marketplace. The central thesis is integration: connect existing physical capacity to autonomous demand using a common trust and settlement language.

Dimension	General-purpose DePIN L1	Compute marketplaces	CPAC design position
Primary position	Ledger and incentive layer for broad hardware networks	Marketplace for GPU or compute rental	M2M commerce settlement and physical SLA assurance
Target consumer	Human operators and users deploying hardware	Software developers renting compute	Autonomous agents purchasing physical resources
Settlement	Standard block-based transactions	Hourly or monthly batch settlement	Micro-streaming state with batched settlement

Dimension	General-purpose DePIN L1	Compute marketplaces	CPAC design position
Risk model	Network-level incentives and operator reputation	Resource availability and rental performance	Identity, telemetry, collateral and policy-based remedies
Integration role	Base infrastructure or network-specific deployment	Resource-specific marketplace	Adapter and clearing layer across physical service categories

The differentiation is conditional

A specialized protocol does not automatically create a defensible market position. CPAC's differentiation will depend on whether it can demonstrate lower settlement friction, better evidence quality, credible collateralization and easier integration than a combination of existing chain infrastructure, device platforms and centralized service providers. The roadmap therefore prioritizes testable primitives over broad category claims.

Governance, controls and operating policy

Institutional adoption requires clear ownership of policy decisions. CPAC governance should separate protocol parameters from operational administration, and should make changes auditable and time-bounded.

Control area	Minimum policy requirement
Parameter governance	Publish tariff, collateral, score-weight, reserve and slashing parameters with effective dates and change history.
Hardware admission	Define device classes, key requirements, firmware baseline, operator eligibility and revocation procedures.
Evidence policy	Specify admissible telemetry sources, confidence thresholds, missing-data handling and dispute windows.
Reserve management	Publish vault accounting, eligible claims, coverage limits, replenishment rules and insolvency treatment.
Emergency response	Define pause, rate-limit and incident procedures without relying on opaque or unilateral state changes.
Auditability	Maintain reproducible state transitions, signed policy versions and independent security review artifacts.

Governance should also address data rights. Physical telemetry may reveal routes, industrial processes, energy use or commercial relationships. The protocol should minimize public disclosure, separate proof from raw data where possible and state who can access, retain or challenge evidence.

> **INSTITUTIONAL CONTROL PRINCIPLE**
> No economic remedy should be triggered by an unpublished rule, an unversioned model or evidence that the affected party had no reasonable way to inspect or contest.

Roadmap and validation gates

The roadmap is structured around validation gates. Each phase should produce evidence that the relevant primitive works under load, failure and adversarial conditions before the next phase expands economic exposure.

Timing	Milestone	Validation focus

Timing	Milestone	Validation focus
Q4 2026	Physical network alpha	Release CPAC-Node Machine-DID SDK and Secure Element integration specification; launch CPAC-Pay M2M micropayment testnet; publish baseline protocol schemas.
Q1 2027	Hardening and pilots	Run device identity, presence, channel-closeout and telemetry integrity pilots with constrained device classes; begin independent security review.
Q2 2027	Proof and settlement beta	Test CPAC-Proof evidence policies, dispute windows, reserve accounting and batched settlement under simulated and field conditions.
Q3 2027	Controlled production readiness	Complete audit remediation, incident response drills, economic stress tests and integration readiness assessment.
Later	Network expansion	Expand device categories and geographic coverage only where evidence quality, legal posture, liquidity and operational support are adequate.

Go / no-go criteria

- Security: key custody, message binding, replay resistance, channel closeout and upgrade paths pass independent review.
- Reliability: the system handles missing telemetry, delayed messages, device restart, network partition and duplicate submissions deterministically.
- Economics: stress tests cover fee compression, low utilization, high claims, token volatility and reserve depletion.
- Operations: operators can register, maintain, rotate and revoke devices without creating unbounded manual dependencies.
- Legal and data: target jurisdictions, token utility, coverage terms, telemetry rights and consumer-facing disclosures are reviewed before launch.

Risks and limitations

The protocol's value proposition depends on multiple systems working together. Institutional diligence should treat the following as first-order risks rather than footnotes.

Risk	Why it matters	Mitigation direction
Hardware compromise	A compromised device can produce valid-looking messages from an invalid physical state.	Hardware roots of trust, measured boot, remote attestation, key revocation and anomaly monitoring.
Location and oracle manipulation	No single location or telemetry source is universally reliable.	Multi-source evidence, confidence scoring, challenge mechanisms and conservative coverage rules.
Telemetry privacy	Proof data may reveal sensitive commercial or personal information.	Data minimization, selective disclosure, retention limits and access controls.
Settlement and bridge risk	Adapters, rollups and external chains add failure and liquidity dependencies.	Limit exposure, isolate domains, test recovery and publish finality assumptions.

Risk	Why it matters	Mitigation direction
Reserve insufficiency	A vault cannot pay claims beyond its available capital and policy limits.	Coverage caps, reserve ratios, stress tests, exclusions and transparent accounting.
Token and market risk	Volatility and concentration can impair collateral, governance and liquidity.	Stable-unit obligations, limits, vesting, concentration monitoring and circuit breakers.
Regulatory and contractual risk	Physical services, payments, insurance and token activity may be regulated differently by jurisdiction.	Jurisdictional analysis, qualified counsel, clear terms and staged deployment.
Adoption risk	The network requires both providers and agent-side demand to reach useful liquidity.	Start with constrained verticals where service value and evidence requirements are clear.

NO GUARANTEE

Cryptographic settlement can improve coordination and auditability, but it cannot guarantee that a physical service will be safe, lawful, profitable, available or fully recoverable after failure.

Conclusion

The next phase of autonomous systems will require more than intelligent software. Agents will need dependable access to power, bandwidth, compute, logistics, storage and other physical resources. Those interactions need a shared vocabulary for identity, authorization, evidence and settlement.

CPAC proposes that vocabulary as a modular protocol stack. CPAC-Node anchors the machine identity. CPAC-Pay reduces friction for continuous micro-settlement. CPAC-Proof connects physical execution to verifiable evidence and economic remedies. The design is deliberately compatible with a multi-chain, multi-device environment, while acknowledging that security, data quality, reserve capital and regulation remain decisive.

The project's credibility will be established through implementation evidence: constrained pilots, adversarial testing, transparent economics, independent audits and clear operating policies. If those validation gates are met, CPAC can serve as a specialized coordination layer for a more autonomous physical economy.

Appendix A: terminology

Term	Working definition
AI agent	Autonomous or semi-autonomous software that can request, authorize or coordinate physical services under defined policies.
CPAC-Node	Identity and security layer for registered physical machines and their operators.
CPAC-Pay	Micro-tariff and settlement layer for bounded, continuous machine-to-machine payments.
CPAC-Proof	Evidence and SLA layer for telemetry commitments, verification and remedies.
Machine-DID	Decentralized identifier or equivalent cryptographic identity record for a physical device.
PoPP	Proof of Physical Presence; a collection of evidence used to make location claims more credible.
SLA	Service-level agreement defining measurable service commitments and remedies.
Collateral	Economic bond posted by a provider and subject to policy-based slashing or claim treatment.
Indemnity vault	Pool of assets reserved for eligible covered events under published coverage rules.
State channel	Off-chain exchange of signed state updates followed by batched or net settlement.

Appendix B: model assumptions and publication discipline

- All supply, allocation, fee, vesting and scenario figures in this version are design parameters or illustrative assumptions.
- Forecast scenarios should be updated when testnet telemetry, pilot utilization, claims data or integration costs become available.
- A production release should publish versioned protocol specifications, contract addresses, audit reports, reserve statements and change logs.
- Any public token distribution or underwriting product requires a separate legal and compliance assessment in each target jurisdiction.
- The protocol should disclose what is guaranteed by cryptography, what depends on external attestations and what remains a contractual or operational promise.

DOCUMENT STATUS

This is an institutional-format technical proposal. It is suitable for architecture review and diligence discussion, but it is not a final protocol specification, securities offering memorandum, insurance policy or investment recommendation.