🏛️ Foundation: Безопасный вход в сферу криптовалюты, OpSec и Налоги

КУРС 1 | ОБЯЗАТЕЛЬНЫЙ МОДУЛЬ — ФУНДАМЕНТ

Добро пожаловать в первый модуль курса. Данный документ представляет собой полное практическое руководство по безопасному входу в мир криптовалют. Материал изложен без лишних деталей и маркетинговых обещаний — исключительно проверенные архитектурные знания, конкретные инструменты и пошаговые инструкции, обеспечивающие защиту Ваших средств с первого дня. Курс охватывает пять критических направлений: архитектуру блокчейн-сетей, операционную безопасность кошельков, P2P-обмен с AML-гигиеной, международную легализацию капитала и анатомию Web3-мошенничества.

Криптовалютный рынок представляет собой пространство значительных возможностей, однако одновременно является зоной повышенного риска. Ежегодно тысячи пользователей несут финансовые потери вследствие элементарных ошибок: отправки активов в неверную сеть, хранения сид-фразы в облачных сервисах, подписания фишинговых транзакций. Настоящий курс разработан с целью предотвращения подобных ситуаций. Каждый модуль основан на реальных прецедентах и апробированных практиках, применяемых профессиональными крипто-операторами.

Материал структурирован по принципу от фундаментальных основ к практическому применению: на начальном этапе Вы получите глубокое понимание внутреннего устройства блокчейна, затем освоите корректные методы хранения ключей, проведения безопасных транзакций с банковскими структурами и легализации дохода. Завершает курс детальный разбор актуальных мошеннических схем и экстренный протокол действий при компрометации кошелька. Настоятельно рекомендуется проходить каждый модуль последовательно — пробелы в базовых знаниях в сфере криптовалют влекут значительные финансовые потери.

📐 Модуль 1. Архитектура сетей и Блокчейн 2.0

РАЗДЕЛ 1.1

Как работает блокчейн: Блоки, Хэширование и Консенсус

Основополагающий принцип: Блокчейн представляет собой распределённый цифровой реестр (базу данных), который одновременно хранится и обновляется на тысячах независимых серверов (нод) по всему миру. Данная система не имеет центрального владельца, банка или администратора. Именно эта децентрализация обеспечивает устойчивость к цензуре, несанкционированному доступу и манипуляциям — для фальсификации записи злоумышленнику потребовалось бы скомпрометировать более 51% всех нод одновременно, что является практически неосуществимым.

При отправке криптовалюты транзакция не проходит через единый сервер. Она транслируется в сеть, где ноды проверяют её корректность: достаточность средств на балансе, правильность цифровой подписи, соответствие правилам протокола. После верификации транзакция поступает в «мемпул» — очередь операций, ожидающих подтверждения. Майнеры (в PoW) или валидаторы (в PoS) собирают транзакции из мемпула и формируют из них новый блок.

Каждый блок содержит криптографическую ссылку на предыдущий блок — это и составляет «цепочку». Хэш каждого блока вычисляется с учётом хэша предыдущего, поэтому изменение данных в любом блоке автоматически влечёт изменение хэшей всех последующих блоков. Сеть незамедлительно обнаруживает несоответствие и отвергает фальсифицированную ветку. Именно эта математическая взаимосвязь обеспечивает неизменяемость блокчейна — не вследствие административного запрета на изменение данных, а в силу технической бессмысленности подобных попыток: фальсификация будет мгновенно отклонена всеми добросовестными нодами.

Анатомия одного блока:

1	2	3
Список транзакций Детализированная запись всех операций внутри блока: *«Адрес А перевёл адресу Б 100 USDT»*. Каждая транзакция содержит адрес отправителя, адрес получателя, сумму, комиссию и цифровую подпись.	**Хэш блока** Уникальный цифровой идентификатор блока, генерируемый посредством алгоритма SHA-256 (Bitcoin) или Keccak-256 (Ethereum). Любое изменение данных внутри блока полностью меняет его хэш — даже единственный изменённый символ.	**Хэш предыдущего блока** Ссылка, которая жёстко связывает текущий блок с предыдущим. Именно данная связь формирует «цепочку» и обеспечивает неизменяемость всей истории транзакций с момента запуска сети.

Защита от подделки: Любое изменение данных внутри блока полностью меняет его хэш. Вся последующая цепочка нарушается, и остальные участники сети автоматически отвергают фальсифицированную версию. Это не политика безопасности — это математическая неизбежность.

Сравнение механизмов консенсуса

Механизм консенсуса представляет собой совокупность правил, по которым участники сети приходят к соглашению относительно следующего валидного блока. От выбора механизма зависят скорость, стоимость транзакций и экологичность сети.

⛏️ Proof-of-Work (PoW)

Майнеры расходуют электроэнергию и вычислительные мощности для решения криптографических задач (Bitcoin, Litecoin). Механизм отличается максимальной надёжностью, подтверждённой многолетней практикой — сеть Bitcoin функционирует без сбоев с 2009 года. Основные недостатки: низкая скорость (10 минут на блок в Bitcoin) и высокое энергопотребление. Комиссии в периоды пиковой нагрузки могут достигать $10–$30 и выше.

🔒 Proof-of-Stake (PoS)

Валидаторы блокируют монеты в залог (стейкинг) вместо майнинга (Ethereum с 2022 года, Solana, Cardano). Механизм обеспечивает высокую скорость подтверждения (1–5 секунд), экологичность (потребление энергии снизилось на 99,95% после перехода Ethereum) и минимальные комиссии. Ключевой риск: теоретическая возможность атаки 51% при концентрации стейка у одного участника.

🌐 Экосистема сетей: L1 vs L2

РАЗДЕЛ 1.2 | ШПАРГАЛКА ПО ПЕРЕВОДАМ

⚠ ⚠️ **Критическое правило:** Не все блокчейны одинаковы. Отправка средств в несовместимую сеть (например, USDT ERC-20 на адрес Solana) влечёт их **безвозвратную утрату**. Перед подтверждением каждой транзакции необходимо убедиться в корректности сети отправления и получения. Транзакции в блокчейне необратимы и не подлежат отмене.

Понимание различий между Layer 1 и Layer 2 является одним из наиболее практически значимых навыков при работе с криптовалютными активами. От правильного выбора сети зависит итоговая стоимость перевода: комиссия может составлять как $0.03, так и $15 за транзакцию USDT. Значительная часть финансовых потерь среди пользователей обусловлена именно недостаточным пониманием архитектуры сетей: аббревиатура «USDT» не указывает на единый актив — данный токен существует одновременно в десятках различных сетей, каждый экземпляр которого представляет собой отдельный токен с собственным смарт-контрактом.

Layer 1 — Базовые сети

Bitcoin, Ethereum, Solana, TRON. Обеспечивают максимальный уровень безопасности и децентрализации, однако в периоды высокой нагрузки комиссии в сети Ethereum могут достигать $10–$30 и более. Сети L1 обрабатывают все транзакции самостоятельно — каждая операция записывается непосредственно в основной блокчейн, что гарантирует максимальную степень защиты, но ограничивает общую пропускную способность.

- Bitcoin — максимальная децентрализация
- Ethereum — лидер по DeFi и NFT
- Solana — высокая скорость, низкие комиссии
- TRON — популярен для USDT-переводов

Layer 2 — Масштабируемые надстройки

Arbitrum, Optimism, Base. Агрегируют сотни транзакций за пределами основного блокчейна, компрессируют их в единый пакет и направляют сводный отчёт в Ethereum L1. По аналогии со скоростной магистралью, проложенной параллельно обычной дороге: трафик обрабатывается значительно быстрее, тогда как конечная точка назначения остаётся неизменной.

- Комиссия снижается до **$0.01–$0.05**
- Скорость возрастает до **1–2 секунд**
- Безопасность обеспечивается L1 (Ethereum)
- Оптимальны для повседневных переводов USDT/USDC

Чек-лист выбора сети при отправке

→ Для повседневных переводов USDT/USDC

Рекомендуется использовать сети L2 (Arbitrum One, Base) либо альтернативные L1 (Solana, TRON). Применение Ethereum Mainnet целесообразно исключительно при переводе значительных сумм, когда приоритет безопасности превышает значимость комиссионных издержек.

→ Нативная монета для газа

Комиссия **всегда** списывается в нативной монете выбранной сети. Пример: для перевода USDT в сети Arbitrum на балансе должен присутствовать ETH именно в сети Arbitrum (а не ETH в сети Ethereum).

→ Проверка адреса получения

Необходимо убедиться в том, что принимающая сторона поддерживает именно ту сеть, которая выбрана для отправки. Адреса в различных сетях могут иметь идентичный формат, однако быть несовместимыми между собой.

Сеть	Тип	Комиссия (USDT)	Скорость	Газ
Ethereum Mainnet	L1	$3–$30+	1–5 мин	ETH
Arbitrum One	L2	$0.01–$0.05	1–2 сек	ETH (Arb)
Base	L2	$0.01–$0.03	1–2 сек	ETH (Base)
Solana	L1	~$0.001	<1 сек	SOL
TRON	L1	~$1	1–3 мин	TRX

🔐 Модуль 2. Кошельки и Операционная Безопасность (OpSec)

РАЗДЕЛ 2.1

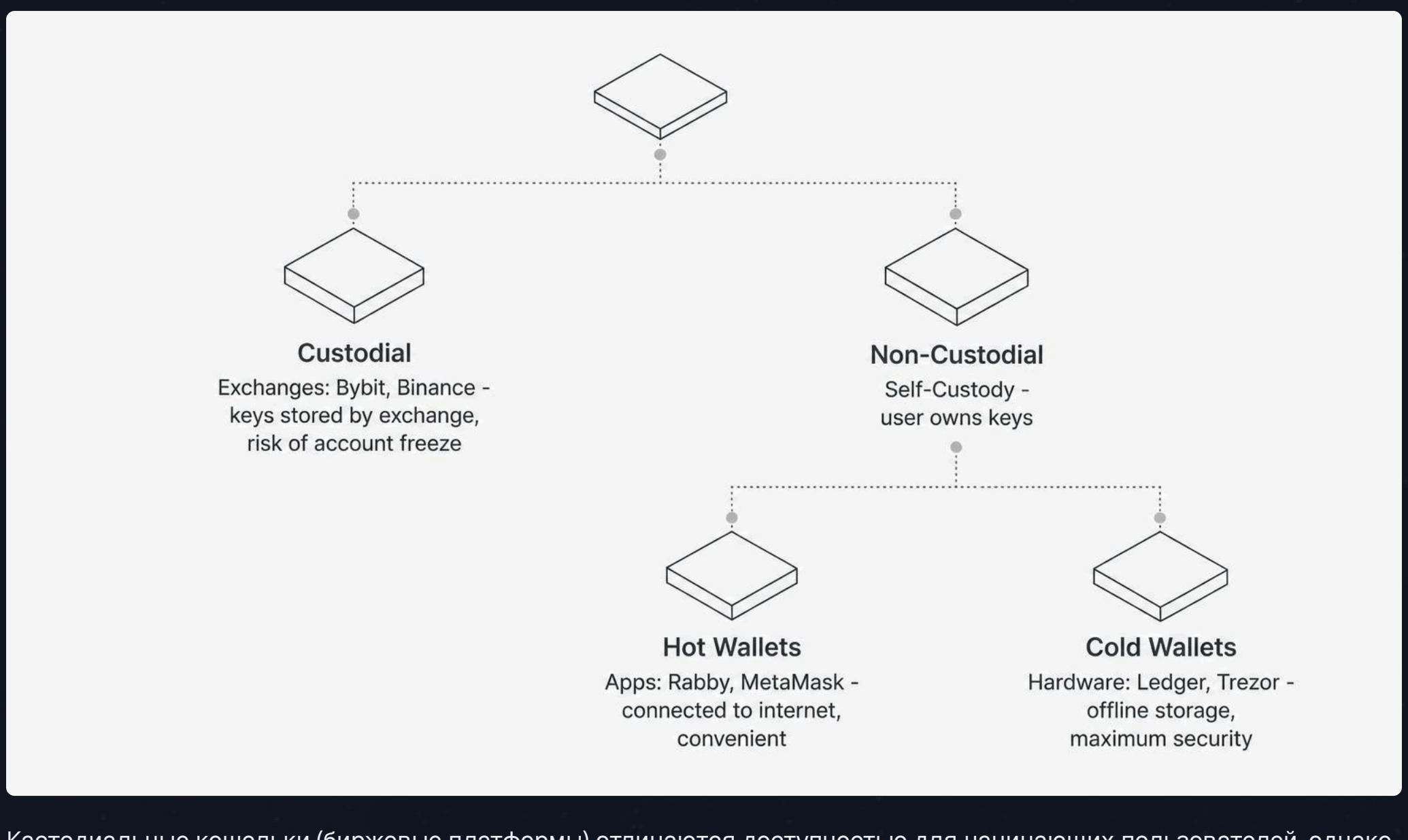
Развенчание фундаментального заблуждения о кошельках

🛑 **Заблуждение:** Криптовалюта физически хранится в приложении на смартфоне или на аппаратном носителе.
✅ **Действительность:** Криптовалюта **ВСЕГДА** находится внутри блокчейна. Кошелёк представляет собой исключительно инструмент управления, содержащий Ваши приватные ключи доступа. Уничтожение инструмента не влечёт уничтожения криптовалюты. Однако утрата ключей означает безвозвратную потерю доступа к активам.

Данное фундаментальное непонимание влечёт за собой критические ошибки. Пользователи создают скриншоты сид-фраз, сохраняют их в облачных хранилищах, передают через мессенджеры в целях «резервного копирования» — и утрачивают все активы при первой же утечке данных. Понимание архитектуры кошельков является первым шагом к обеспечению подлинной безопасности.

Приватный ключ представляет собой большое случайное число, математически связанное с Вашим публичным адресом в блокчейне. Подписывая транзакцию приватным ключом, Вы криптографически подтверждаете право распоряжения средствами на данном адресе. Сид-фраза из 12 или 24 слов является удобочитаемым представлением мастер-ключа, из которого по установленному стандарту (BIP-39) генерируются все приватные ключи для различных монет и сетей.

Классификация кошельков



Кастодиальные кошельки (биржевые платформы) отличаются доступностью для начинающих пользователей, однако несут существенный операционный риск: биржа может заморозить счёт, подвергнуться взлому или прекратить деятельность (показательный пример — крах FTX в 2022 году). Некастодиальные кошельки обеспечивают полный контроль над активами, однако возлагают на пользователя исключительную ответственность — восстановление доступа при утрате сид-фразы не представляется возможным ни при каких обстоятельствах.

Кастодиальные

Bybit, Binance, OKX. Ключи хранятся на стороне биржи. Рекомендованы для начального этапа, однако сопряжены с риском заморозки счёта, выполнением требований KYC и зависимостью от третьей стороны.

Горячие (программные)

Rabby, MetaMask, Trust Wallet. Ключи хранятся на устройстве пользователя, которое постоянно подключено к сети Интернет. Оптимальны для проведения ежедневных операций, однако уязвимы к воздействию вредоносного программного обеспечения.

Холодные (аппаратные)

Ledger, Trezor. Приватные ключи не покидают устройство ни при каких условиях. Обеспечивают максимальную защиту от угроз удалённого доступа. Настоятельно рекомендованы для хранения значительных сумм (от $1 000 и выше).

🔑 Сид-фраза и Revoke.cash

РАЗДЕЛЫ 2.2 – 2.3

Сид-фраза (Seed Phrase) — основной документ владельца кошелька

Сид-фраза из 12 или 24 слов представляет собой математический мастер-ключ, из которого генерируются все приватные ключи. Лицо, владеющее сид-фразой, получает полный доступ ко всем средствам на всех адресах кошелька — без каких-либо исключений. Это не пароль, поддающийся восстановлению через службу поддержки, и не учётная запись, которую можно вернуть через электронную почту. Это абсолютный и безоговорочный доступ к Вашим цифровым активам.

Стандарт BIP-39, по которому генерируются сид-фразы, использует словарь из 2048 слов. Комбинация 12 слов предоставляет 2^128 возможных вариантов — это число превышает количество атомов в наблюдаемой вселенной. Подбор сид-фразы методом перебора исключён даже при использовании всей совокупной вычислительной мощи современных компьютеров. Вместе с тем хищение сид-фразы представляет собой реальную угрозу при несоблюдении правил хранения.

1 Исключение цифровых носителей

Категорически не рекомендуется создавать скриншоты, сохранять сид-фразу в заметках, мессенджерах, iCloud или Google Диске. Любое облачное хранилище подвержено риску несанкционированного доступа. Компрометация одной учётной записи влечёт безвозвратную утрату всех цифровых активов.

2 Использование физических носителей

Рекомендуется записать фразу от руки на бумажном носителе в двух экземплярах либо зафиксировать её на металлической пластине (например, Cryptosteel). Копии следует хранить в разных физических местах — в целях защиты от пожара, затопления или кражи.

3 Ввод исключительно при восстановлении

Сид-фраза вводится **исключительно** в официальном приложении кошелька при первоначальной настройке или процедуре восстановления. Любой интернет-ресурс, запрашивающий сид-фразу, является мошенническим. Биржи, службы поддержки и процедуры верификации не вправе запрашивать данную информацию.

Пошаговое руководство: Управление разрешениями в Revoke.cash

При обмене токенов на децентрализованных биржах (Uniswap, PancakeSwap) пользователь предоставляет смарт-контракту разрешение (*Approval*) на доступ к своим токенам. В случае компрометации соответствующего протокола злоумышленники получают возможность вывести средства без ведома владельца — поскольку выданное разрешение остаётся активным. Регулярная проверка и отзыв устаревших разрешений являются обязательным элементом операционной безопасности для пользователей Web3.

Рекомендуется проводить проверку через Revoke.cash с периодичностью один раз в 1–2 месяца, в особенности после активного взаимодействия с новыми DEX-протоколами. Данная процедура позволяет предотвратить значительные финансовые потери в случае компрометации любого из протоколов, с которыми Вы ранее взаимодействовали.

💳 Модуль 3. P2P, Работа с Банками и AML-гигиена

РАЗДЕЛ 3.1

Механика P2P-обмена

P2P (Peer-to-Peer) представляет собой прямой обмен фиатных денежных средств на криптовалюту между двумя участниками, где биржа выступает независимым арбитром (гарантом/эскроу). Данный способ является основным методом ввода и вывода средств для пользователей из стран СНГ, в которых прямые банковские переводы на криптобиржи заблокированы или существенно ограничены.

Механика функционирования следующая: продавец формирует объявление с курсом и условиями, покупатель находит его и открывает ордер. Криптовалюта продавца блокируется на эскроу-счёте биржи. Покупатель осуществляет перевод фиатных средств на банковскую карту продавца. После получения денежных средств продавец подтверждает факт их поступления в интерфейсе биржи, после чего криптовалюта разблокируется и зачисляется на счёт покупателя. В случае возникновения спора арбитр биржи рассматривает доказательства, предоставленные обеими сторонами.

1

Покупатель

Открывает ордер и осуществляет перевод фиата на карту продавца по указанным реквизитам

2

Биржа / Эскроу

Блокирует криптовалюту продавца до подтверждения факта получения фиатных средств

3

Продавец

Получает фиат, верифицирует баланс в банковском приложении и разблокирует криптовалюту

Защита от схемы «Треугольник» и P2P-гигиена

⚠ ⚠️ **Схема «Треугольник»:** Злоумышленник создаёт ордер на бирже, вынуждает третье лицо перевести денежные средства на Вашу карту, а сам получает Вашу криптовалюту. В результате Ваша банковская карта блокируется, а Вы получаете претензии от пострадавшего лица, которое не осведомлено о существовании биржи и расценивает Вас как участника мошеннической схемы.

Схема реализуется следующим образом: злоумышленник находит жертву вне биржи (например, в мессенджере Telegram) и предлагает условия «выгодного» обмена валюты. Он передаёт жертве реквизиты Вашей карты, полученные из размещённого на бирже P2P-ордера. Жертва осуществляет перевод денежных средств, полагая, что совершает обмен с мошенником напрямую. Злоумышленник фиксирует поступление средств по Вашему P2P-ордеру, подтверждает получение и получает Вашу криптовалюту. Жертва, не получив обещанного, обращается в банк с заявлением о мошенничестве — с указанием Вашей карты. Банк блокирует карту в соответствии с требованиями 115-ФЗ, а Вы лишаетесь криптовалюты и доступа к счёту.

Совпадение ФИО

Принимайте и отправляйте денежные средства **исключительно** с карт, где имя владельца полностью совпадает с ФИО верифицированного аккаунта на бирже. В случае несовпадения имени в реквизитах — отменяйте ордер и выбирайте иного контрагента.

Проверка банк-клиента

Не следует подтверждать получение средств на основании SMS-уведомлений или скриншотов квитанций. Необходимо лично авторизоваться в банковском приложении и проверять актуальный баланс. Скриншоты поддаются фальсификации в течение нескольких секунд посредством стандартных графических редакторов.

Чистые комментарии

В назначении платежа при банковском переводе **категорически запрещается** указывать следующие слова и словосочетания: «крипта», «USDT», «bitcoin», «p2p», «бинанс». Поле назначения платежа следует оставлять пустым или указывать «перевод физическому лицу». Использование данных терминов активирует AML-фильтры банка.

AML-безопасность и прогрев карт

РАЗДЕЛ 3.3

AML-безопасность и профилактика блокировок по 115-ФЗ

AML (Anti-Money Laundering) — система верификации происхождения криптовалютных средств. В случае если актив проходил через даркнет-маркетплейсы, миксеры (Tornado Cash) или скомпрометированные биржи, ему присваивается статус **High Risk**. Банковские учреждения и биржевые платформы применяют специализированные AML-сервисы (Crystal, Chainalysis, Bitquery) для отслеживания происхождения средств. Получение криптовалюты с высоким уровнем риска может повлечь блокировку счёта и обязательное предоставление документов, подтверждающих законность источника средств.

Федеральный закон 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём» обязывает банки осуществлять мониторинг подозрительных операций. Систематические P2P-транзакции, в особенности на идентичные или округлённые суммы, подпадают под критерии подозрительной активности. Блокировка по 115-ФЗ не является уголовным преследованием, однако процедура разблокировки сопряжена со значительными административными трудностями: банк запрашивает документальное подтверждение происхождения средств, что представляет нетривиальную задачу для участников P2P-рынка.

Профилактика блокировок карт (115-ФЗ)

- Заведите **отдельную банковскую карту** исключительно для P2P-операций — не допускайте смешения со счётом для заработной платы
- Не превышайте лимит в **3–5 транзакций в день** — частота операций имеет приоритетное значение перед их объёмом
- Избегайте **идентичных округлённых сумм** (50 000, 50 000, 50 000) — подобные паттерны активируют алгоритмы автоматического контроля
- Совершайте стандартные бытовые расходы с данной карты — формируйте профиль обычного потребительского поведения
- Проверяйте входящую криптовалюту через **AML-сервисы** (Crystal, AMLBot) до осуществления вывода средств на карту

Инструменты AML-проверки

До вывода значительных сумм необходимо провести верификацию истории кошелька посредством следующих инструментов:

- **Crystal (crystal.ai)** — профессиональный AML-сканер, применяемый биржевыми платформами
- **AMLBot** — Telegram-бот для оперативной проверки адреса кошелька
- **Bitquery** — ончейн-аналитика с визуализацией графа транзакций
- **Chainalysis Reactor** — корпоративный инструмент с расширенной функциональностью

При значении AML-скора адреса свыше 50% рекомендуется отказаться от приёма данных средств. Необходимо уведомить отправителя о необходимости использования верифицированного кошелька с приемлемым уровнем риска.

3–5

Транзакций в день

Максимально допустимый лимит P2P-операций на одну карту при минимальном уровне риска

98%

Выполнения ордеров

Минимально допустимый показатель надёжности продавца на P2P-платформе

$10K+

Порог для OTC

Пороговое значение суммы, при достижении которого рекомендован переход на лицензированные OTC-платформы

🌍 Модуль 4. Международная Инфраструктура и Легализация

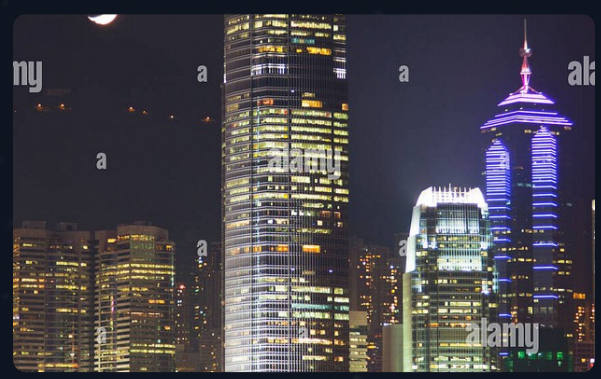
РАЗДЕЛЫ 4.1 – 4.2

Вывод в фиат и крипто-дружелюбные юрисдикции

Для работы с крупным капиталом (от $10 000) стандартного P2P-формата недостаточно. Лимиты P2P-платформ, риски блокировки карт и отсутствие документального подтверждения делают данный метод непригодным для легальной работы с существенными суммами. Профессиональные крипто-операторы применяют легальные международные каналы, обеспечивающие документальную прозрачность и защиту от регуляторных рисков.

🇦🇪 ОАЭ (Дубай)

Лицензированные крипто-обменники (OTC-дески) обеспечивают официальный обмен USDT на дирхамы (AED) или доллары (USD) с зачислением средств на банковский счёт. Дубай располагает чёткой регуляторной базой в лице VARA (Virtual Assets Regulatory Authority). Прохождение процедуры KYC является обязательным условием, однако взамен предоставляется полная легальность операций и комплект документов для целей compliance.



🇭🇰 Гонконг / 🇬🇪 Грузия

Развитая сеть физических криптоматов и OTC-офисов с минимальной налоговой нагрузкой для нерезидентов. Грузия не взимает налог на крипто-доход с физических лиц, не являющихся налоговыми резидентами. Гонконг располагает лицензированными крипто-операторами с возможностью официального проведения обменных операций.

Подтверждение происхождения средств (Source of Funds)

При выводе значительных сумм через международные банки (Wise, Revolut, зарубежные счета) финансовое учреждение запросит документацию о происхождении капитала. Данная процедура является стандартным требованием KYC/AML для всех финансовых институтов. Отсутствие необходимых документов влечёт блокировку счёта и заморозку средств на период проведения расследования.

01

Выписка по P2P-сделкам

Trading History с биржи за последние 6–12 месяцев. Документ должен отражать историю покупок и продаж, суммы, даты и сведения о контрагентах. Выгружается в личном кабинете биржи в формате PDF или CSV.

02

Подтверждение первичного дохода

Налоговая декларация (форма 2-НДФЛ или 3-НДФЛ), договор купли-продажи имущества, расчётный листок по заработной плате либо выписка по счёту, удостоверяющая легальный источник первоначального капитала, направленного на приобретение криптовалюты.

03

История On-Chain транзакций

Выгрузка транзакций с кошелька (посредством Etherscan, Solscan и аналогичных сервисов), подтверждающая прирост капитала через торговую деятельность, стейкинг или иные легальные активности. Данные сведения должны быть согласованы с историей P2P-операций.

Рекомендация: Формирование пакета документов целесообразно начинать с первого дня активной торговой деятельности. Необходимо обеспечить хранение всех выписок, подтверждений ордеров и ончейн-истории в структурированной системе документооборота. При поступлении запроса от банка вся документация должна быть предоставлена в течение 24 часов.

🚨 Модуль 5. Анатомия Скама и Социальная Инженерия

РАЗДЕЛ 5.1

Основные виды Web3-мошенничества

Понимание механизмов мошенничества является наиболее эффективной защитой от него. Каждый из представленных ниже типов скама повлёк значительные финансовые потери у опытных участников рынка. Злоумышленники непрерывно совершенствуют свои методы, однако базовые паттерны остаются неизменными. Рекомендуется тщательно изучить каждый тип — распознавание атаки на ранней стадии позволяет сохранить средства.

🍯 Honeypot (Медовая ловушка)

Смарт-контракт токена написан таким образом, что функция покупки доступна всем участникам, тогда как функция продажи заблокирована создателем. График монеты демонстрирует рост, создавая иллюзию успешного актива, однако вывод средств невозможен. Рекомендация: перед приобретением нового токена необходимо проверить контракт на **Honeypot.is** или **TokenSniffer**.

🏃 Rug Pull (Изъятие ликвидности)

Создатели токена допускают покупку актива, аккумулируют средства инвесторов в пуле ликвидности, после чего резко изымают всю ликвидность и прекращают деятельность. График обваливается до нулевых значений в течение секунд. Защита: необходимо убедиться в наличии блокировки ликвидности (liquidity lock) и реального продукта у проекта.

💉 Drainers (Дрейнеры)

Фишинговый ресурс запрашивает подписание транзакции (например, «для получения бесплатного аирдропа»). Подписывая её, пользователь предоставляет контракту разрешение на списание всех ценных токенов и NFT с кошелька. **Категорически не рекомендуется подписывать транзакции на незнакомых ресурсах.** Рекомендуется использовать Rabby Wallet — он отображает полное содержание подписываемой транзакции.

🚨 ЭКСТРЕННЫЕ МЕРЫ: Порядок действий при подписи скам-транзакции

В случае подписания подозрительной транзакции необходимо незамедлительно действовать в соответствии с установленным алгоритмом. Каждая минута промедления увеличивает объём финансовых потерь.

1 Сохраняйте хладнокровие

Паника является главным препятствием для эффективных действий. Необходимо действовать строго по алгоритму. Эмоциональные решения в сфере криптовалют влекут значительные финансовые потери.

2 Незамедлительно перейдите на Revoke.cash

Отключите кошелёк от всех контрактов. Найдите все активные разрешения (Approval) и выполните их отзыв (Revoke). Данная мера позволит предотвратить дальнейшее несанкционированное списание средств.

3 Создайте новый кошелёк

В случае если дрейнер успел получить разрешение — создайте новый кошелёк на **изолированном устройстве**, не задействованном в предыдущей работе.

4 Переведите оставшиеся средства

Переведите оставшиеся нативные монеты и незатронутые токены на новый кошелёк. Не оставляйте никаких активов на скомпрометированном адресе.

5 Выведите из использования скомпрометированный кошелёк

Скомпрометированный кошелёк подлежит полному выводу из эксплуатации — дальнейшее его использование недопустимо. Даже при отсутствии средств на балансе в настоящий момент, данный адрес представляет потенциальную угрозу в будущем.

🛠️ Специальные материалы и Итоговое задание

SOP-ИНСТРУКЦИЯ | ГЛОССАРИЙ | ПРАКТИКА

SOP: Чек-лист перед заведением $10,000+ на P2P

Данный чек-лист представляет собой стандартную операционную процедуру (SOP) для безопасного проведения крупных P2P-сделок. Следуйте ему при каждой операции без исключений. Пропуск даже одной проверки может повлечь полную утрату средств.

1

Проверка продавца

Мерчант/продавец должен иметь не менее **200 сделок** за последний месяц с процентом выполнения **>98%**. Рекомендуется ознакомиться с отзывами, уделив особое внимание негативным оценкам.

2

Совпадение ФИО

ФИО в реквизитах карты должно на **100%** **совпадать** с верифицированным именем продавца на бирже. Любое расхождение является основанием для немедленной отмены ордера.

3

Разбивка суммы

Сумма сделки разбивается на **2–3 отдельных перевода** в случае, если лимит карты ограничен или сумма превышает стандартный поведенческий паттерн.

4

Личная проверка банка

Личный кабинет банка должен быть открыт в соседней вкладке для **ручной проверки баланса** до подтверждения получения средств.

📖 Web3-Глоссарий (Термины от A до Z)

Термин	Определение
Gas (Газ)	Комиссия, выплачиваемая майнерам/валидаторам за обработку транзакции в блокчейне
Gwei	Мелкая единица Ethereum для измерения цены газа: $1\ \text{Gwei} = 0.000000001\ \text{ETH}$
Slippage (Проскальзывание)	Допустимый процент отклонения цены при исполнении ордера на DEX
Non-Custodial	Способ хранения, при котором исключительно пользователь владеет приватными ключами
Approval	Разрешение смарт-контракту на доступ к токенам на кошельке пользователя
Escrow (Эскроу)	Временное хранение средств третьей стороной до выполнения условий сделки

🏁 Практическое итоговое задание по Курсу 1

Теоретические знания без практического применения не имеют самостоятельной ценности в сфере криптовалют. Выполните все три задания последовательно — на их выполнение потребуется не более 60 минут, однако результатом станет формирование реальных навыков обеспечения безопасности.

Задание 1: Кошелёк

Установите **Rabby Wallet** и надёжно зафиксируйте сид-фразу на физическом носителе (бумага или металл). Проверьте восстановление кошелька по фразе на стороннем устройстве.

Задание 2: P2P-тест

Проведите тестовую P2P-сделку на бирже на **минимальную сумму**, соблюдая требования совпадения ФИО и верификации баланса в банк-клиенте.

Задание 3: Revoke.cash

Проверьте Ваш адрес на сервисе **Revoke.cash** и убедитесь в отсутствии сторонних бессрочных доступов. Отзовите все неизвестные Approval.

Поздравляем! Вы успешно завершили Курс 1 — фундаментальный модуль безопасной работы с криптовалютами. Вы освоили принципы функционирования блокчейна, методы защиты кошелька, правила безопасного проведения P2P-сделок и алгоритм действий в нештатных ситуациях. Полученные знания составляют основу, на которой формируются все последующие компетенции крипто-оператора.