

# Agent Contracts: A Formal Framework for Resource-Bounded Autonomous AI Systems

Qing Ye<sup>1</sup> and Jing Tan<sup>2</sup>

<sup>1</sup> Independent Researcher [yeqi519@gmail.com](mailto:yeqi519@gmail.com)

<sup>2</sup> Independent Researcher [jt看@live.de](mailto:jt看@live.de)

**Abstract.** The Contract Net Protocol (1980) introduced coordination through contracts in multi-agent systems. Modern agent protocols standardize connectivity and interoperability, yet none provide formal resource governance—normative mechanisms to bound *how much* agents may consume or *how long* they may operate. We introduce *Agent Contracts*, a formal framework that extends the contract metaphor from task allocation to resource-bounded execution. An Agent Contract  $C = (I, O, S, R, T, \Phi, \Psi)$  unifies input/output specifications, multi-dimensional resource constraints, temporal boundaries, and success criteria into a coherent governance mechanism with explicit lifecycle semantics. For multi-agent coordination, we establish conservation laws ensuring delegated budgets respect parent constraints, enabling hierarchical coordination through contract delegation. Empirical validation across four experiments demonstrates 90% token reduction with  $525\times$  lower variance in iterative workflows, zero conservation violations in multi-agent delegation, and measurable quality-resource tradeoffs through contract modes. Agent Contracts provide formal foundations for predictable, auditable, and resource-bounded autonomous AI deployment.

## 1 Introduction

In late 2025, an engineering team deployed a multi-agent research system with four specialized agents. Two agents fell into a recursive clarification loop, running undetected for eleven days. When the invoice arrived, the team discovered a \$47,000 API bill [33]. The system had no stop conditions, no budget limits, and no real-time cost monitoring. This incident encapsulates a fundamental problem—we have built AI agents capable of autonomous action but lack formal mechanisms to bound their behavior.

Such failures reflect systemic gaps, not implementation bugs [15]. Gartner predicts that over 40% of agentic AI projects will be canceled by 2027 due to escalating costs or inadequate risk controls [20], even as agentic AI is projected to appear in 33% of enterprise software by 2028 [19]. A recent MIT Sloan study finds that 35% of organizations already deploy agentic AI, with leaders citing the tension between *supervision and autonomy* as a core challenge requiring centralized governance infrastructure [45]. Agents are becoming capable of sustained autonomous operation spanning hours or days [47, 9], yet the protocols governing

them address *connectivity* and *interoperability* but not *resource governance*—how much an agent may consume or how long it may operate.

**Agent Contracts** address this gap by extending the contract metaphor from task allocation to resource governance. Where the Contract Net Protocol [57] asks “who should do this task?”, Agent Contracts ask “within what bounds may this task be performed?” We draw on contract theory from economics, coordination theory from distributed systems, and resource-bounded computation from real-time systems to form a formal framework for resource-bounded autonomous AI.

This paper makes two contributions. First, we define an Agent Contract as a formal tuple  $C = (I, O, S, R, T, \Phi, \Psi)$  that unifies input/output specifications, resource constraints, temporal boundaries, and success criteria into a coherent governance mechanism. Second, we establish conservation laws for multi-agent systems that ensure budget discipline across delegation hierarchies, enabling composable coordination patterns where contracting itself becomes an agent capability. We validate these contributions across four experiments demonstrating 90% token reduction in iterative workflows, zero conservation violations in multi-agent delegation, and measurable quality-resource tradeoffs. Together, these contributions provide formal foundations for explicit resource governance in autonomous AI systems.

## 2 Theoretical Foundations

Agent Contracts draw on three theoretical traditions: contract theory from economics, multi-agent coordination from computer science, and resource-bounded computation from real-time systems.

**Contract Theory.** Bolton and Dewatripont (2005) [11] formalize how agreements are constructed under asymmetric information. Three concepts apply to agent governance: *moral hazard* (hidden actions; in LLM agents, unpredictable resource consumption), *incomplete contracts* (separating success criteria from execution strategies) [27], and *mechanism design* (specifications that elicit desired behavior). Recent work [50, 32] identifies principal-agent dynamics in LLM systems but provides conceptual rather than operational frameworks.

**Multi-Agent Coordination.** Classical MAS research [62, 53] established foundations for agent coordination. The Contract Net Protocol [57] demonstrated that explicit contracting could coordinate distributed systems. Coordination theory [42] identifies fundamental problems (managing shared resources, producer-consumer relationships, and simultaneity constraints), each corresponding to challenges in multi-agent LLM systems. Research on normative multi-agent systems [10] formalizes how norms govern agent behavior through obligations, prohibitions, and permissions. Closely related, social commitments [56, 14] endow agents with normative accountability: a committed agent that violates its

obligation can be sanctioned. Agent Contracts operationalize the normative perspective for LLM systems: resource constraints function as prohibitions (agents *must not* exceed budgets), success criteria as obligations (agents *must* achieve quality thresholds), and the contract lifecycle provides regimented enforcement where violations trigger automatic termination. However, unlike classical committed agents, LLM agents are typically ephemeral—instantiated per task and discarded—making agent-level sanctions inapplicable. We address this asymmetry through structural enforcement (Section 7.2).

A key insight from MAS theory is that coordination mechanisms must respect *conservation laws*—resources allocated to subtasks cannot exceed parent resources. This principle requires explicit enforcement in LLM systems where token consumption is stochastic and observable only after the fact.

**Resource-Bounded Computation.** Simon’s theory of bounded rationality [54, 55] established that agents with limited cognitive resources must *satisfice* rather than maximize. Agent Contracts operationalize satisficing by defining acceptable quality thresholds within resource budgets.

The algorithmic foundation comes from contract algorithms [68], which specify computation budgets *before* activation. Unlike anytime algorithms [69] that can be interrupted arbitrarily, contract algorithms enable strategic resource allocation. An Agent Contract transforms an LLM agent into a contract algorithm where bounds  $R$  are known in advance. Real-time systems theory [13] contributes the distinction between hard constraints (violation causes termination) and soft constraints (permitting graceful degradation).

### 3 Related Work

#### 3.1 Agent Architectures and Coordination Protocols

The development of LLM-based agents has accelerated rapidly since 2022. ReAct [65] introduced the paradigm of synergizing reasoning and acting. Chain-of-Thought prompting [60] established that computational depth correlates with output quality, motivating explicit resource governance. Toolformer [52] showed that language models can learn to use external tools, expanding the resource consumption profile of agents. Fully autonomous systems like AutoGPT [24] and Generative Agents [49] revealed both the potential and governance challenges of unbounded execution.

Coordination protocols have evolved to address different concerns. The Contract Net Protocol [57] established task allocation through bidding; MCP [7] standardizes tool connectivity between models and external resources; A2A [21] enables discovery and interoperability across heterogeneous agent systems. The recent formation of the Agentic AI Foundation [39] under the Linux Foundation—with contributions including MCP, OpenAI’s AGENTS.md, and Block’s goose—signals

industry consensus on connectivity and documentation standards. However, resource governance remains outside this scope; none of these initiatives formalize how much agents may consume.

### 3.2 Budget-Aware Reasoning and Resource Management

A growing body of work addresses resource efficiency in LLM reasoning. The TALE framework [26] introduces token-budget-aware reasoning, achieving 68% reduction in token usage with less than 5% accuracy degradation. Critically, the authors identify “token elasticity”: LLMs often exceed specified budgets when constraints are tight, demonstrating that prompting alone is insufficient for strict enforcement. BudgetThinker [61] addresses this through control tokens injected during inference, coupled with reinforcement learning to achieve precise budget adherence. SelfBudgeter [38] enables models to predict required token budgets based on task complexity. Liu et al. (2025) [40] demonstrate that simply granting larger tool-call budgets fails to improve agent performance; their Budget-Aware Tool Selection (BATS) framework shows that explicit budget awareness enables effective scaling.

Wang et al. (2024) [59] provide a budget-aware evaluation framework, demonstrating that when compute is equalized, sophisticated reasoning strategies often do not outperform simpler baselines; much apparent improvement comes from using more resources rather than using them more intelligently. This finding underscores the importance of explicit resource accounting.

Infrastructure-level resource management has matured separately. LLM serving systems [66, 34] optimize throughput and memory efficiency at the inference layer. LLMOps platforms provide budget tracking, alerting, and rate limiting at the organizational level. However, these operate below or above the application layer; neither provides formal contracts that govern individual agent behavior within multi-agent workflows.

### 3.3 Agent Safety and Formal Verification

Foundational AI safety work [5, 51] identifies problems including reward hacking and safe exploration. Recent work calls for responsible LLM-empowered multi-agent systems [29], recognizing that uncertainties compound across agent interactions.

Formal verification approaches have begun addressing agentic AI specifically. Zhang et al. (2025) [2] propose a modeling framework with 17 properties for host agents and 14 for task lifecycles, expressed in temporal logic. This work is complementary to Agent Contracts. Formal verification addresses *whether* systems satisfy properties; Agent Contracts specify *what* resource constraints systems must satisfy.

### 3.4 Multi-Agent Coordination Frameworks

LLM-based multi-agent systems have proliferated, with frameworks addressing different coordination paradigms: workflow-based collaboration [28], conversational coordination [63], graph-based orchestration [35], and role-based delegation [16]. Recent surveys [58, 43, 18, 64] characterize the landscape systematically but consistently note that resource governance remains underdeveloped. Research on self-resource allocation [3] demonstrates that LLMs can serve as effective resource allocators, but studies allocation *capability* rather than providing a formal governance *framework*.

Table 1 clarifies this gap, summarizing resource governance features across eight major frameworks. All provide operational controls (iteration limits, timeouts, rate limiting), but none provide the formal governance layer that Agent Contracts introduce: cost budgets, temporal deadlines, success criteria, or conservation laws for multi-agent delegation.

Table 1: Governance features across agent frameworks. Y = native, P = partial, – = none. *Italic*: operational controls. **Bold**: governance features unique to Agent Contracts. LG = LangGraph, AG = AutoGen, Crew = CrewAI, OAI = OpenAI Agents SDK, ADK = Google ADK, BR = Amazon Bedrock, LI = LlamaIndex, smol = smolagents. <sup>a</sup>AutoGen is being merged with Semantic Kernel into Microsoft Agent Framework. [37, 44, 17, 48, 22, 4, 41, 30]

	LG	AG <sup>a</sup>	Crew	OAI	ADK	BR	LI	smol
<i>Max iterations</i>	Y	Y	Y	Y	Y	Y	Y	Y
<i>Timeout</i>	Y	Y	Y	Y	Y	Y	Y	Y
<i>Rate limiting</i>	Y	P	Y	P	P	Y	P	Y
<i>Token limits</i>	P	Y	Y	Y	Y	Y	Y	Y
<i>Observability</i>	Y	Y	Y	Y	Y	Y	Y	Y
<i>Guardrails</i>	P	–	P	Y	Y	Y	P	–
<b>Agent Contract</b>	–	–	–	–	–	–	–	–

While recent practitioner perspectives frame “agent engineering” as iterative refinement for reliability [36], resource governance remains unaddressed. The following section presents Agent Contracts to fill this gap.

## 4 The Agent Contract Framework

### 4.1 Contract Definition

An **Agent Contract**  $C$  is defined as a seven-tuple:

$$C = (I, O, S, R, T, \Phi, \Psi)$$

The components capture the complete specification for bounded agent execution. The input specification  $I$  defines the schema and constraints for acceptable inputs. The output specification  $O$  defines the schema and quality criteria for deliverables. The skill set  $S$  enumerates the capabilities (tools, functions, and knowledge domains) available to the agent. Resource constraints  $R$  specify a multi-dimensional budget governing consumption. Temporal constraints  $T$  establish time-related boundaries and duration limits. Success criteria  $\Phi$  define measurable conditions for contract fulfillment. Finally, termination conditions  $\Psi$  specify events that end the contract regardless of fulfillment.

This formulation synthesizes contract theory in economics, where contracts align incentives and define obligations between parties [11], with real-time systems theory, where correctness depends on meeting explicit timing constraints [13]. The contract serves as both specification (defining what the agent should do) and governance mechanism (constraining how the agent may operate).

An important distinction separates  $I$  from  $R$ . The input specification  $I$  defines *what* the agent receives: task content, context, and parameters. The resource constraints  $R$  define *how much* the agent may consume while processing: token budgets, API call limits, time bounds. An agent may receive a small input but consume many resources through complex reasoning, or receive a large input but consume few resources through simple transformation.

## 4.2 Contract Components

**Input and Output Specifications.** The input specification  $I = (\sigma_I, \mathcal{V}_I, \mathcal{P}_I)$  comprises the input schema  $\sigma_I$ , validation rules  $\mathcal{V}_I$ , and preprocessing transformations  $\mathcal{P}_I$ . For example, a code review agent might specify  $\sigma_I$  as `{repository: string, pr_id: integer}`,  $\mathcal{V}_I$  as `pr_id > 0`, and  $\mathcal{P}_I$  as `fetch_diff(pr_id)`.

The output specification  $O = (\sigma_O, Q_{min}, \mathcal{F}_O)$  comprises the output schema  $\sigma_O$ , minimum acceptable quality threshold  $Q_{min}$ , and formatting requirements  $\mathcal{F}_O$ . For the code review agent,  $\sigma_O$  might be `{summary: string, issues: list, approval: boolean}`,  $Q_{min} = 0.8$  (requiring 80% of issues correctly identified), and  $\mathcal{F}_O$  as markdown format with severity labels.

**Skills and Capabilities.** The skill set  $S = \{s_1, s_2, \dots, s_m\}$  where  $s_i \in \mathcal{S}_{available}$  enumerates what the agent *can* do [67]. Each skill  $s_i$  may have associated costs  $c(s_i)$  and success probabilities  $p(s_i)$ . Skills encompass tool invocations (web search, code execution, API calls), knowledge domains (legal, medical, technical), and cognitive capabilities (reasoning, planning, summarization). Recent industry standards for agent skills employ *progressive disclosure*—loading meta-data (\$50tokens) *initially* and *full specifications* (\$500+ tokens) on-demand [8]—reflecting resource-aware design even in capability definitions. The contract restricts the agent to skills in  $S$ ; for example, an agent contracted for data analysis cannot invoke payment APIs even if technically accessible.

**Resource Constraints.** The resource constraint  $R = \{r_1, r_2, \dots, r_n\}$  defines a multi-dimensional budget. Common resource dimensions include:

Resource	Symbol	Unit	Example
LLM Tokens	$r_{tok}$	tokens	100,000
API Calls	$r_{api}$	calls	50
Iterations	$r_{iter}$	rounds	10
Web Searches	$r_{web}$	queries	10
Compute Time	$r_{cpu}$	seconds	300
External Cost	$r_{cost}$	USD	5.00

Each resource  $r_i$  has a budget  $b_i$  and consumption function  $c_i(t)$ . Constraint satisfaction requires  $\forall i : c_i(t) \leq b_i$ .

**Temporal Constraints.** The temporal constraint  $T = (t_{start}, \tau)$  comprises the contract activation timestamp  $t_{start}$  and the contract duration (time-to-live)  $\tau$ . The constraint requires  $t_{current} - t_{start} \leq \tau$ . While users often think in terms of deadlines (“complete by 5pm”), duration is the operational primitive—a deadline is simply  $t_{deadline} = t_{start} + \tau$ .

**Success Criteria and Termination.** Success criteria  $\Phi = \{(\phi_1, w_1), (\phi_2, w_2), \dots, (\phi_k, w_k)\}$  pair measurable conditions  $\phi_i$  with weights  $w_i$ . The contract is fulfilled when  $\sum w_i \cdot \mathbb{1}[\phi_i] \geq \theta$  for threshold  $\theta$ . Conditions may include task completion (`all_items_processed`), quality metrics (`accuracy > 0.95`), or business logic (`response_generated AND reviewed`).

The output quality threshold  $Q_{min}$  (in specification  $O$ ) is a *structural requirement* on output format and minimum acceptability. Success criteria  $\Phi$  are *fulfillment conditions* that may include quality checks (e.g.,  $\phi_1 = Q \geq Q_{min}$ ) along with other conditions. An agent might produce output meeting  $Q_{min}$  but fail  $\Phi$  if other criteria are unmet.

Termination conditions  $\Psi = \{\psi_1 \vee \psi_2 \vee \dots \vee \psi_l\}$  define when the contract ends regardless of success. Common termination conditions include resource exhaustion ( $\exists r_i : c_i \geq b_i$ ), duration expiration ( $t - t_{start} > \tau$ ), explicit cancellation (external signal), and unrecoverable errors (critical failure states). The existential quantifier ensures that exceeding *any* resource budget causes termination, not just aggregate overruns.

### 4.3 Contract Lifecycle

Contracts progress through distinct states following the transition pattern `DRAFTED`  $\rightarrow$  `ACTIVE`  $\rightarrow$  `{FULFILLED, VIOLATED, EXPIRED, TERMINATED}`. A contract begins in the `DRAFTED` state, where its parameters are specified but execution has not begun. Activation transitions the contract to

ACTIVE, at which point resources are reserved and monitoring begins. From ACTIVE, the contract reaches exactly one of four terminal states.

The terminal state FULFILLED indicates that success criteria  $\Phi$  were satisfied within all resource and temporal constraints. VIOLATED indicates that some constraint in  $R$  or  $T$  was breached before success criteria were met. EXPIRED indicates that the duration  $\tau$  was exceeded. TERMINATED indicates external cancellation, regardless of progress toward success criteria.

Transitions between states are governed by formal guard conditions:

From	To	Guard Condition
DRAFTED	ACTIVE	activate() $\wedge$ resources_available()
ACTIVE	FULFILLED	$\sum w_i \cdot \mathbb{1}[\phi_i] \geq \theta$
ACTIVE	VIOLATED	$\exists r_i : c_i \geq b_i$
ACTIVE	EXPIRED	$t - t_{start} > \tau$
ACTIVE	TERMINATED	cancel_signal()

The lifecycle model ensures clear accountability. Every contract reaches exactly one terminal state, enabling unambiguous resource release and audit logging.

## 5 Resource Tracking and Monitoring

The preceding section defined what contracts *are*: their structure, components, and lifecycle. This section addresses how resources are *tracked* during execution. While the framework tracks multiple resource types (tokens, API calls, tool invocations, compute time, cost), we focus here on two foundational aspects: how token budgets decompose into measurable categories, and how runtime monitoring provides visibility into constraint utilization.

### 5.1 Token Budget Decomposition

Modern LLMs distinguish input, reasoning, and output tokens. We model this as  $R_{tok} = (r_{in}, r_r, r_{out})$ . Since input tokens  $r_{in}$  are largely determined by task context, the *controllable budget* is  $B_{ctrl} = B_{tok} - r_{in}$ , representing tokens available for reasoning and output. This decomposition enables fine-grained monitoring across categories, supporting both real-time adaptation and post-hoc analysis.

### 5.2 Runtime Monitoring

During execution, a monitoring system tracks both resource consumption and temporal progress in real-time. The monitor function  $\text{Monitor} : (C, t) \rightarrow (\vec{c}, \vec{u}, \tau_{util})$  takes a contract  $C$  and current time  $t$  and returns three values: the resource

consumption vector  $\vec{c}$ , the resource utilization vector  $\vec{u} = \vec{c}/\vec{b}$  (computed element-wise), and the duration utilization  $\tau_{util} = (t - t_{start})/\tau$  ranging from 0 to 1. The agent can query these values at any time to adapt its strategy as constraints tighten. Note that utilization is monotonically non-decreasing since resource consumption is cumulative.

A useful aggregate metric captures the most-constrained resource:

$$\text{utilization}(t) = \max\left(\frac{t_{current} - t_{start}}{\tau}, \max_i \frac{c_i(t)}{b_i}\right)$$

This single value summarizes how close the agent is to any constraint boundary, enabling simple threshold-based policies (e.g., “warn when utilization exceeds 80%”) without requiring sophisticated optimization.

**Communicating Budget to Agents.** A current approach is *budget-aware prompting*: injecting remaining budget into system prompts or providing dynamic status updates during execution. This enables agents to self-regulate—producing concise outputs when budget is tight or taking exploratory actions when resources are ample. As the field matures, native solutions may emerge (e.g., models with built-in resource awareness), but prompt-based communication provides a practical mechanism with current infrastructure.

## 6 Multi-Agent Coordination Under Contracts

The preceding sections establish contracts for individual agents. However, complex tasks often require multiple agents working together: a researcher gathering data, an analyzer identifying patterns, a reporter synthesizing findings. This extension from single-agent to multi-agent governance raises new questions: How should a parent budget be divided among child agents? What happens when one agent exceeds its allocation while others remain under budget? How can the system guarantee that aggregate consumption respects the original constraint?

These questions have theoretical grounding in coordination theory. Malone and Crowston (1994) [42] identified managing shared resources as a fundamental coordination problem. In LLM-based multi-agent systems, the shared resource is typically the token budget (and associated cost), but the same principles apply to API call limits, compute time, and other constrained resources. The key insight is that contracts provide a natural unit of delegation. When an orchestrator creates subcontracts for workers, the contract specification ensures that each worker operates within defined bounds, and the aggregate of those bounds respects the parent constraint.

## 6.1 Conservation Laws and Budget Allocation

When multiple agents collaborate, contracts must govern how resources flow between them. The fundamental constraint is **conservation**: total consumption cannot exceed the system budget:

$$\sum_{j \in \text{agents}} c_j^{(r)} \leq B^{(r)} \quad \forall r \in R$$

This invariant holds regardless of execution pattern—sequential, parallel, hierarchical, or competitive.

**Initial Allocation.** Before execution, the total budget  $B$  must be divided among agents. Three strategies apply depending on available information:

- *Proportional*:  $b_j = \omega_j / \sum \omega_k \cdot (B - B_{reserve})$ , where  $\omega_j$  reflects estimated task complexity
- *Equal*:  $b_j = (B - B_{reserve}) / n$ , when complexity is unknown
- *Negotiated*: Agents request budgets; a coordinator allocates based on requests with caps to prevent over-claiming

A reserve buffer  $B_{reserve}$  (typically 10–15%) accommodates coordination overhead and unexpected costs.

**Dynamic Reallocation.** As agents complete, unused budget returns to a shared pool:

$$B_{available}(t) = B_{reserve} + \sum_{j \in \text{completed}} (b_j - c_j)$$

This enables *budget pooling*—efficient agents effectively subsidize those requiring more resources, improving overall throughput while maintaining total budget discipline.

## 6.2 Coordination Patterns Through a Contract Lens

Recent work has identified recurring design patterns for agentic AI systems, including routing, orchestration, parallelization, and iterative refinement [46, 6, 23].

We organize these patterns through a **contract-centric lens**, focusing on how resource constraints govern each pattern’s behavior and where contracts provide critical safety guarantees. We focus here on two typical **control flow patterns**, task routing and delegation decisions, since these are where contracts add the most value. Execution within any pattern can be sequential or parallel; these are orthogonal concerns that compose naturally with contract governance.

**Routing.** An input classifier directs requests to specialized handlers based on task characteristics, selecting the best-suited agent for each input and allocating

the corresponding budget [6]. Budget is reserved per potential branch; unused allocations return to the pool. This enables separation of concerns—specialized agents outperform generalists on their specific tasks.

When specialists have explicit contracts, routing becomes more principled: the router matches task requirements against specialist capabilities, resource profiles, and success criteria. Furthermore, with well-defined contracts, the router need not be limited to a fixed pool; it can dynamically instantiate or configure an agent specifically for the required contract. This blurs the line between routing and orchestration, with the contract serving as the specification for agent creation, not just agent selection.

**Orchestrator-Workers.** A central orchestrator dynamically decomposes tasks and delegates to worker agents, synthesizing results [6, 23]. This pattern can extend to multiple levels (hierarchical orchestration).

From a contract perspective, this pattern is particularly significant: the orchestrator **drafts and issues subcontracts** to workers. Each subcontract specifies the worker’s task, allocated budget, and success criteria:

$$\text{orchestrator}(C_{parent}) \rightarrow \{C_i = (I_i, O_i, S_i, R_i, T_i, \Phi_i, \Psi_i)\}_{i=1}^k$$

This frames **contracting as a capability**: the orchestrator must understand the contract framework to effectively delegate work. The conservation law (Section 6.1) constrains subcontract allocation:  $\sum R_i \leq R_{parent}$ .

The implications of contracting as a capability are significant:

Implication	Description
<i>Recursive delegation</i>	Agents spawn sub-agents that themselves have contracting capability, enabling hierarchical self-organization
<i>Bounded autonomy</i>	Even highly capable orchestrators remain governed by their parent contract: they can create subcontracts but cannot exceed their own constraints
<i>Dynamic team formation</i>	Agents form coalitions and delegate work without centralized coordination, as long as conservation laws are satisfied
<i>Dynamic agent instantiation</i>	Rather than selecting from a fixed pool, agents instantiate specialists on-demand; the contract becomes the specification for agent creation, not just selection

Implication	Description
<i>Meta-governance</i>	Contracts can govern the creation of other contracts, enabling principled scaling of multi-agent systems

These patterns demonstrate how contracts can govern increasingly complex multi-agent systems. However, practical enforcement faces fundamental constraints that shape what contracts can and cannot guarantee.

## 7 Fundamental Limitations and Practical Enforcement

### 7.1 Single-Call Enforcement Constraints

A critical limitation exists. Token consumption is only known *after* an LLM call completes, not during execution:

$$c_{tok}(t) = \begin{cases} \text{unknown} & \text{during API call} \\ c_{actual} & \text{after API returns} \end{cases}$$

Even streaming APIs provide total usage metadata only after generation completes. This asymmetry has three important consequences: contracts cannot prevent a single expensive call from exceeding budget, contracts can prevent subsequent calls after budget is exceeded, and the primary value is therefore multi-call protection.

### 7.2 Enforcement Capabilities

Agent Contracts employ two complementary enforcement layers. *Soft enforcement* operates cooperatively: budget-aware prompts (Section 5) communicate remaining resources, enabling agents to self-regulate. This is best-effort—agents may ignore or exceed stated constraints, as documented by the “token elasticity” phenomenon [26]. *Hard enforcement* operates structurally: an external monitor tracks consumption after each action and halts execution when constraints are breached, regardless of agent behavior. This follows the *agent harness* pattern emerging in production systems—an infrastructure layer that wraps the agent, intercepts its actions, and enforces invariants without relying on the agent’s cooperation. Hard enforcement requires no model-level support; it operates at the orchestration layer between actions. This structural approach replaces the normative sanctions of social commitments (Section 2): where persistent agents are sanctioned for violations, ephemeral LLM agents are simply halted, with accountability attributed to the orchestrator’s allocation strategy and recorded for audit.

Despite single-call limitations, hard enforcement provides substantial value across multiple enforcement dimensions:

Constraint	Enf.	Mechanism
Multi-call budgets	Full	Stop after cumulative threshold
Iteration limits	Full	Count and halt at $r_{iter}$
API call limits	Full	Count external invocations
Duration limits	Full	Check elapsed time before each action
Cost ceilings	Approx	Track cumulative cost; bound via <code>max_tokens</code>

Contracts provide particularly high value in iterative workflows (retry loops, validation cycles), multi-agent delegation, and tool-heavy agents—scenarios validated empirically in Section Section 8.

### 7.3 Future Infrastructure Requirements

True real-time enforcement would require API-level changes: interruptible generation, token reservation, and budget-aware inference [26, 61]. Such infrastructure would extend hard enforcement from the inter-call level to the intra-call level. Until then, Agent Contracts provide hard enforcement between actions and soft enforcement within them.

## 8 Empirical Evaluation

We validate Agent Contracts through four complementary experiments spanning single-agent and multi-agent settings. Each experiment targets specific framework components; collectively they validate the enforcement mechanisms ( $R$ ,  $T$ ,  $\Phi$ ,  $\Psi$ ) and coordination primitives (conservation laws, contract delegation) that distinguish Agent Contracts from existing approaches. Experiments use a reference implementation with Google ADK (Code Review, Research Pipeline, Crisis Communication) or LiteLLM (Strategy Modes), using Gemini 2.5 Flash and Flash-Lite (knowledge cutoff: January 2025).<sup>3</sup> Statistical analysis employs bootstrap confidence intervals (10,000 resamples) using the percentile method.

### 8.1 Experimental Overview

The following table summarizes our experimental design, with each experiment validating a distinct aspect of the framework.

<sup>3</sup> Implementation available at <https://github.com/flyersworder/agent-contracts>. The framework is under active development; we provide experiment code and data for reproducibility.

Experiment	n Validates	Key Result
Code Review	70 Runaway prevention	90% token reduction
Research Pipeline	50 Conservation laws	0 violations
Strategy Modes	50 Satisficing tradeoffs	70%→86% success
Crisis Comm.	24 Failure prevention	23% fewer tokens

## 8.2 Runaway Prevention in Iterative Workflows

The “\$47K problem” from the Introduction illustrates the danger of unbounded agent loops. We evaluate iteration governance using a Coder Reviewer pipeline where agents iteratively refine code solutions. The Coder writes Python code; the Reviewer executes it against test cases using a `test_code` tool and either approves or requests revision. The experiment uses 70 problems from LiveCodeBench [31] (released post-February 2025, after model cutoff): 31 easy and 39 medium difficulty.

**Design.** Each problem is executed twice in a within-subjects design: CONTRACTED (50K token budget, max 3 iterations) versus UNCONTRACTED (no token limits, max 6 iterations). CONTRACTED agents receive budget-aware prompts and dynamic status updates showing both token consumption and iteration progress; UNCONTRACTED agents use identical base prompts without resource awareness.

**Results.** CONTRACTED execution achieves 90% token reduction compared to UNCONTRACTED ( $p = 0.0007$ , paired  $t$ -test), with  $525\times$  lower variance (5.29B vs 10.1M)—directly addressing the “\$47K problem.” The success rate difference of 7.1 percentage points (52.9% vs 60.0%) is not statistically significant ( $p = 0.13$ ). Governance value increases with task complexity: medium-difficulty problems show 92% token savings versus 76% for easy.

Metric	UNCONTRACTED	CONTRACTED	Change	$p$ -value
Token Usage	34,606	3,461	−90%	0.0007***
Variance	5.29B	10.1M	$525\times$ lower	—
Iterations	3.00	1.71	−43%	<0.0001***
LLM Calls	9.0	4.5	−50%	<0.0001***
Success Rate	60.0%	52.9%	−7.1pp	0.13 (NS)

A complementary single-agent experiment with 24 time-critical crisis communication scenarios provides additional evidence: agents with explicit quality thresholds ( $Q \geq 0.80$ ) and iteration limits achieved 23% token reduction ( $p = 0.005$ ) with statistically equivalent quality ( $p = 0.32$ ). Notably, one UNCONTRACTED agent failed entirely—stuck in an evaluation loop without submitting output—while the CONTRACTED version succeeded, demonstrating that iteration governance prevents agent failures, not just improves efficiency.

### 8.3 Conservation Laws in Multi-Agent Coordination

We evaluate conservation laws and contract delegation (Section 6) using a three-agent research pipeline: Researcher  $\rightarrow$  Analyzer  $\rightarrow$  Reporter. The orchestrator delegates sub-contracts to each worker via `DelegatingAdkAgent`, enforcing both the conservation invariant  $\sum b_i \leq B$  and per-tool limits at allocation time.

**Design.** Fifty research topics across five categories (technology, science, business, health, society) are evaluated. CONTRACTED agents receive explicit budget allocations with per-tool limits (e.g., Researcher limited to 6 web searches) and budget-aware prompts; UNCONTRACTED agents operate without constraints. Quality is assessed via multi-judge LLM evaluation following best practices for rating indeterminacy [25].

**Results.** CONTRACTED execution achieves zero conservation violations across all 50 trials, demonstrating that conservation laws ( $\sum b_i \leq B$ ) are fully enforceable. In one trial, the enforcement mechanism successfully detected and halted a runaway agent that exceeded its 40K token budget (56K consumed), providing evidence that runtime enforcement works as designed. Quality variance is  $26.7\times$  lower than UNCONTRACTED ( $\sigma$ : 1.75 vs 9.07), though partly driven by one catastrophic failure in the UNCONTRACTED condition. Excluding this outlier, CONTRACTED still shows  $1.4\times$  lower variance (88.5% Bayesian probability). The key insight is not mean quality improvement but variance reduction—contracts eliminate catastrophic failures where agents consume resources without producing useful output.

### 8.4 Quality-Resource Tradeoffs via Contract Modes

Contract modes operationalize Simon’s satisficing principle [54]: agents achieve acceptable quality within defined resource bounds. We test whether different contract configurations produce measurable behavioral differences using logic reasoning problems from OpenR1 (released February 2025, after model cutoff).

**Design.** Fifty medium-difficulty logic puzzles are evaluated under three contract modes: URGENT (no extended reasoning, 30s timeout), ECONOMICAL (low reasoning effort, 60s timeout), and BALANCED (medium reasoning effort, 90s timeout). Success requires exact numeric answer match.

**Results.** Contract modes produce a clear quality-resource gradient. BALANCED mode achieves 86% success rate versus 70% for URGENT, investing 75% more tokens for 16 percentage points higher success ( $p \approx 0.05$ ). The `reasoning_effort` parameter provides direct control: users requiring speed accept lower accuracy (URGENT); those requiring accuracy invest more resources (BALANCED).

Mode	Success Rate	Reasoning Tokens	Avg Time	Timeout Rate
URGENT	70%	0	6.9s	26%
ECONOMICAL	76%	718	12.5s	14%

Mode	Success Rate	Reasoning Tokens	Avg Time	Timeout Rate
BALANCED	86%	1,519	16.9s	10%

Across all four experiments, the consistent finding is not cost optimization but *governance*: contracts transform unpredictable agent behavior into bounded, auditable operations. Code Review demonstrates multi-dimensional resource enforcement (90% token reduction,  $525\times$  variance reduction). Research Pipeline validates conservation laws and runtime enforcement (zero conservation violations; one runaway agent detected and halted). Crisis Communication shows that quality thresholds prevent failures, not just reduce costs. Strategy Modes confirms that contract configurations operationalize satisficing tradeoffs (70%→86% success).

Framework Component	Experiment	Validation	Specification
Budget awareness	All	Prompts; dynamic status	"Budget: $\frac{\text{used}}{\text{total}}$ "
Resource constraints $R$	Code Review	Tokens, iterations, calls	$r_{tok}=50K, r_{iter}=3, r_{llm}=6$
Agent delegation	Research	Conservation, per-tool limits	$\sum R_i \leq 100K;$ $\text{web\_search} \leq 6$
Success criteria $\Phi$	Crisis Comm.	Quality thresholds	$Q_{min} = 0.80$
Contract modes	Strategy	URGENT/ECON./BAL- ANCED	$\tau: 30s / 60s / 90s$

## 9 Conclusion

Agent Contracts provide a formal framework for governing autonomous AI agents through explicit resource and temporal constraints. The contract specification  $C = (I, O, S, R, T, \Phi, \Psi)$  unifies resource, temporal, and quality governance with conservation laws for multi-agent delegation.

Empirical validation demonstrates that the formal framework translates into practical governance: resource constraints enable 90% token reduction with  $525\times$  lower variance; conservation laws achieve 100% compliance in multi-agent delegation; and contract modes operationalize satisficing tradeoffs (70%→86% success).

Extensions include *learning-based contract design* [26, 61], *formal verification* of contract properties [1, 12], and *runtime cancellation* via API-level support. As agentic AI moves to production, formal governance becomes essential for cost control, accountability, and value alignment. Agent Contracts provide one such foundation.

## 10 References

- [1] Alechina, N., Logan, B., Nguyen, H.N., Rakib, A.: Resource-bounded alternating-time temporal logic. In: Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems (AAMAS). pp. 481–488 (2010)
- [2] Allegrini, E., Shreekrumar, A., Celik, Z.B.: Formalizing the safety, security, and functional properties of agentic ai systems. arXiv preprint arXiv:2510.14133 (2025)
- [3] Amayuelas, A., Yang, J., Agashe, S., Nagarajan, A., Antoniadis, A., Wang, X.E., Wang, W.: Self-resource allocation in multi-agent llm systems. arXiv preprint arXiv:2504.02051 (2025)
- [4] Amazon Web Services: Amazon bedrock agents documentation. <https://docs.aws.amazon.com/bedrock/latest/userguide/agents.html> (2025)
- [5] Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., Mané, D.: Concrete problems in ai safety. arXiv preprint arXiv:1606.06565 (2016)
- [6] Anthropic: Building effective agents. <https://www.anthropic.com/research/building-effective-agents> (December 2024)
- [7] Anthropic: Introducing the model context protocol. <https://www.anthropic.com/news/model-context-protocol> (November 2024)
- [8] Anthropic: Building agents with skills: Equipping agents for specialized work. <https://claude.com/blog/building-agents-with-skills-equipping-agents-for-specialized-work> (January 2025), introduces progressive disclosure architecture for agent skills
- [9] Anthropic: Introducing claude sonnet 4.5. <https://www.anthropic.com/news/claude-sonnet-4-5> (September 2025)
- [10] Boella, G., van der Torre, L., Verhagen, H.: Introduction to normative multiagent systems. Computational and Mathematical Organization Theory **12**(2-3), 71–79 (2006)
- [11] Bolton, P., Dewatripont, M.: Contract Theory. MIT Press (2005)
- [12] Bulling, N., Dastani, M.: Norm-based mechanism design. Artificial Intelligence **239**, 97–142 (2016). <https://doi.org/10.1016/j.artint.2016.07.001>
- [13] Buttazzo, G.C.: Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications. Springer Science & Business Media (2011)
- [14] Castelfranchi, C.: Engineering social order. In: Engineering Societies in the Agents World, pp. 1–18. Springer (2000)
- [15] Cemri, M., Pan, M.Z., Yang, S., Agrawal, L.A., Chopra, B., Tiwari, R., Keutzer, K., Parameswaran, A., Klein, D., Ramchandran, K., Zaharia, M.,

- Gonzalez, J.E., Stoica, I.: Why do multi-agent llm systems fail? arXiv preprint arXiv:2503.13657 (2025)
- [16] CrewAI: Crewai: Framework for orchestrating role-playing, autonomous ai agents. <https://github.com/crewAIInc/crewAI> (2024)
- [17] CrewAI: Crewai documentation. <https://docs.crewai.com/> (2025)
- [18] Derouiche, H., Brahmi, Z., Mazeni, H.: Agentic ai frameworks: Architectures, protocols, and design challenges. arXiv preprint arXiv:2508.10146 (2025)
- [19] Gartner: Gartner identifies the top 10 strategic technology trends for 2025. <https://www.gartner.com/en/newsroom/press-releases/2024-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2025> (October 2024)
- [20] Gartner: Gartner predicts over 40% of agentic ai projects will be canceled by end of 2027. <https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027> (June 2025)
- [21] Google: Announcing the agent2agent protocol (a2a). <https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interopability/> (April 2025)
- [22] Google: Google agent development kit (adk). <https://google.github.io/adk-docs/> (2025)
- [23] Google Cloud: Choose the right design pattern for your agentic ai system. <https://cloud.google.com/architecture/choose-design-pattern-agentic-ai-system> (2025)
- [24] Gravitas, S.: Autogpt: An autonomous gpt-4 experiment. <https://github.com/Significant-Gravitas/AutoGPT> (2023)
- [25] Guerdan, L., Barocas, S., Holstein, K., Wallach, H., Wu, Z.S., Choudhchova, A.: Validating llm-as-a-judge systems under rating indeterminacy. In: Advances in Neural Information Processing Systems (NeurIPS) (2025)
- [26] Han, T., Wang, Z., Fang, C., Zhao, S., Ma, S., Chen, Z.: Token-budget-aware llm reasoning. arXiv preprint arXiv:2412.18547 (2024)
- [27] Hart, O.: Firms, Contracts, and Financial Structure. Oxford University Press (1995)
- [28] Hong, S., Zhuge, M., Chen, J., Zheng, X., Cheng, Y., Zhang, C., Wang, J., Wang, Z., Yau, S.K.S., Lin, Z., Zhou, L., Ran, C., Xiao, L., Wu, C., Schmidhuber, J.: Metagpt: Meta programming for multi-agent collaborative framework. arXiv preprint arXiv:2308.00352 (2023)
- [29] Hu, J., Dong, Y., Ao, S., Li, Z., Wang, B., Singh, L., Cheng, G., Ramchurn, S.D., Huang, X.: Position: Towards a responsible llm-empowered multi-agent systems. arXiv preprint arXiv:2502.01714 (2025)

- [30] Hugging Face: smolagents: A simple library to build agents. <https://huggingface.co/docs/smolagents/> (2025)
- [31] Jain, N., Han, K., Gu, A., Li, W.D., Yan, F., Zhang, T., Wang, S., Solar-Lezama, A., Sen, K., Stoica, I.: Livecodebench: Holistic and contamination free evaluation of large language models for code. arXiv preprint arXiv:2403.07974 (2024)
- [32] Kaltenpoth, S., Müller, O.: Getting in contract with large language models: An agency theory perspective on large language model alignment. arXiv preprint arXiv:2509.07642 (2025)
- [33] Kusireddy, T.: Ai agents horror stories: How a \$47,000 ai agent failure exposed the hype and hidden risks of multi-agent systems. <https://techstartups.com/2025/11/14/ai-agents-horror-stories-how-a-47000-failure-exposed-the-hype-and-hidden-risks-of-multi-agent-systems/> (November 2025)
- [34] Kwon, W., Li, Z., Zhuang, S., Sheng, Y., Zheng, L., Yu, C.H., Gonzalez, J.E., Zhang, H., Stoica, I.: Efficient memory management for large language model serving with pagedattention. Proceedings of the 29th Symposium on Operating Systems Principles pp. 611–626 (2023)
- [35] LangChain: Langgraph: Build stateful, multi-actor applications with llms. <https://github.com/langchain-ai/langgraph> (2024)
- [36] LangChain: Agent engineering: A new discipline. <https://blog.langchain.com/agent-engineering-a-new-discipline/> (December 2025)
- [37] LangChain: Langgraph documentation. <https://docs.langchain.com/oss/python/langgraph/> (2025)
- [38] Li, Z., Dong, Q., Ma, J., Zhang, D., Jia, K., Sui, Z.: Selfbudgeter: Adaptive token allocation for efficient llm reasoning. arXiv preprint arXiv:2505.11274 (2025)
- [39] Linux Foundation: Linux foundation announces the formation of the agentic ai foundation (aaif). <https://www.linuxfoundation.org/press/linux-foundation-announces-the-formation-of-the-agentic-ai-foundation> (December 2025), founding members include Anthropic, OpenAI, Google, Microsoft, AWS
- [40] Liu, T., Wang, Z., Miao, J., Hsu, I.H., Yan, J., Chen, J., Han, R., Xu, F., Chen, Y., Jiang, K., Daruki, S., Liang, Y., Wang, W.Y., Pfister, T., Lee, C.Y.: Budget-aware tool-use enables effective agent scaling. arXiv preprint arXiv:2511.17006 (2025)
- [41] LlamaIndex: Llamaindex documentation. <https://developers.llamaindex.ai/> (2025), framework for building LLM applications with data

- [42] Malone, T.W., Crowston, K.: The interdisciplinary study of coordination. *ACM Computing Surveys* **26**(1), 87–119 (1994)
- [43] Masterman, T., Besen, S., Sawtell, M., Chao, A.: The landscape of emerging ai agent architectures for reasoning, planning, and tool calling: A survey. arXiv preprint arXiv:2404.11584 (2024)
- [44] Microsoft: Autogen: Enabling next-gen llm applications via multi-agent conversation. <https://microsoft.github.io/autogen/> (2025)
- [45] MIT Sloan Management Review, Boston Consulting Group: The emerging agentic enterprise: How leaders must navigate a new age of ai. <https://sloanreview.mit.edu/projects/the-emerging-agentic-enterprise-how-leaders-must-navigate-a-new-age-of-ai/> (2025), research report on agentic AI adoption in enterprises
- [46] Ng, A.: Agentic design patterns. <https://www.deeplearning.ai/the-batch/issue-241/> (March 2024), the Batch, Issue 241
- [47] OpenAI: Introducing deep research. <https://openai.com/index/introducing-deep-research/> (February 2025)
- [48] OpenAI: Openai agents sdk. <https://openai.github.io/openai-agents-python/> (2025)
- [49] Park, J.S., O’Brien, J.C., Cai, C.J., Morris, M.R., Liang, P., Bernstein, M.S.: Generative agents: Interactive simulacra of human behavior. arXiv preprint arXiv:2304.03442 (2023)
- [50] Phelps, S., Ranson, R.: Of models and tin men: A behavioural economics study of principal-agent problems in ai alignment using large-language models. arXiv preprint arXiv:2307.11137 (2023)
- [51] Russell, S.: *Human Compatible: Artificial Intelligence and the Problem of Control*. Viking (2019)
- [52] Schick, T., Dwivedi-Yu, J., Dessì, R., Raileanu, R., Lomeli, M., Zettlemoyer, L., Cancedda, N., Scialom, T.: Toolformer: Language models can teach themselves to use tools. arXiv preprint arXiv:2302.04761 (2023)
- [53] Shoham, Y., Leyton-Brown, K.: *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*. Cambridge University Press (2008)
- [54] Simon, H.A.: A behavioral model of rational choice. *The Quarterly Journal of Economics* **69**(1), 99–118 (1955)
- [55] Simon, H.A.: Rational choice and the structure of the environment. *Psychological Review* **63**(2), 129–138 (1956)
- [56] Singh, M.P.: An ontology for commitments in multiagent systems. *Artificial Intelligence and Law* **7**(1), 97–113 (1999)

- [57] Smith, R.G.: The contract net protocol: High-level communication and control in a distributed problem solver. *IEEE Transactions on Computers* **29**(12), 1104–1113 (1980)
- [58] Tran, K.T., Dao, D., Nguyen, M.D., Pham, Q.V., O’Sullivan, B., Nguyen, H.D.: Multi-agent collaboration mechanisms: A survey of llms. *arXiv preprint arXiv:2501.06322* (2025)
- [59] Wang, J., Jain, S., Zhang, D., Ray, B., Kumar, V., Athiwaratkun, B.: Reasoning in token economies: Budget-aware evaluation of llm reasoning strategies. In: *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing (EMNLP)*. pp. 19916–19939 (2024)
- [60] Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q., Zhou, D.: Chain-of-thought prompting elicits reasoning in large language models. *Advances in Neural Information Processing Systems* **35**, 24824–24837 (2022)
- [61] Wen, H., Wu, X., Sun, Y., Zhang, F., Chen, L., Wang, J., Liu, Y., Liu, Y., Zhang, Y.Q., Li, Y.: Budgetthinker: Empowering budget-aware llm reasoning with control tokens. *arXiv preprint arXiv:2508.17196* (2025)
- [62] Wooldridge, M.: *An Introduction to MultiAgent Systems*. John Wiley & Sons (2009)
- [63] Wu, Q., Bansal, G., Zhang, J., Wu, Y., Li, B., Zhu, E., Jiang, L., Zhang, X., Zhang, S., Liu, J., Awadallah, A.H., White, R.W., Burger, D., Wang, C.: Autogen: Enabling next-gen llm applications via multi-agent conversation. *arXiv preprint arXiv:2308.08155* (2023)
- [64] Yan, B., Zhou, Z., Zhang, L., Zhang, L., Zhou, Z., Miao, D., Li, Z., Li, C., Zhang, X.: Beyond self-talk: A communication-centric survey of llm-based multi-agent systems. *arXiv preprint arXiv:2502.14321* (2025)
- [65] Yao, S., Zhao, J., Yu, D., Du, N., Shafran, I., Narasimhan, K., Cao, Y.: React: Synergizing reasoning and acting in language models. *arXiv preprint arXiv:2210.03629* (2023)
- [66] Yu, G.I., Jeong, J.S., Kim, G.W., Kim, S., Chun, B.G.: Orca: A distributed serving system for transformer-based generative models. *16th USENIX Symposium on Operating Systems Design and Implementation (OSDI 22)* pp. 521–538 (2022)
- [67] Zhang, B., Lazuka, K., Murag, M.: Equipping agents for the real world with agent skills. <https://www.anthropic.com/engineering/equipping-agents-for-the-real-world-with-agent-skills> (October 2025), engineering at Anthropic
- [68] Zilberstein, S.: Optimizing decision quality with contract algorithms. In: *Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence (IJCAI)*. pp. 1576–1582. Montreal, Canada (1995)

- [69] Zilberstein, S.: Using anytime algorithms in intelligent systems. *AI Magazine* **17**(3), 73–83 (1996)