**Observatoire ARGA**

# Крипторасследования как новый канал злоупотребления международным розыском:

# типология неправомерных запросов, уязвимости процедур и стратегии защиты

Автор:

Сергей Храбрых — президент ARGA, PhD

Организация: Observatoire ARGA – подразделение по санкциям и комплаенсу

Адрес для корреспонденции: 21 route de l’Aviation, 12 C, 64600 Anglet, FRANCE

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

Сайт: www.argaobservatory.org

Париж, 23 января 2026

## Оглавление

# Аннотация

Настоящий доклад посвящён анализу злоупотреблений механизмами международного розыска в делах, связанных с криптовалютами и цифровыми активами. Рассматриваются типовые сценарии неправомерных запросов, при которых экономические и корпоративные конфликты трансформируются в уголовные криптодела с целью давления, экстрадиции или перераспределения активов. Особое внимание уделено уязвимостям процедурных фильтров, проблеме доказательственных стандартов, политико-экономическому контексту и стратегии защиты через международные механизмы, включая процедуры контроля файлов (CCF).

# 1. Введение

Рост криптопреступности и транснациональных финансовых схем усилил роль международного полицейского сотрудничества. Вместе с тем криптовалютная тематика стала новым каналом злоупотребления международным розыском: технологическая сложность, отсутствие единых стандартов доказывания и трансграничность операций позволяют оформлять экономические конфликты как «нейтральные» уголовные дела.

В результате механизмы международного розыска могут использоваться не только против реальных преступных сетей, но и как инструмент давления в политико-экономических конфликтах.

# 2. Почему криптоквалификация удобна для неправомерных запросов

Криптовалюты обладают рядом свойств, создающих благоприятную среду для манипуляций:

- терминологическая сложность и асимметрия компетенций;
- отсутствие унифицированных судебных стандартов;
- возможность квалифицировать широкий спектр действий как мошенничество или отмывание;
- трансграничность и юрисдикционные конфликты.

Это позволяет придавать делу видимость нейтральности, даже если его реальная природа связана с активами и контролем.

# 3. Типология неправомерных запросов в криптоделах

В международной практике можно выделить несколько устойчивых типов:

1. Корпоративно-рейдерский тип

Уголовное дело инициируется для давления в споре о долях, собственности, управлении компанией или инфраструктурой.

2. Санкционно-политический тип

   Криптоквалификация используется как оболочка для преследования лиц, связанных с санкционными конфликтами, обходом ограничений или политическими разногласиями.

3. Коммерческий конфликт с криминализацией

   Гражданско-правовой спор ретроспективно квалифицируется как мошенничество.

4. Давление на посредников и «facilitators»

   Запросы используются для принуждения к сотрудничеству, передаче ключей, раскрытию информации.

5. Конфискационно-ориентированные дела

   Процесс направлен на блокировку и изъятие криптоактивов как первичный результат.

## 4. Уязвимости процедурных фильтров

Механизмы международного розыска опираются на информацию, предоставляемую национальными органами. В криптоделах процедурные фильтры уязвимы из-за:

- сложности проверки доказательств;
- зависимости от формальной квалификации;
- отсутствия доступа к первичным данным (биржи, кошельки, офчейн);
- разрыва между аналитическими выводами и юридическими фактами.

Это повышает вероятность принятия запроса без выявления политико-экономического контекста.

## 5. Доказательственные риски: ончейн-гипотезы как основание розыска

В криптоделах нередко используются:

- вероятностные выводы блокчейн-аналитики;
- кластеризация адресов;
- предположения о контроле над кошельками.

При отсутствии независимой судебной экспертизы такие выводы могут превращаться в основание международного розыска, что создаёт риск ошибочной атрибуции и неправомерного преследования.

## 6. Несоразмерность мер и трансграничные последствия

Даже в делах с ограниченным ущербом международный розыск способен привести к:

- задержаниям в третьих странах;
- длительным экстрадиционным процедурам;
- блокировке активов и счетов;
- разрушению деловой и социальной жизни.

Несоразмерность мер характеру обвинений является ключевым индикатором неправомерного использования.

## 7. Политико-экономическое измерение: конфликт контроля и собственности

Во многих криптокейсах реальный конфликт лежит в сфере:

- контроля над цифровыми активами;
- доступа к инфраструктуре;
- распределения доходов;
- корпоративного управления.

Уголовная форма используется как инструмент изменения баланса сил и перераспределения собственности.

## 8. Международная практика: повторяющиеся паттерны злоупотреблений

Повторяющиеся признаки неправомерных криптозапросов включают:

- резкая криминализация коммерческих действий;
- отсутствие прозрачной доказательной базы;
- акцент на блокировке активов;
- параллельные корпоративные споры;
- использование розыска как рычага переговоров.

Эти паттерны воспроизводятся вне зависимости от юрисдикции.

## 9. Стратегии защиты в международных механизмах

Эффективная защита требует:

- реконструкции экономической природы конфликта;
- документирования процессуальных нарушений;
- демонстрации несоразмерности мер;
- анализа доказательств и выявления ошибок атрибуции;
- аргументации политико-экономического контекста.

Ключевым является переход от эмоциональной защиты к структурной аналитике.

## 10. Процедуры контроля файлов (CCF) и их значение

Обращения в CCF являются основным инструментом:

- проверки законности обработки данных;
- выявления нарушений нейтральности;
- корректировки неправомерных запросов.

В криптоделах CCF приобретает особое значение из-за высокой вероятности доказательственных ошибок и политико-экономического контекста.

## 11. Роль правозащитной и медийной стратегии

В ряде случаев необходима параллельная стратегия:

- правозащитная (международные инстанции, мониторинг);
- медийная (минимизация репутационных потерь и фиксация контекста).

Однако медийный контур должен использоваться как вспомогательный инструмент и не подменять юридическую аргументацию.

## 12. Риски для государств и международных институтов

Злоупотребления международным розыском:

- подрывают доверие к механизмам сотрудничества;
- снижают готовность государств исполнять запросы;
- усиливают фрагментацию правоприменения.

Для международных институтов это означает утрату легитимности.

# 13. Выводы

Криптовалютная тематика стала новым каналом злоупотребления международным розыском. Формальная нейтральность экономических квалификаций и сложность доказательств создают уязвимости, которые используются в политико-экономических конфликтах. Эффективная защита требует аналитической реконструкции конфликта и использования международных процедур контроля файлов.

# 14. Рекомендации

1. Повышение стандартов проверки доказательств в криптозапросах.
2. Выявление и документирование политико-экономического контекста.
3. Усиление роли CCF и процедурных гарантий.
4. Развитие независимой криптоэкспертизы в судебных процедурах.
5. Институционализация защиты жертв и добросовестных лиц в трансграничных делах.

# Перечень использованных источников и материалов


1. https://www.fatf-gafi.org/en/topics/virtual-assets.html
2. https://www.imf.org/en/publications/fandd/issues/2022/09/regulating-crypto-narain-moretti
3. https://www.bis.org/publ/qtrpdf/r_qt2103.htm
4. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html
5. https://www.europol.europa.eu/crime-areas/economic-crime
6. https://www.unodc.org/unodc/en/cybercrime/home.html
7. https://www.interpol.int/What-you-can-do/Crimes/Financial-crime
8. https://argaobservatory.org
9. https://www.interpol.int/How-we-work/Notices
10. https://www.interpol.int/How-we-work/Data-protection
11. https://www.bis.org/publ/qtrpdf/r_qt2103.htm