ISSLP
Interdisciplinary Studies in Society, Law and Politics

OPEN PEER REVIEW

International Privacy Protection Laws in Smart Contracts

Amin. Karimpour Aliabad[1]

[1] Department of Law, Yas.C., Islamic Azad University, Yasuj, Iran

*** Corresponding author email address**: 4231891915@iau.ac.ir

Received: 2026-01-08 **Revised:** 2026-05-04 **Accepted:** 2026-05-13 **Published:** 2026-05-01

EDITOR:
Ghasem Eftekhari
Associate Professor, Department of Political Science, University of Tehran, Tehran, Iran. Email: eftekhari@ut.ac.ir
REVIEWER 1:
Kaushalya Koralage
Assistant Lecturer in Sociology
REVIEWER 2:
Asghar Jafari
Associate Professor, Department of Psychology, Kashan University, Iran. Email: as_jafari@sbu.ac.ir

1. Round 1

1.1. Reviewer 1

Reviewer:

The explanation of hybrid legal-technological governance (p. 2–3) is well-articulated, yet the text could be improved by explicitly mapping roles of developers, validators, and front-end providers to corresponding privacy responsibilities to avoid ambiguity regarding accountability.

The treatment of consent (p. 4) is thorough, but the statement "Users may interact with code they cannot read" should discuss potential mitigations, such as standardized consent protocols or user-friendly interfaces, to provide actionable recommendations.

The principle of data minimization (p. 4) is addressed, but the manuscript could include a comparative evaluation of on-chain versus off-chain storage strategies, illustrating trade-offs between immutability and privacy compliance.

On transparency (p. 4–5), the dual meaning between technical and legal transparency is introduced; however, a table or diagram contrasting these two dimensions could enhance reader comprehension of the conceptual distinction.

The accountability section (p. 5) notes cross-border challenges but could be strengthened by proposing concrete jurisdictional allocation frameworks or referencing model regulatory guidelines to operationalize the discussion.

The analysis of fairness and power asymmetries (p. 8–9) is compelling but would benefit from including empirical evidence of actual user harm or case studies demonstrating exploitation of data asymmetries.

Authors revised the manuscript and uploaded the document.

1.2. Reviewer 2

Reviewer:

The cryptographic analysis (p. 5–6) provides technical depth, but the manuscript would benefit from integrating examples of zero-knowledge proofs or secure multiparty computation to illustrate how these techniques address privacy risks practically.

The discussion on behavioral profiling risks (p. 6) could include an explicit link between pseudonymous activity and GDPR-like compliance obligations, demonstrating how legal frameworks interpret blockchain transaction analytics.

In the section on immutability (p. 6), the argument that on-chain personal data may create legal tension could be enhanced by citing specific jurisdictional rulings or enforcement cases where blockchain immutability conflicted with erasure rights.

The treatment of oracles and off-chain data sources (p. 6–7) is comprehensive, but the manuscript could benefit from proposing architectural controls or monitoring mechanisms to mitigate oracle-induced privacy violations.

Cross-border data flows (p. 7) are well described; however, integrating a diagram showing data replication across jurisdictions could clarify the complex regulatory landscape for international readers.

The insufficiency of anonymization (p. 7) raises important points, but the authors might strengthen the argument by presenting experimental data or simulation results showing re-identification probability across pseudonymous addresses.

User comprehension and consent (p. 7–8) discussion could be improved by referencing human-computer interaction research on smart contract interfaces, supporting the claim that users often lack meaningful understanding.

Security vulnerabilities (p. 8) are addressed, but the text should discuss practical mechanisms for continuous auditing, incident response, and cryptographic key lifecycle management to operationalize security recommendations.

The governance discussion (p. 8–9) outlines hybrid control, yet the manuscript could provide concrete frameworks or international standards for decentralized accountability to clarify enforcement mechanisms.

Authors revised the manuscript and uploaded the document.

2. Revised

Editor’s decision: Accepted.
Editor in Chief’s decision: Accepted.