**Article Review 2: Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways**

Student Name: Brandon Rollinson Jr

School of Cybersecurity, Old Dominion University

CYSE201S: Cybersecurity Social Sciences

Instructor Name: Professor Diwakar Yalpi

11/11/2025

## Introduction/BLUF

The article shows tension that increases between the decentralization of blockchain technologies and the requirements of data protection like GDR. BLUF: blockchain is designed to often conflict with data protection legal principles, this paper argues that both pathways require technical design and regulatory policy adjustment that will align with the blockchain and data protection goals.

## Relation/Connection to social science principles

Power and Inequality- This is showing how data can control shift and that individuals may lose control when they use block chain

Social change and technology diffusion- This shows the spread of blockchain and how it is done and altering social expectation about privacy, data control and trust

Ethics and social responsibility- Balancing transparency block chain with privacy individual rights

Risk, Trust, and perception- Individuals trust systems that use blockchain and how risk are socially constructed

Structure vs agency- Blockchain archetype, constraining user choices in data management

Human behaviour and agency- this is how individuals data rights and autonomy are affected when the data enters immutable ledgers

**Research Question/ Hypothesis/ Independent variable/ dependent variable**

The overall research question therefore is: How can blockchain technology be aligned with data protection requirements, in spite of the conflicting principles? The implied hypothesis is that alignment is possible only through combined policy and technical adaptations. The independent variables are blockchain design features and legal requirements; the dependent variable is how well the two can be reconciled in practice.

**Types of research methods**

The study adopts a qualitative, normative‑analytical rather than a purely empirical‑quantifying research method. It reviews literature and such materials as legal frameworks, blockchain technical architectures, and regulatory commentaries. Doctrinal legal analysis is combined with review of the technology and with policy analysis in an effort to identify conflicts and offer solutions. There is no experimental trial or statistical hypothesis testing; instead, the approach is interpretive, conceptual, and multidisciplinary, involving law, technology, and policy.

## Types of Data used

The article utilizes interpretive and thematic analysis in the assessment of tensions between blockchain design and requirements for the protection of data. The author conducts comparative legal analysis by considering how particular provisions of the GDPR interact with blockchain features. This is followed by a gap analysis that identifies where characteristics of blockchain such as its immutability clash with the legal expectations of the right to erase or modify personal data.

## Connections to the concerns or contributions of marginalized groups

While not the central focus, the implications of the article greatly impact marginalized groups who may already not have much control over their data. Blockchain's immutability makes this even worse because it prevents the vulnerable populations from correcting or removing sensitive information. Ensuring compliance with data-protection laws helps protect these groups from digital harm.

## Conclusion

Overall, helps society understand how blockchain can be developed in a responsible manner, keeping in mind the protection of privacy rights. It also underlines the importance of collaboration by technologists and regulators from interdisciplinary backgrounds. The study furthers insight into ways emerging technologies have to adapt in the protection of individuals and promoting equity.

## Cites

Zafar, A. (2025). *Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways*. *Journal of Cybersecurity, 11*(1), tyaf002. https://doi.org/10.1093/cybsec/tyaf002