Comment: There are several instances of long source strings that make unclear the specific contribution.

Response: I sincerely thank the reviewer for this critical observation. Based on this comment, I identified three types of problematic instances where my specific contributions were obscured:

- **Type 1: Prior work and our contributions narratively intertwined** - Long prose paragraphs mixing prior work limitations with our novel solutions, compounded by **heavy citation clustering** that reduces readability and makes it unclear where existing work ends and our contribution begins.
- **Type 2: Implementation details obscuring conceptual contributions** - Technical descriptions that present system operations in implementation-oriented "source string" format, reading like technical documentation rather than scholarly analysis of novel contributions.
- **Type 3: Standard operations and novel techniques visually indistinguishable** - Code listings and explanations that present both conventional operations and our innovations in identical format without visual or narrative separation.

Manuscript revision:

Type 1 Example: Related Work (Section 2, Lines 113-119)

- **Original problem:** 180-word "long source string" with **excessive citation clustering** (three citation groups totaling 18+ references) that obscures the narrative distinction between prior work limitations and our contribution.

  Original text: "While blockchain-privacy regulation integration research is actively progressing, current approaches involving centralized controls[18,26,29,42,44], reliance on immutable smart contracts[22,27–30,41–43], and adoption of relationship-centric compliance models[18,26,29,31,35,39,42–44] reveal fundamental incompatibility with blockchain's transaction-based and pseudonymous architecture, necessitating a paradigmatic shift to dynamic, proactive transaction-level enforcement. This section analyzes these limitations and advocates for transaction-centric compliance mechanisms."

- **Revision:** Categorized prior work into three groups (centralized controls (e.g., [18,26]); smart contracts (e.g., [27,28]); relationship-centric models (e.g., [35,39])) + explicitly stated "the research gap that **our approach** addresses."

  Revised text: "Though research on blockchain privacy regulation is actively progressing, current approaches reveal a fundamental incompatibility with blockchain's architecture. The incompatibility of prior approaches falls into three categories. First, centralized intermediaries conflict with decentralization (e.g., [18,26]). Second, smart contract rule checking is reactive, wastes resources, and cannot promptly reflect regulatory updates (e.g., [27,28]). Third, relationship-centric models struggle to assign responsibility under pseudonymity (e.g., [35,39]). This section analyzes these limitations in detail and identifies the research gap that our approach addresses."

Type 2 Examples:

Example 2a: Listing 1 Explanation (Lines 316-317)

- **Original problem:** A 120-word "long source string" presenting the process as a flat enumeration of steps without distinguishing standard ontology population from our novel automated reasoning contribution, making the "specific contribution" unclear.

  Original text: "The process continues with integration of jurisdictional adequacy decisions and technical safeguard requirements into I (e.g., adding specific regulatory data instances such as "US has no GDPR adequacy decision", "health data requires AES-256 encryption"), and definition and implementation of axioms and inference rules (A) for automated legal reasoning (e.g., defining inference rules such as "special category data + US transfer → additional protective measures required")."

- **Revision:** Broke down the "long source string" into structured sentences that clearly articulate our "specific contribution": the automated derivation of compliance requirements through domain-independent axioms, rather than manual encoding of legal scenarios.

Revised text: "Listing 1 shows the RDF triple representation resulting from converting GDPR Article 9 into the O_{GDPR} ontology structure. This process continues with two key steps**.** First, we integrate jurisdictional adequacy decisions and technical safeguard requirements into the knowledge base I. Second**,** unlike existing approaches that require manual rule creation for each legal scenario, we define and implement domain-independent axioms and inference rules (A) that automatically derive compliance requirements from the knowledge base. For example, when our system encounters special category data being transferred to the US, it automatically infers that 'additional protective measures are required' by combining the axioms about data sensitivity, jurisdictional adequacy status, and transfer requirements—without requiring explicit encoding of this specific scenario**."**

Example 2b: Listing 2 (Lines 337-343)

- **Original problem:** 7 RDF triples presented in uniform format with no visual distinction between standard blockchain extraction and our AI inference contributions.
- **Revision:** Separated with inline comments (Lines 1-4: "Standard extraction from blockchain"; Lines 5-7: "Our AI-powered inference (Novel contribution)") + used aiInference: namespace prefix to mark our ontology extensions.*Example 2c: Listing 2 Explanation (Lines 344-355).*

Example 2c: Listing 2 Explanation (Lines 344-355)

- **Original problem:** A 120-word "long source string" that mixes standard metadata extraction techniques with our novel AI inference contribution, making the "specific contribution" unclear.

  Original text: "This example demonstrates that AI-based metadata extraction is implemented through explicit information extraction (extraction of directly verifiable information from transaction data such as health data inclusion, US destination, lack of encryption, use of Standard Contractual Clauses), contextual inference where the AI inference engine performs comprehensive analysis of individual elements to derive contextual information, intent classification involving inference of processing purpose based on transaction patterns and data types (e.g., classification as medical research purpose), and risk assessment through comprehensive evaluation of complex risk factors to determine compliance risk level (e.g., high risk assessment

due to unencrypted international transfer of special category data). This AI inference process provides intelligent analytical capabilities that go beyond simple rule-based matching to interpret transaction meanings in regulatory contexts and proactively assess compliance risks."

- **Revision:** Transformed the implementation-oriented enumeration into scholarly prose by (1) replacing the "source string" format with a conceptually-focused explanation that highlights how our approach differs from existing methods, and (2) breaking down the complex sentence into shorter statements that clearly articulate our "specific contribution": a context-aware inference framework that interprets regulatory meaning beyond pattern matching.

  Revised text: "Listing 2 separates two distinct layers. Lines 1–4 extract verifiable properties using standard parsing with OGDPR vocabulary. These properties include data type, destination, encryption, and transfer mechanism. Lines 5–7 show our novel contribution. AI inference derives processing purpose via AI classification. It also derives risk level via our assessment algorithm and legal basis via our reasoning engine. The aiInference: namespace marks our ontology extensions for AI-generated metadata. This dual-layer approach combines deterministic extraction with probabilistic inference. It enables transaction-level verification without predefined relationships."

Type 3 Example: Query Reason Subsystem (Lines 357-379)

- **Original problem:** 300-word "long source string" with nested clauses where general SPARQL query execution and our dynamic generation technique are described without distinction, obscuring the "specific contribution."
- **Revision:** Added upfront contrastive statement ("Unlike rule-based systems... our AI dynamically generates") + converted to numbered list of three novel capabilities (dynamic query construction; semantic matching; integrated reasoning) + separated Transaction001 example into sequential steps clearly showing our system's operations.

Other revision: English Language Improvement (Total Corrections: 442)

Abstract (12): Grammar & verb forms (4), Word choice (3), Articles (2), Punctuation (2), Relative clauses (1)

Introduction (70): Punctuation (18), Word choice & prepositions (12), Sentence structure (9), Articles (8), Grammar & verb forms (7), Currency notation (6), Redundancy elimination (5), Capitalization (3)

Related Work (82): Capitalization consistency (16), Sentence structure (14), Punctuation (13), Word choice & prepositions (12), Articles (11), Grammar & verb forms (8), Hyphenation (6), Other (2)

System Model (54): Capitalization consistency (18), Articles (14), Sentence structure (8), Punctuation (7), Grammar & verb forms (5), Redundancy elimination (2)

Proposed Method (71): Punctuation (19), Grammar & verb forms (15), Articles (12), Word choice & prepositions (9), Sentence structure (8), Capitalization (5), Number style (2), Other (1)

Experimental Results (89): Capitalization consistency (21), Articles (18), Punctuation (15), Sentence structure (12), Grammar & verb forms (9), Number style (6), Word choice & prepositions (5), Hyphenation (3)

Discussion (42): Sentence structure/conciseness (12), Punctuation (10), Articles (8), Capitalization (5), Word choice & prepositions (4), Hyphenation (2), Redundancy elimination (1)

Conclusions (22): Articles (8), Grammar & verb forms (5), Word choice & prepositions (4), Punctuation (2), Sentence structure (2), Hyphenation (1)

Other Sections (10): Articles (6), Sentence structure (2), Capitalization (2)

Figures and Tables: All figures (2) regenerated at 300 DPI with enhanced readability (color-coding, larger fonts, repositioned legends). Tables (5) reformatted with consistent alignment, clear headers, Capitalization, and improved spacing.