Blockchain Collisions and Legal Liability

Author & Research: Celic Torres
co-Research: ariutokitumi

General Aspects

What is an address collision?
It is a situation where the same address can simultaneously exist as an external account (EOA) or smart contract (CA) on one chain ‘A’ and as a smart contract (CA) on another chain ‘B’, generating risks of asset loss and digital property conflicts.

Why are collisions relevant from a legal perspective?
The impact of collisions can result in significant financial losses, disputes over digital asset ownership, legal liabilities for protocols lacking legal protection, developers, and users. This represents a systemic risk that must be addressed both technically and legally.

Legal Responsibility

Who is responsible when a collision loss occurs?
Responsibility can be distributed among various actors:

1. Protocol: For not implementing adequate preventive security measures to avoid collisions
2. Developers: For omission of verification systems
3. Operators: For not warning about known risks
4. Users: According to their level of diligence in verification

Is there legal liability for not implementing verification systems?
The decentralized ecosystem introduces revolutionary challenges for crypto asset management and custody, where user responsibility and blockchain transaction immutability establish a very different liability framework from the traditional financial system. For example, unlike conventional banking where transaction reversibility is possible, blockchain does not yet attribute this possibility.

However, these characteristics do not completely exempt the various ecosystem actors from legal responsibility and the possibility that it may be explored and have binding effects in the future.

The existence of viable technical solutions to prevent collision losses, such as DoppelgangETH, establishes a due diligence standard that protocols cannot ignore without incurring potential technical negligence.

This responsibility is especially magnified when three critical factors converge:

1. The availability of preventive technical solutions

2. The existence of documentation about risks and their implications
3. The predictability and materiality of potential losses

In this context, the adoption of verification systems represents not merely an optional good practice, but a technical and legal imperative for protocols seeking to operate with the due diligence that the decentralized ecosystem demands. The inherent autonomy of blockchain does not dilute responsibilities; it redefines them and, in many aspects, could intensify them.

Rights and Obligations

What rights might users affected by collisions have?

1. Right to claim for losses
2. Right to information about risks
3. Right to reasonable preventive measures
4. Right to compensation in cases of proven negligence

What obligations do blockchain protocols have?

1. Implement adequate security measures
2. Explicitly warn about known risks
3. Maintain updated verification systems

Is there an obligation to return funds received through collision?

Yes, under the principle of unjust enrichment. However, practical execution can be complex due to: Blockchain transaction irreversibility, difficulty in identifying recipients, and due to transaction globalization, which will always depend on the applicable jurisdiction.

Regulatory Aspects

What regulatory frameworks apply to collisions?

Digital financial services regulation
Consumer protection regulations
Civil liability laws
Specific cryptoasset regulation

How does jurisdiction affect collision cases?

Collisions pose jurisdictional challenges due to:
Transnational nature of blockchain
Diversity of regulatory frameworks
Difficulty in determining applicable law
Complexity in enforcing judgments

Prevention and Mitigation

What preventive measures are legally recommended?

1. Implement robust verification systems

2. Maintain updated technical documentation
3. Provide clear risk warnings
4. Establish incident response protocols

How can protocols reduce their legal exposure?
Implementing systems like DoppelgangETH
Maintaining regular audits
Documenting security measures
Establishing clear risk management policies