**Observatoire ARGA**

# Risks for users of grey cryptocurrency schemes: why “rational” circumvention strategies inevitably end in losses

Author:

Sergei Khrabrykh — President of ARGA, PhD

Organization: Observatoire ARGA – Sanctions and Compliance Unit

Mailing address: 21 route de l’Aviation, 12 C, 64600 Anglet, FRANCE

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org

Paris, 18 January 2026

## Table of Contents

# Abstract

This report analyzes the risks faced by users who, knowingly or unknowingly, become involved in grey cryptocurrency schemes, including unregulated OTC operations, informal exchangers, non-custodial routes, DeFi infrastructure, and pseudo-legal investment structures. It examines typical illusions of safety, errors in risk assessment, institutional traps, and legal consequences that lead to loss of assets, criminal and sanctions risks, and the impossibility of legal protection. Particular attention is given to why "knowledgeable" users and professional market participants often prove to be the most vulnerable.


# Introduction

Grey cryptocurrency schemes are often perceived as a compromise between legality and efficiency. Users assume that partial compliance with rules, technical literacy, and avoidance of overtly criminal tools allow them to minimize risks.

Practice demonstrates the opposite. Grey zones become the primary concentration point for legal, financial, and reputational losses. Users operating outside transparent regulation lose both institutional protection and the ability to appeal to good faith.

# What is meant by grey crypto schemes

Grey schemes refer to models of cryptocurrency use that:

- are not formally prohibited;
- but bypass or blur regulatory requirements;
- rely on informal intermediaries;
- exclude standard procedures for protecting rights.

These include:

- OTC exchanges outside licensed frameworks;
- non-custodial routes without identification;
- private peer-to-peer exchanges;
- pseudo-investment products without risk disclosure.

# Illusion of control and technical competence

One of the key user errors is the belief that:

- knowledge of blockchain;

- control over private keys;
- use of “proper” networks and wallets

ensure safety. In practice, technical autonomy means the absence of an arbiter, guarantees, and mechanisms for restoring violated rights.

## OTC operations as a zone of maximum risk

The OTC market is often perceived as a “professional” segment. However, it is characterized by:

- absence of formal contracts;
- opacity of settlements;
- impossibility of proving transaction terms;
- high dependence on the good faith of intermediaries.

In the event of conflict or loss of funds, the user remains outside the legal framework.

## Non-custodial routes and lack of protection

The use of non-custodial wallets excludes:

- the possibility of blocking a fraudster;
- intervention by a third party;
- suspension of a transaction.

Any mistake, abuse, or conflict results in irreversible loss of funds without compensation.

## DeFi as a risk multiplier

DeFi protocols are often used as part of grey schemes. Users underestimate:

- smart contract risks;
- governance asymmetry within DAOs;
- absence of procedural protection.

In the event of a hack, exploit, or change in protocol rules, there is no protection of user rights.

## Retroactive legal qualification

Grey schemes are particularly vulnerable to retrospective qualification. What appears permissible today may tomorrow be classified as:

- facilitating money laundering;
- sanctions evasion;
- participation in unlicensed financial activity.

At the same time, the user is deprived of arguments based on good faith.

## Sanctions and secondary risks

Participation in grey crypto schemes may result in:

- freezing of assets;
- denial of service by platforms;
- inclusion in sanctions frameworks;
- secondary sanctions.

Even indirect involvement in a transaction chain can lead to exclusion from financial infrastructure.

## Risks of criminal and administrative prosecution

Law enforcement in grey zones is selective in nature. Users may become:

- convenient procedural targets;
- sources of evidence against others;
- objects of pressure to “uncover” the scheme.

The absence of formal status and contractual basis increases vulnerability.

## Inability to prove good faith

In grey schemes, the user:

- cannot confirm the terms of the transaction;
- lacks evidence of compliance with procedures;

- is deprived of the ability to rely on market standards.

This leads to the loss of the presumption of good faith.

## Secondary victimization of users

Even when they are victims, users of grey schemes:

- are not recognized as victims;
- are blamed for carelessness;
- are deprived of procedural status;
- are excluded from compensation mechanisms.

The system perceives them as participants in the risk.

## Behavioral traps and cognitive biases

Key psychological factors include:

- the effect of “I understand more than others”;
- illusion of control;
- normalization of grey practices;
- fear of formal regulation.

These biases are systematically exploited by intermediaries and schemes.

## Why the “knowledgeable” lose more often

Professional users are more likely to:

- engage in complex schemes;
- assume higher risks;
- operate outside formal frameworks.

As a result, they become the most vulnerable when law enforcement intervenes.

## Institutional consequences of the spread of grey schemes

Widespread use of grey practices:

• undermines trust in the market;

• intensifies regulatory pressure;

• leads to collective punishment of bona fide participants.

Grey schemes accelerate strict and often excessive regulation.

## Conclusions

Grey cryptocurrency schemes are not a compromise between efficiency and safety. They represent a zone of maximum risk where users lose both financial and legal protection. The illusion of rationality in such strategies systematically leads to losses.

## Recommendations

- Excluding grey schemes from operational practice.
- Using licensed and regulated frameworks.
- Recording transaction terms in legally significant form.
- Assessing not only technical but also legal risks.
- Recognizing that autonomy without institutional protection equals vulnerability.

## List of sources and materials used


1. https://www.fatf-gafi.org/en/topics/virtual-assets.html
2. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
3. https://www.imf.org/en/publications/fandd/issues/2022/09/regulating-crypto-narain-moretti
4. https://www.europol.europa.eu/crime-areas/economic-crime
5. https://www.interpol.int/What-you-can-do/Crimes/Financial-crime
6. https://argaobservatory.org