
Subject: Feedback on Guidelines 02/2025 — The Need for Legal Coherence Respecting Decentralized Technologies and Fundamental Rights

To the European Data Protection Board,

I submit this feedback with deep concern regarding the implications of Guidelines 02/2025 for decentralized public blockchains — in particular, Bitcoin.

Bitcoin is not a speculative instrument or a niche innovation. It is a global, open, decentralized monetary protocol that embodies the principles of **individual sovereignty, privacy, and censorship resistance**. These are not fringe values: they are essential for the protection of human rights in an increasingly digital and centralized world.

However, the draft guidelines — as currently written — pose an **existential legal threat** to this technology, by imposing regulatory expectations that are incompatible with its core design and purpose.

1. Immutability Is a Feature, Not a Violation

Bitcoin's ledger is immutable by design. This immutability ensures integrity, trustlessness, and transparency — all essential to its function as a decentralized system.

To demand erasure of data from Bitcoin, or to declare it non-compliant due to this impossibility, is to fundamentally misunderstand the technology. The assertion in §4.2 that “technical impossibility cannot justify non-compliance” places Bitcoin — and by extension, all truly decentralized systems — in permanent legal jeopardy.

It is not acceptable to demand that **mathematics change to accommodate bureaucracy**. The real world must acknowledge that decentralization introduces new legal paradigms, not errors to be corrected.

2. Anonymity is Not Criminal — It Is Necessary

The suggestion that data must be anonymised before publication collides head-on with anti-money laundering regulations, which treat **privacy-preserving tools as inherently suspicious**.

This false equivalence between **privacy and criminality** is dangerous and must be challenged. Privacy is a **fundamental human right**, not a red flag. In an era of mass surveillance, financial privacy is critical to personal freedom, democratic participation, and protection from authoritarian abuse.

If one must choose between violating the GDPR or violating AML laws — as the current draft implies — then **Europe has failed to provide a coherent legal framework for ethical technological use.**

3. Public Keys Are Not Personal Data in the Context of Bitcoin

A Bitcoin public key, by itself, is not tied to any natural person and carries no semantic meaning. It is a pseudonymous mathematical identifier used in a system explicitly designed to **minimize unnecessary data collection.**

Declaring all public keys “personal data” under GDPR creates an impossibly wide net and criminalizes the use of basic internet infrastructure, not just blockchains.

The EDPB should **clearly distinguish** between systems designed to collect personal data, and those designed to **preserve privacy by default.**

4. Bitcoin Does Not Need “Permission” to Exist

Bitcoin operates outside of any centralized control — that is its strength and its purpose. It cannot and should not be subject to legal standards written for centralized intermediaries.

Attempting to fit decentralized protocols into frameworks designed for custodians, banks, or SaaS platforms is a category error. **Legal frameworks must adapt to the reality of decentralization,** not the reverse.

Trying to retrofit these systems into compliance will not outlaw Bitcoin — it will simply **push it out of Europe** and **further undermine the EU’s credibility in the global digital innovation space.**

Recommendations:

- Recognize the **fundamental incompatibility** between full GDPR compliance and blockchain immutability, and **create regulatory exemptions or safe harbors** accordingly.
- Stop conflating privacy-preserving technologies with criminal behavior. Demand **coherence between GDPR and AMLR/TFR** to prevent paradoxical compliance obligations.
- Refrain from classifying public keys as personal data in all cases. Adopt a **contextual standard** that accounts for decentralization and pseudonymity.

- Open a working group with blockchain developers, protocol experts, and civil rights advocates to ensure that European regulation **supports digital freedom rather than suppressing it**.

Europe must decide whether it supports **open, decentralized, censorship-resistant infrastructure**, or whether it wishes to become inhospitable to the very technologies that uphold civil liberties in the 21st century.

Respectfully,
Thomas R