

Whitepaper товарного токена

Декларация

**проекта по выпуску товарных
токенов на платформе**

“Lockton Finance”

Ташкент, Узбекистан

1. ВВЕДЕНИЕ

За последнее десятилетие лет мир стал свидетелем бурного роста принятия цифровых решений в сфере обмена товарными активами. Эти инструменты дали возможность людям по всему миру совершать транзакции между собой, а также контролировать товарные потоки удобно и быстро. Но, несмотря на их распространенность, большинство таких систем представляют собой всего лишь новые логические слои поверх устаревшей банковской системы. Они работают в изолированных, наследственных средах, напрямую свидетельствующих об устаревшей архитектуре технологий на которых они основаны.

Хотя сегодня информация и передается свободно, передвижение стоимости остается замкнутым внутри традиционных рамок.

Технология блокчейна и криптографические активы имеют все основания улучшить эти традиционные стандарты. Они предоставляют надежное и децентрализованное управление данными между разнообразными участниками и предоставляют новые методы передачи стоимости, соотносимые с современным глобальным экономическим контекстом.

Модуль по токенизации товарных активов на платформе Lockton Finance был создан с целью **построения** открытой и интегрированной системы обмена ценностями. Этот сервис представляет товарный мировой рынок как технологичный, открытый, децентрализованный, высокоэффективный и доступный каждому.

Lockton Finance предоставляет комплексное решение **для обмена товарными ценностями между компаниями по всему миру**. Объединив передовые технологические инструменты и эффективные организационные механизмы, платформа реализует передачу товарных активов через токенизацию RWA актива в товарный токен:

- Товарный токен: Цифровой аналог товара, который может использоваться для отслеживания цепочки поставок или как инструмент обмена на товар или услугу.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Платформа Lockton Finance (оказывающая услуги на информационных ресурсах: lockton.uz – для резидентов Республики Узбекистан, и lcktn.com – для иностранных резидентов) предоставляет своим зарегистрированным пользователям, доступ к функционалу модуля структурированной токенизации.

В общем смысле под токенизацией понимается процесс выпуска и оборота специальных товарных токенов, для осуществления сделок и учета прав в отношении токенизируемых товаров и/или партий товаров.

В данном контексте под токенизируемыми товарами понимаются как непосредственно сами товары (объекты материального мира), так и услуги и различные категории активов (права требования).

Под товарными партиями понимается определенное количество (от одной и более единицы измерения) одной или нескольких товарных групп/категорий. При этом, их оборот может осуществляться на повторяющейся основе в рамках единых договоренностей между сторонами, и с одним и тем же составом участников (контрагентов).

На платформе Lockton Finance, в соответствии с нормами действующего законодательства Республики Узбекистан, под товарными токенами понимаются цифровые отражения токенизируемого товара (товарных партий), которые учитывают предоставленное инициатором сделки (правообладателем) право собственности / требования на токенизируемые товары и/или товарные партии.

Инициаторы сделки¹ (правообладатели на товар / товарные партии) могут провести токенизацию на общих правилах эмиссии товарных токенов, по правилам платформы и действующего законодательства Республики Узбекистан, либо воспользоваться отдельным решением по структурированной токенизации. Данная Декларация содержит условия и правила в отношении данного решения.

Структурированная токенизация на платформе Lockton Finance предоставляет возможность оптимизировать процессы заключения и исполнения сделок с токенизированными товарами, с использованием специального решения по товарным токенам от Lockton Finance.

В этом случае Lockton Finance предоставляет для зарегистрированных пользователей платформы инфраструктуру и сервис учета передачи прав в

¹ В контексте данного документа термин «сделка» применяется по отношению к разовой передаче прав на токенизируемый товар, а повторяющиеся сделки – в отношении товарных партий. В последующем применение термина «сделка», также распространяется и на повторяющиеся сделки, которые осуществляются между сторонами в аналогичном режиме, что и разовая сделка с токенизированными товарами на платформе в рамках модуля структурированной токенизации.

отношении токенизируемых товаров/товарных партий на принципах схожих с аккредитивом.

Все операции на платформе Lockton Finance осуществляются посредством учетного токена доступа LCH. Условия по эквивалентной ставке (номинальном стоимостном выражении) в отношении токенов LCH, а также условия их хранения и учета, устанавливаются Правилами платформы, Декларацией токенов LCH, а также другими документами крипто-депозитария и соглашениями с пользователями.

Товарные токены токенизируемых на платформе Lockton Finance товаров, так же, как и токен LCH, являются невыводимыми и не могут функционировать вне экосистемы крипто-депозитария.

В рамках структурированной токенизации, Lockton Finance имеет право выпускать товарный токен, а правообладатель как инициатор сделки имеет право только инициировать выпуск товарных токенов на платформе Lockton Finance на принадлежащие (на основании права собственности, или на основании права требования) товары / товарные партии.

2.2. СТРУКТУРИРОВАННАЯ ТОКЕНИЗАЦИЯ

Подача заявки

Для осуществления сделок с токенизированными товарами начальным этапом действий является подача заявки через модуль структурированной токенизации на платформе Lockton Finance по выпуску товарного токена в отношении товара / товарных партий.

Инициатор сделки (правообладатель) должен быть зарегистрированным пользователем платформы Lockton Finance и должен иметь статус хозяйствующего субъекта, исходя из требований применимого законодательства.

Для этого инициатор сделки (правообладатель) предоставляет Lockton Finance как эмитенту информацию о приобретателе (зарегистрированном пользователе платформы) и необходимую информацию в отношении токенизируемых товаров/товарных партий, что может включать в себя следующее:

- полное описание товара, услуги или актива, включая характеристики, свойства, и особенности;
- сертификаты, лицензии или другие документы, подтверждающие происхождение и соответствие токенизируемых товаров, в том числе таможенные документы, если товар ввозиться из другой страны;

- накладные или счета-фактуры с указанием количества, цены и других важных деталей в отношении токенизируемых товаров;
- документы, подтверждающие права собственности (права требования) в отношении токенизируемых товаров (например, договоры с поставщиками или производителями, свидетельства о регистрации прав и/или объектов);
- прочие документы, которые могут потребоваться в зависимости от характера и специфики конкретного товара, услуги или актива.

Lockton Finance резервирует за собой право затребовать любую дополнительную информацию и документы, чтобы в разумной мере убедиться в факте наличия товара, его безопасности и законности происхождения.

Помимо этого, при подаче заявки со стороны инициатора должен быть сформулирован Лист условий (Term Sheet), который описывает основные условия и параметры будущих отношений в отношении токенизируемых товаров / товарных партий.

Лист условий (Term Sheet) должен отражать:

- количественный и качественный состав товара / товарных партий;
- соответствующее количество и учетное стоимостное выражение товарных токенов (эквивалентное определенному количеству токенов платформы – LCN) и коррелирующие с этим товаром (товарными партиями);
- сроки и место перевода права собственности /права требования на товары / товарные партии;
- если применимо, условия фактической передачи товара / товарных партий приобретателю;
- прочие существенные условия сделки (сделок).

В итоге, подаваемая заявка со стороны инициатора должна содержать полную информацию о токенизируемом товаре/товарных партиях, характере отношений между инициатором сделки (правообладателем) и приобретателем (приобретателями).

Все это в последующем позволяет Lockton Finance и сторонам эффективно производить учет прав требования в отношении токенизированных товаров в соответствии с правилами платформы и нормами действующего законодательства Республики Узбекистан.

Выпуск товарного токена. После одобрения заявки Lockton Finance выпускает товарные токены на условиях и в объеме согласованными в заявке.

Для соблюдения необходимых нормативных требований регистрация товарного токена от Lockton Finance происходит единовременно в момент первичной инициации выпуска. Последующий выпуск товарных токенов происходит в соответствии с запросами пользователей.

Реализация товарного токена.

Реализация выпускаемых товарных токенов в рамках решения по структурированной токенизации на платформе Lockton Finance происходит только в формате закрытой продажи, где инициатором сделки (правообладателем) является только хозяйствующий субъект, при этом обе стороны являются зарегистрированными пользователями платформы.

Не допускается инициация сделки на товары, принадлежащие третьим лицам (а не правообладателю), а также приобретение товаров в отношении / в интересах третьих лиц (а не приобретателем).

После выпуска товарных токенов в рамках одобренной заявки, приобретатель может совершить сделку в отношении токенизируемых товаров.

В таком случае, при получении платформой Lockton Finance одобрения (акцепта) сделки от приобретателя (приобретателей), с его (их) счета (счетов)-LCH на платформе депонируется определенное эквивалентное количество токенов LCH в рамках условий данной заявки и/или Листа условий (Term Sheet) к ней. Одновременно Lockton Finance фиксирует передачу прав на товарные токены их приобретателю.

Депонированные активы приобретателя остаются в его собственности, однако платформа ограничивает распоряжение ими, до момента совершения либо прекращения сделки.

Завершение сделки.

Для завершения сделки требуется подтверждение факта передачи от правообладателя и получения приобретателем товара / товарной партии.

При получении такого извещения от приобретателя платформой Lockton Finance, товарные токены считаются использованными (исполненными) и происходит процесс их сжигания (burning) одновременно с этим происходит фиксация прав за продавцом на ранее депонированные LCH токены.

В случае, если фактически токенизированные товары были переданы во владение и распоряжение их приобретателю, однако приобретатель отказывается предоставлять извещение об их получении, либо имеются разногласия по сделке, то в таком случае Lockton Finance предлагает сторонам

выступить медиатором в их споре. В противном случае, сторонам рекомендуется обратиться в суд надлежащей юрисдикции. До разрешения спора, по существу, депонированные средства будут находиться в недоступном к распоряжению состоянии для приобретателя.

После завершения сделки, и высвобождении депонированных токенов, эти токены LCN могут быть использованы продавцом в рамках общих возможностей, предусмотренных платформой Lockton Finance.

В случае, если сделка с тонируемыми товарами не была осуществлена в полном объеме в рамках согласованных условий (по количеству, качеству, срокам и прочим существенным условиям), то доступ приобретателя к ранее депонированным активам восстанавливается в полном объеме.

Права и обязанности сторон

Инициатор сделки (правообладатель) имеет право на:

- безопасное и своевременное получение депонированных активов от приобретателя при завершении сделки;
- защиту конфиденциальных данных, предоставленных при токенизации товара;
- согласования условий сделки с приобретателем;
-

Инициатор сделки обязан:

- Предоставить полный и достоверный пакет документов на токенизируемый товар / товарные партии, в том числе дополнительно запрашиваемый со стороны платформы Lockton Finance;
- обеспечить безопасность и сохранность товара /товарной партии до момента передачи приобретателю;
- соблюдать установленные сроки и условия, оговоренные в Листе условий (Term Sheet)
- соблюдать действующее законодательство Республики Узбекистан, правила платформы Lockton Finance, а также международные нормы в отношении противодействия отмыванию преступных доходов и финансированию терроризма, содействия в обходе международных санкций.

Приобретатель имеет право на:

- получение достоверной и полной информации от правообладателя о токенизируемом товаре / товарной партии;

- своевременное получение товара в согласованном количестве, качестве и в рамках прочих согласованных условий, в полное распоряжение на свое собственное усмотрение, без каких-либо иных обременений;
- защиту конфиденциальности своих данных, предоставленных при токенизации товара;
-

Покупатель обязан:

- известить платформу Lockton Finance после получение товара / товарной партии для завершения сделки;
- своими действиями не вводить в заблуждение правообладателя и администрацию платформы относительно факта получения им товаров / товарных партий, а также относительно состояния / комплектности товара / товарной партии на момент получения;
- предоставить дополнительные документы и информацию по запросу платформы Lockton Finance;
- соблюдать конфиденциальность и защищать персональные данные, полученные в рамках сделки.
- соблюдать действующее законодательство Республики Узбекистан, правила платформы Lockton Finance, а также международные нормы в отношении противодействия отмыванию преступных доходов и финансированию терроризма, содействия в обходе международных санкций.

Ответственность Lockton Finance:

- **Отсутствие ответственности Lockton Finance за товар:** важно отметить, что Lockton Finance не несет ответственности перед приобретателем за получение товара, соблюдение сроков, соблюдения количества, качества, комплектности товара и иных существенных условий сделки. Эта обязанность полностью лежит на правообладателе (инициаторе сделки). Lockton Finance действует исключительно как провайдер, предоставляющей инфраструктуру учета совершения сделок с токенизируемыми товарами через соответствующее решение на платформе и не является стороной в отношениях между правообладателем и приобретателем, в частности в вопросах исполнения сторонами своих обязательств.

• **Выпуск товарного токена по заявке пользователя:** Lockton Finance как лицензированный провайдер в сфере оборота крипто-активов выступает эмитентом товарных токенов на платформе.

- **Фиксация факта сделки:** Lockton Finance фиксирует факт совершения сделки между правообладателем и приобретателем. Это включает в себя сохранение записей о каждой сделке и ее существенных условиях. После получения товара /товарной партии Lockton Finance осуществляет фиксацию прав на депонированные токены LCH за правообладателем в соответствии с согласованными условиями.

- **Обеспечение безопасности сделок:** Lockton Finance принимает меры для обеспечения безопасности и надежности сделок на платформе. Это включает в себя использование современных технологий и механизмов защиты данных для предотвращения мошенничества и несанкционированного доступа к информации.
- **Поддержка пользователей:** Lockton Finance обеспечивает поддержку пользователей платформы в случае возникновения вопросов или проблем, связанных с процессом токенизации товаров и осуществлением сделок. Пользователи могут обращаться в службу поддержки Lockton Finance для получения консультаций и решения проблем.
- **Соблюдение нормативных требований:** Lockton Finance строго соблюдает нормативные требования и стандарты безопасности, установленные в отрасли. Это включает в себя соблюдение законодательства о защите персональных данных; о предотвращении отмыывания преступных доходов и финансирования терроризма, обходе международных санкций, а также другие применимых требований со стороны действующего законодательства Республики Узбекистан.

2. РИСКИ, СВЯЗАННЫЕ С КРИПТОАКТИВАМИ

Работа в сфере оборота крипто-активов сопряжена с различными рисками, которые могут затронуть как крупных инвесторов, так и обычных пользователей. Основываясь на опыте и понимании рынка, можно выделить следующие основные аспекты:

В первую очередь, большая разновидность крипто активов подвержена волатильности. Стоимостные колебания могут зависеть от многих факторов: от мировых экономических новостей до решений регулирующих органов разных стран. Кроме того, технология блокчейн, хоть и предлагает высокую степень безопасности, не является непреступной, как и любая другая технология: возможны технические ошибки или уязвимости.

С другой стороны, любой сервис или платформа, включая Lockton, также имеют собственные риски. Это могут быть риски операционного характера, связанные с обслуживанием серверов, обновлениями программного обеспечения или человеческим фактором.

Мы делаем все возможное, чтобы их минимизировать, но абсолютная безопасность в цифровом мире — это постоянная работа.

В работе с крипто активами также необходимо учитывать риски, связанные с действиями третьих лиц. К ним относятся мошенничество, фишинг и хакерские атаки.

Особенное внимание следует уделять сохранности своих личных данных и ключей доступа.

Всегда стоит помнить: инвестирование в крипто активы – это решение, принимаемое на свой страх и риск, и каждый участник рынка должен осознавать возможные последствия своих действий.

Данная Декларация и другие документы платформы содержат достаточную информацию для понимания этих рисков, и возможность с ней ознакомиться, для формирования понимания и их адекватной оценки со стороны пользователей.

3. ПРИВЕРЖЕННОСТЬ НОРМАТИВНЫМ ТРЕБОВАНИЯМ И МЕЖДУНАРОДНЫМ СТАНДАРТАМ

Развитие в условиях постоянно изменяющихся нормативных требований представляет собой сложную задачу.

Команда юристов и консультантов Lockton Finance гарантирует, что все операции компании соответствуют нормативным требованиям региона.

Вместе с тем, важный аспект соблюдения локального законодательства, представляет собой только часть решения.

В современном взаимосвязанном мире, где цифровые активы легко перемещаются через границы, важно глобальное понимание задачи. Именно здесь проявляется актуальность соответствия **Lockton Finance** рекомендациям “Группы по финансовым мерам борьбы с отмыванием денег” (ФАТФ).

Доверие рынка формируется не только из принципа номинального соответствия локальным законодательным нормам, но и из стремления сделать так чтобы внутренние нормы компании соответствовали общемировым стандартам.

Для Lockton Finance соблюдение законодательства и приверженность регулятивным стандартам являются основой его этических принципов.

ФАТФ играет ключевую роль в разработке международных стандартов и рекомендаций в отношении криптовалют и криптографических активов. ФАТФ признается мировым авторитетом в области противодействия легализации доходов от преступной деятельности и финансированию терроризма. Группа активно работает над разработкой и распространением стандартов для регулирования крипто-валютных платежных систем и обмена крипто активами, с целью предотвращения и выявления финансовых преступлений, связанных с этими технологиями.

ФАТФ определяет принципы «Знай своего клиента» (KYC) и «Знай свой продукт» (KYP) для платформ и сервисов обмена крипто активами, а также налагает

обязанности в отношении мониторинга транзакций и предотвращения участия в незаконных операциях.

Соблюдение **Lockton Finance** рекомендаций ФАТФ свидетельствует о преданности принципам и ценностям противодействия отмыванию денег (ПОД), и указывает на ответственный подход в создании прозрачной и безопасной цифровой финансовой экосистемы.

Следуя стандартам ФАТФ, в частности в сфере регулирования виртуальных активов, **Lockton Finance** демонстрирует, что платформа защищена от незаконных финансовых операций, мошенничества и других вредоносных действий.

4. БОРЬБА С ФИНАНСОВЫМИ ПРЕСТУПЛЕНИЯМИ

Для платформы **Lockton Finance** первостепенной задачей является защита нашей платформы и ее пользователей от угроз финансовых преступлений.

Нами разработаны комплексные меры и стратегии, направленные на соблюдение международных стандартов и формирования атмосферы доверия среди наших пользователей.

На стадии регистрации каждого пользователя, наша комплаенс служба тщательно проверяет предоставленные им данные. Этот этап включает в себя детальный процесс проверки личности, в ходе которого требуется предоставление соответствующих документов и персональной информации. Кроме того, мы регулярно обновляем и сверяем информацию пользователей, чтобы наша база данных всегда была актуальной и достоверной.

В цифровой финансовой сфере особую важность приобретает точное понимание источников и движения активов. Основываясь на этом принципе, **Lockton Finance** активно применяет ончейн-аналитику для исследования оборота крипто активов.

С помощью передовых систем анализа и мониторинга, мы осуществляем тщательную проверку всех крипто активов, циркулирующих через нашу платформу. Исключая рискованные и сомнительные активы, мы страхуем своих пользователей от возможных потерь и стимулируем качественный рост нашего цифрового финансового пространства.

Прозрачность и безопасность — ключевые принципы нашей работы.

Особое внимание уделяется анализу операций и поведению пользователей на платформе. Это позволяет нам выявлять и предотвращать попытки отмывания денег. Любой пользователь, уличенный в подобных незаконных действиях, может быть заблокирован, а также подвергнут правовым последствиям.

На протяжении всего времени работы **Lockton Finance** мы активно сотрудничаем с регуляторными органами, поддерживая открытый диалог и гарантируя соответствие последним законодательным требованиям. При возникновении любых вопросов или расследований со стороны регуляторов, мы предоставляем всю необходимую информацию и оказываем активное содействие.

В нашей системе предусмотрена программа сбора уведомлений о случаях подозрительной активности. Если пользователь или сотрудник делится информацией о необычной активности, мы сохраняем его конфиденциальность.

Мы гарантируем анонимность информатора и принимаем решительные меры на основе полученной информации для обеспечения безопасности платформы и ее пользователей.

Заключая, хочется подчеркнуть, что благодаря внедрению этих строгих мер против финансовых преступлений, **Lockton Finance** подтверждает свою приверженность предоставлению безопасной, прозрачной и надежной платформы для своей базы пользователей.

5. ТЕХНОЛОГИЯ РАСПРЕДЕЛЕННОГО РЕЕСТРА И ИНФОРМАЦИЯ О ПЛАТФОРМЕ

Крипто депозитарий Lockton Finance — это гибридная блокчейн-платформа, выполняющая ряд финансовых функций. Цель платформы - внедрить сервисную инфраструктуру, которая предоставит необходимые инструменты для работы с крипто активами в соответствии со всеми требованиями современного правового поля и призвана соединить сектор крипто активов с финансовым. Это позволяет выпускать, приобретать и хранить активы с высоким уровнем конфиденциальности, безопасности и возможностью аудита, следуя регулированию юрисдикции.

Ключевой особенностью предлагаемого решения является регистрация всех операций платформы в собственном блокчейне системы.

Базовые возможности платформы:

- Хранение цифровых активов с возможностью выбора типа доступа – аппаратный либо программный.
- Поддержка наиболее актуальных видов активов.
- Возможность выбора варианта администрирования системы: использование мультиподписи, пороговых подписей и других инструментов для диверсификации ответственности.
- Возможность выбора метода резервного копирования (например, создание общего секрета, шифрование ключей от кошельков с его

помощью и разделение между любым количеством администраторов с разными весами).

- Возможность подключения любого провайдера идентификации (при наличии открытого API у провайдера) и услуг AML.
- Возможность создавать роли, устанавливать лимиты и проверку потока транзакций в зависимости от роли.
- Возможность создавать разные пулы с активами для создания производных финансовых инструментов.
- Возможность предоставлять ликвидность протоколам DeFi с возможностью возвращения дивидендов потребителям.
- Возможность интеграции платежных шлюзов и услуг (с возможностью внесения/вывода фиатной валюты, а также обмена ее на крипто или цифровой актив).
- Возможность получения криптовалютных займов.
- Возможность обмена между фиатом и криптоактивами.
- Возможность выпуска карт с привязкой к криптоактивам.
- API для интеграции с существующими сервисами и другими услугами.

Давайте рассмотрим основные архитектурные принципы крипто депозитария Lockton Finance:

Гибкость: Гибкость заключается в разделении процессов в учете: управление идентичностью, управление аккаунтами, передача и обмен активов, управление ролями, управление жизненным циклом токенов и внесение/снятие средств. Все эти процессы выполняются независимыми модулями и могут быть настроены через регулируемые шаблонные смарт-контракты, которые поддерживает платформа. Сочетание этих подходов позволяет легко интегрироваться с существующими унаследованными системами.

Безопасность: Секретные данные пользователя никогда не передаются на сервер. Система позволяет взаимодействие, при котором пользователи никогда не передают свои секретные данные (например, пароль) серверу. Это означает, что компрометация этих данных во время сетевой передачи, а также через взлом ключевого сервера, исключена. Следовательно, владелец платформы больше не несет ответственности за риски, связанные с хранением секретных данных пользователя, а также нет необходимости расходовать ресурсы на обеспечение дополнительной безопасности связанной с передачей секретных данных доступа. Состояние балансов пользователей полностью зависит от выполненных транзакций. Поскольку все транзакции иницируются самими пользователями с помощью криптографических ключей, злоумышленник не сможет изменить блокчейн записи, даже имея полный доступ к одному из серверов, ее хранящих.

Аудитоспособность: Возможно проводить аудит системы в реальном времени независимой стороной 24/7. В частности, аудитору может быть предоставлен узел с блокчейном, синхронизированным в реальном времени, и автоматически (с использованием специализированного программного обеспечения) проверить правильность текущих процессов.

Адаптивность: Система поддерживает адаптивное управление разрешениями, которое относится как к пользователям, так и к администраторам. Уровни доступа могут быть полностью настроены для каждой учетной записи в соответствии с факторами, которые регулирует администрация платформы (например, страна, возраст, доход и т. д.). Это позволяет адаптировать бизнес-логику системы в соответствии с законодательством конкретной юрисдикции.

Целевая аудитория: Существует мнение, что люди, мало понимающие в крипто активах, но желающие их приобрести, в первую очередь обратятся к лицензированному институциональному оператору. Целевая аудитория включает в себя розничных пользователей, инвесторов, корпоративных клиентов, ИТО, фонды, биржи, а также традиционные банки и финансовые организации, стремящиеся расширить свою функциональность в направлении работы с крипто активами.

Функциональность: Lockton Finance предоставляет ряд функций, включая выпуск и первичное размещение крипто активов, депозитные программы, многоуровневое хранение, крипто валютные займы, токенизация активов и автоматизированные модули крипто/фиат ввода/вывода с настраиваемыми лимитами.

Особенности и преимущества Lockton Finance соответствуют стандартам традиционных финансовых институтов, предлагая многоуровневый доступ к активам, фрагментированное хранение, высокую степень гибкости и репутацию институционального учреждения, способствующую быстрому выходу на рынок и безопасную, универсальную рыночную нишу.

3.1 Архитектура

Lockton Finance это платформа, характеризующейся высокой модульностью системы, используя архитектуру микросервисов. Платформа крипто депозитария делится на два основных компонента: логику, основанную на DLT, (Node), обрабатывающий ключевые функции, такие как управление токенами и распределение, управление правами и т. д., и вспомогательные модули, связывающие DLT с внешними системами и хранением данных пользователя.

3.1.1 Node

Node, ключевой компонент платформы, обрабатывает транзакции, управляет историей и предлагает доступный API для взаимодействия с данными блокчейна. Он состоит из двух модулей:

Core — это реплицируемый автомат состояний, который поддерживает локальную копию криптографического реестра и обрабатывает транзакции на его основе по согласованию с набором одноранговых узлов. Он реализует протокол федеративного консенсуса и отвечает за учет токенов и управление ролями.

Клиентский сервер REST API. Он действует как интерфейс между ядром и приложениями, которым требуется доступ к сети. Он позволяет отправлять транзакции в сеть, проверять состояние счетов и просматривать историю транзакций.

3.1.2 Вспомогательные модули

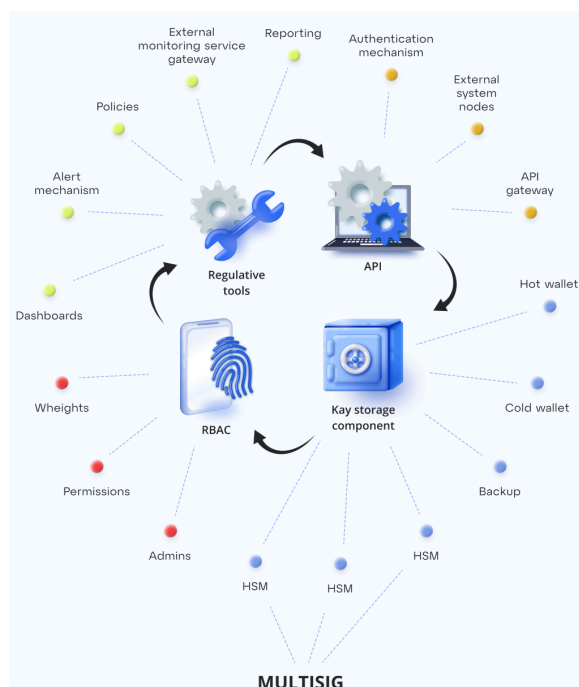
Эти модули связывают блокчейн с приложениями внешнего мира, каждый отвечает за различные процессы, такие как внешние интеграции, платежные системы, биржи, проверку личности и т. д.

3.1.3 Модуль интеграции сервисов

Этот набор модулей служит мостом между публичными блокчейнами, банками, платежными шлюзами и биржами, отражая операции, такие как депозиты, снятие средств и колебания курсов в других системах. Он включает в себя системы CRM, ERP, SCM; KYC; уведомления о событиях; отслеживание взаимодействий и т. д.

Другие модули, связывающиеся с узлами через API:

- Модуль мониторинга – это инструмент реализации мониторинга всей системы в реальном времени.
- Модуль отчетов — это инструмент, который позволяет создавать отчеты на основе информации, собранной с помощью другого модуля.
- Файловый модуль хранения данных.
- Модуль сервера ключей — это инструмент, который позволяет генерировать новые пары ключей для пользователей и хранить их.



Управление ключами

4.1 Пары ключей и учетные записи

Все учетные записи идентифицируются открытым ключом и, по сути, представляют собой часть данных, хранящихся в реестре. Все остальные данные в реестре, такие как активы, предложения или данные KYC, связаны с учетными записями.

Вес ключа определяет его уровень доступа для инициирования конкретной операции. Вес необходим для определения порога выполнения операции.

4.2 Разрешения

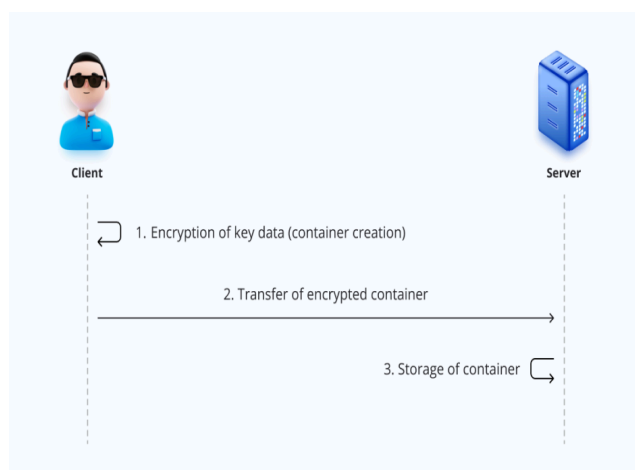
Для совершения операций у всех учетных записей существует набор разрешений. Разрешения настраиваются администраторами и могут быть настроены для каждой отдельной учетной записи (это также относится к администраторам, которые должны иметь соответствующие разрешения для настройки разрешений других учетных записей). Как и любая другая система, Lockton Finance требует от пользователей регистрации и авторизации. Однако решающее различие заключается в следующих аспектах:

- Пароль никогда не покидает устройство пользователя. Злоумышленнику нет смысла прослушивать общение пользователя с сервером (никакие конфиденциальные данные никогда не передаются).
- Сервер не хранит конфиденциальные/чувствительные данные пользователя. Конфиденциальные данные пользователей больше не находятся под угрозой утечки. Нет аутентификации по паролю, однако

порядок действий пользователя остается прежним: введите пароль.

- Компрометация базы данных бессмысленна. Информация, передаваемая и хранящаяся на сервере, не представляет ценности для злоумышленника, поскольку она зашифрована ключами, известными только пользователю.
- Ключи хранятся на сервере, но доступ имеет только пользователь. Сервер является всего лишь хранителем зашифрованных ключей, расшифровать которые может только пользователь.

Хранение данных ключей на удаленном сервере позволяет пользователю удобно получить доступ к своим ключам в любое время и с любого устройства, имеющего соответствующее программное обеспечение. Важно, что данные ключей хранятся в зашифрованном виде, а шифрование должно осуществляться непосредственно пользователем. Также в случае атаки данные ключа не будут скомпрометированы, если используется секрет, известный только пользователю.



Протокол предусматривает генерацию ключа шифрования из секрета пользователя. Для этого система использует функцию односторонней генерации ключей, которая принимает на вход набор параметров.

Таким образом, только стороны, обладающие секретом, могут расшифровать контейнер и получить доступ к данным ключей.

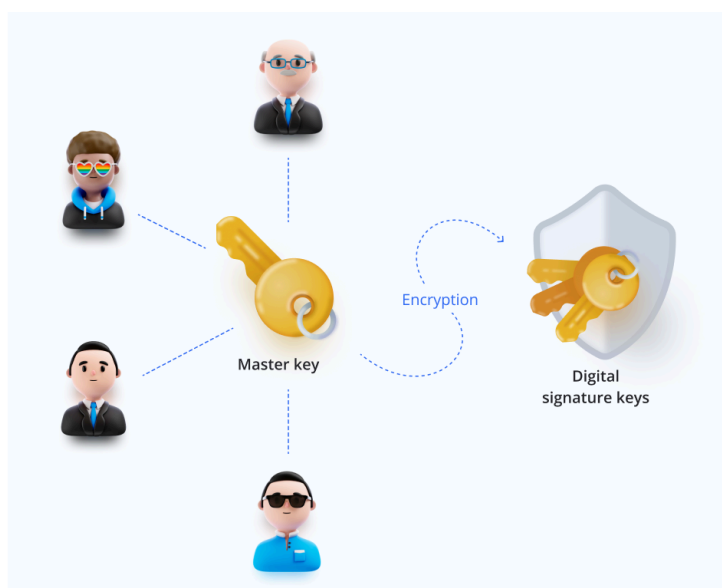
После успешной аутентификации сервер отправляет зашифрованный кошелек пользователю, пользователь расшифровывает его, используя свой ключ шифрования (сгенерированный путем ввода пароля локально на устройстве) и получает доступ к своим ключам. Авторизация завершена, и пользователь готов использовать свои ключи для подписи дальнейших операций, которые он хотел бы выполнить в системе.

4.3 Резервное копирование

Меры безопасности могут включать резервное копирование ключей, например, следующим образом:

Формируется новый секрет, с помощью которого шифруются ключи мультиподписи.

Секрет распределяется между 3 разными участниками по схеме распределения ключей Ади-Шамира (администраторы и владелец) с необходимым порогом 2 из 3. Зашифрованные ключи хранятся в нескольких хранилищах.



В этом случае, если один из администраторов потеряет закрытый ключ, владелец системы может сгенерировать общий секрет (с частью секрета, предоставленного другим администратором) и расшифровать с его помощью необходимый ключ. После этого можно сгенерировать мультиподпись и разблокировать средства.

4.4 Безопасность

Криптокастодиальные сервисы имеют дело с критической необходимостью безопасного хранения ключей и восстановления доступа. Данные сервисы сохраняют полный контроль над криптографическими ключами и управляют механизмами взаимодействия с клиентами. Инициирование транзакции требует запроса клиента, который обрабатывает служба, а крипто депозитарий подписывает окончательную транзакцию. Крипто депозитарий выступает в качестве безопасного хранилища для значительных средств, используя многоэтапные процедуры доступа. Несмотря на то, что клиенты передают

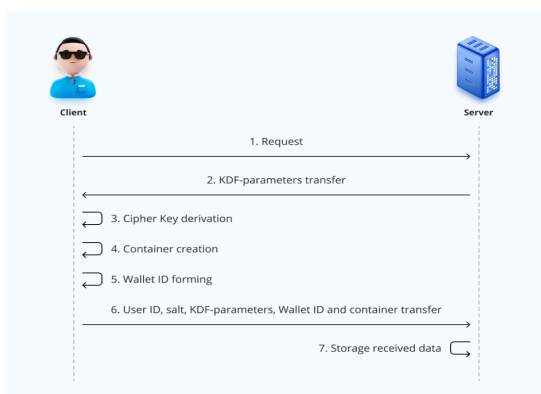
прямой контроль над активами, этот подход оказывается эффективным по ряду причин:

- Высокая безопасность ключей. Служба крипто депозитария непосредственно специализируется на обеспечении безопасности хранимых ключей. Наша служба использует HSM и механизм мультиподписи, чтобы минимизировать риски взлома и сбоев. Дополнительные механизмы резервного копирования исключают риски в случае отказа сервера в обслуживании и т.п.
- Простой механизм восстановления доступа пользователей. Потеря паролей (или чего-то еще в зависимости от того, какой механизм аутентификации используется) не влияет на потерю доступа сервиса к ключам.
- Возможность регулирования на всех этапах работы и простота подключения средств мониторинга. Поскольку каждая транзакция должна быть подписана кастодианом на основании запроса, полученного от учетной системы, на любом этапе подтверждения запроса (в случае возникновения подозрений) она может быть остановлена и обработана вручную ответственным администратором.

Регистрация и авторизация пользователя и администратора

5.1 Регистрация пользователя

Пользователи проходят процесс регистрации, аналогичный традиционным онлайн-платформам. Они предоставляют телефонный сотовый номер, электронную почту, пароль и подтверждают регистрацию. Несмотря на то, что пользователя просят проделать довольно простую работу, техническая часть процесса довольно сложна.



Регистрация объекта происходит следующим образом:

- Объект отправляет запрос на регистрацию на сервер. Сервер отправляет объекту kdf-параметры.

- Объект генерирует значение соли и ключ шифрования контейнера.
- Объект шифрует ключевые данные (т.е. создает контейнер) Объект формирует значение Wallet ID
- Объект отправляет на сервер зашифрованный контейнер и следующие значения: идентификатор пользователя, соль, параметры kdf, идентификатор кошелька.
- Сервер сохраняет полученные данные. Пользователь зарегистрирован.

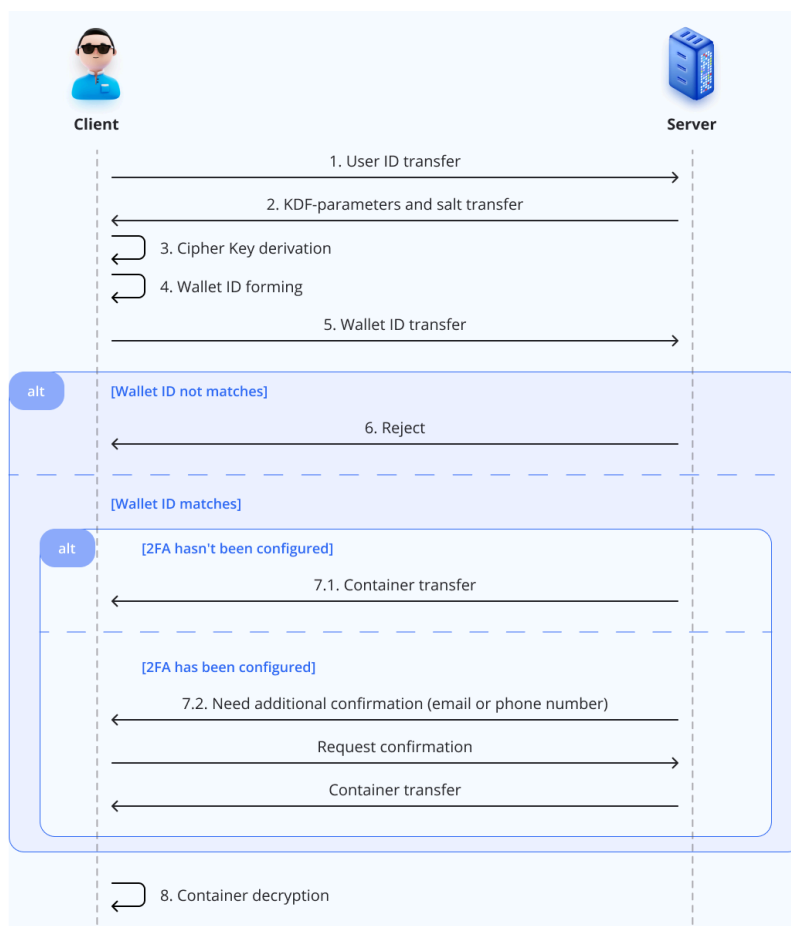
Пользователь проходит регистрацию и аутентификацию, при этом должна быть обеспечена конфиденциальность и целостность передаваемых на сервер данных. Значение идентификатора кошелька генерируется на основе значения ключа шифрования контейнера. Для генерации значения идентификатора кошелька используется криптографическая хеш-функция.

При регистрации секрет пользователя обрабатывается только на его устройстве и никогда не сохраняется на сервере и поэтому не может быть украден при передаче по сети (потому что он не передается по сети) или в результате атаки на сервер. Исходя из приведенных выше данных, надежность доступа к аккаунту пользователя – полная ответственность пользователя.

5.2 Авторизация

Как уже было сказано, пароли пользователей никогда не затрагивают серверы ни во время авторизации, ни когда-либо еще.

Этот протокол обеспечивает метод аутентификации объекта с последующей авторизацией. В этом случае сервер аутентификации снимает с себя ответственность за безопасное хранение и обработку паролей пользователей. Нарушение безопасности сервера хранения ключей не ставит под угрозу ключи и пароли пользователей.



Вместе с тем, настоятельно рекомендуется использовать безопасный канал для передачи всех данных от клиента на сервер и обратно. Также рекомендуется обеспечить целостность передаваемых сообщений (например, использование MAC в случае установления безопасного канала (общий секрет и симметричное шифрование) между клиентом и сервером).

5.3 Изменение/восстановление пароля

Безопасность пароля имеет первостепенное значение, поскольку он необходим для генерации ключа шифрования. Если пользователи теряют или забывают свой пароль, они теряют доступ к ключу.

Поскольку сервер не знает пароль пользователя, процедура восстановления пароля происходит с помощью повторной процедуры KYC, после прохождения которой пароль будет восстановлен. Это означает, что старые ключи удаляются (вместе с их весом и разрешениями), генерируется новый ключ, для нового ключа устанавливаются разрешения и вес, и вновь созданный кошелек шифруется с использованием нового пользовательского пароля.

Управление учетными записями

Учетная запись является основной единицей на платформе управления активами. Каждая операция в учетной системе связана с учетной записью, которая ее инициировала. Каждый пользователь в системе обладает парой ключей: публичным ключом, который действует как идентификатор учетной записи, и приватным ключом, который дает доступ к выполнению операций в системе. Каждая учетная запись связана с конкретной ролью, которую она может выполнять в учетной системе.

Все операции, связанные с учетной записью — создание, обновление, удаление — также инициируются транзакциями и подписываются пользователем с соответствующими разрешениями.

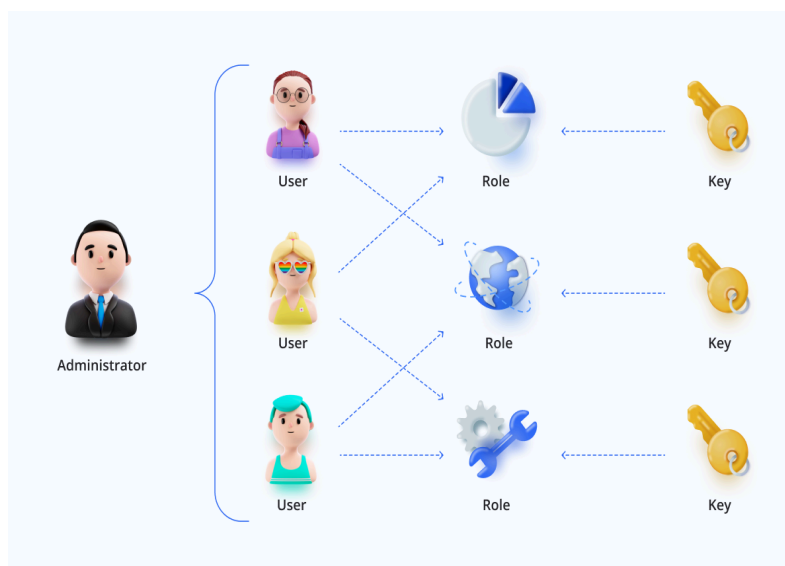
Роль на платформе управления активами представлена набором доступных операций. Максимальное количество ролей на платформе может быть равно общему числу возможных операций, причем каждая роль в системе имеет свой собственный ID.

При создании учетной записи администратор указывает роль, которую соответствующая учетная запись может выполнять. Поскольку у большинства пользователей в системе похожие разрешения (например, обычный пользователь имеет разрешения только на передачу и обмен активов), подход на основе ролей более эффективен и менее затратен, чем ручная настройка разрешений для каждой отдельной учетной записи (хотя эта функция также имеется).

Управление ролями

6.1 RBAC - Role-Based Access Control

В нашем подходе мы используем модель RBAC для получения доступа к системным услугам: для каждой созданной в системе роли определяется набор разрешений, лимитов и т. д. Каждому участнику платформы присваивается одна из существующих ролей (после регистрации и прохождения процедуры идентификации), после чего для конкретной целевой учетной записи назначаются все специфические политики.

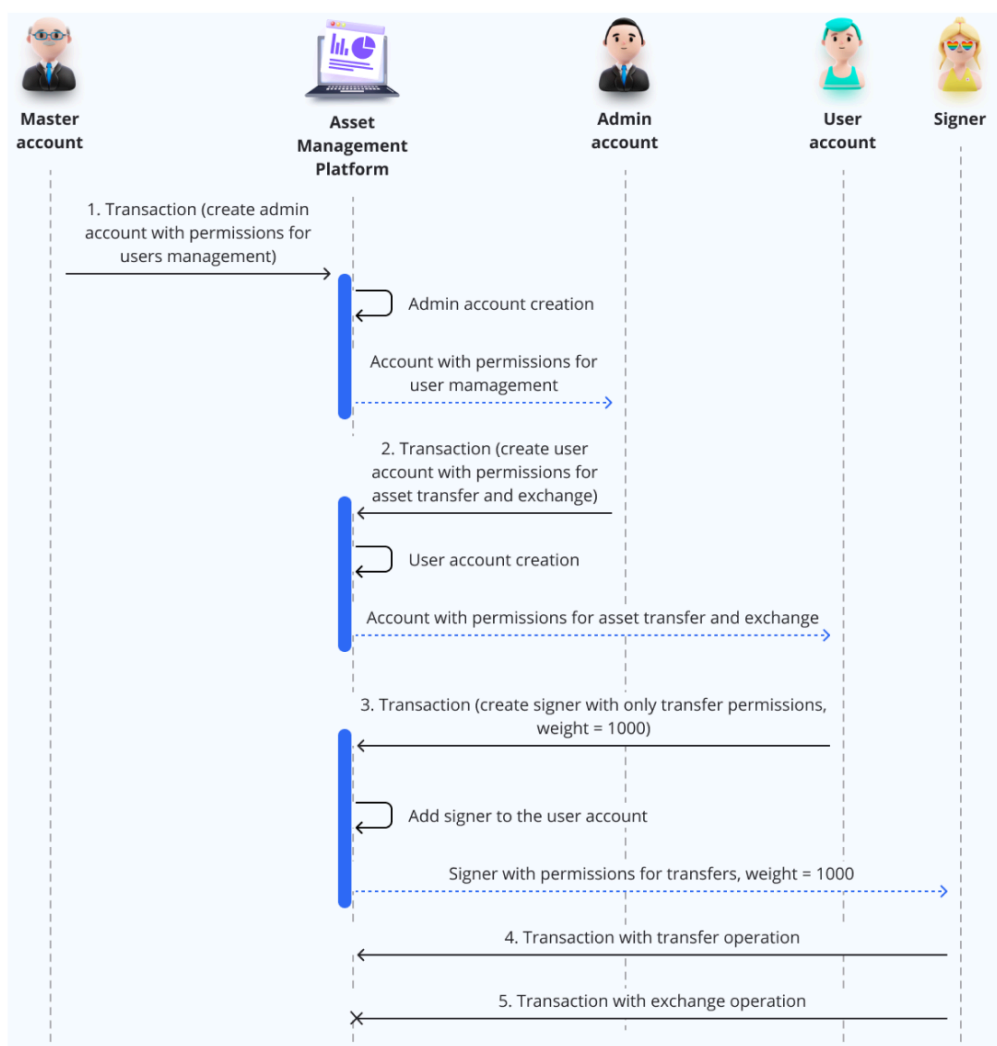


6.2 Типы учетных записей

Все учетные записи можно разделить на два типа: администраторы и пользователи. Администраторы принимают решения по настройке системы и установке бизнес-правил, а также проверяют пользователей и предоставляют им права (разрешения) на выполнение определенных действий на платформе. Пользователи используют функциональные возможности системы, выполняя операции, на которые у них есть разрешение.

6.3 Процесс распределения разрешений на платформе

На платформе управления активами изначально существует только одна учетная запись, главная учетная запись, которая имеет разрешения на выполнение всех административных операций на платформе. Начальное распределение ролей в системе подразумевает распределение ролей системных администраторов; их разрешения могут отличаться, но, тем не менее, должны охватывать все административные операции в системе.



6.4 Администраторы

На платформе Lockton Finance, можно настроить количество администраторов, набор доступных каждому администратору разрешений и вес, который у каждого администратора есть при предоставлении разрешенной операции (мультиподпись). Каждому администратору выдается ключ, который позволяет выполнять только строго определенный набор операций (например, утверждение/отклонение запросов KYC пользователей из определенного региона + установка комиссий).

6.5 Учетные записи

Учетные записи являются центральной структурой данных на платформе. Каждая учетная запись имеет криптографические ключи (с их весом), разрешения, представляющие, какие операции могут быть выполнены, и каждая учетная запись связана с определенной ролью, которую она может выполнять в учетной системе.

Управление токенами

7.1 Жизненный цикл токена

Жизненный цикл токена состоит из следующих этапов: Создание, Предварительный выпуск, Выпуск, Передача, Хранение, Погашение.

7.1.1 Создание

На этом этапе токен не может быть продан или передан, потому что он фактически не существует. Это просто объявление о деталях токена: название, максимальное количество выпуска, разрешения, необходимые для взаимодействия с этим токеном.

7.1.2 Предварительный выпуск

После этапа предварительного выпуска фактические токены существуют, но ими никто еще не владеет — они все заблокированы на смарт-контракте. Предварительный выпуск происходит либо автоматически, либо вручную, с использованием офлайн-приложения, что повышает безопасность во время предварительного выпуска токенов и обеспечивает диверсификацию рисков.

7.1.3 Выпуск

На этом этапе токены выпускаются в оборот, что может быть выполнено либо путем прямого выпуска, либо через краудинвестинг.

7.1.4 Передача

Платформа поддерживает передачу токенов пользователям либо напрямую либо путем размещения на площадку первичных предложений.

7.1.5 Торговля

Платформа поддерживает внутренний модуль размещения, позволяющий эмитентам реализовывать выпущенные на платформе токены без необходимости интеграции с внешними обменными сервисами.

7.1.6 Погашение

Погашение токенов — это процесс вывода соответствующего количества токенов из обращения.

Транзакции и операции

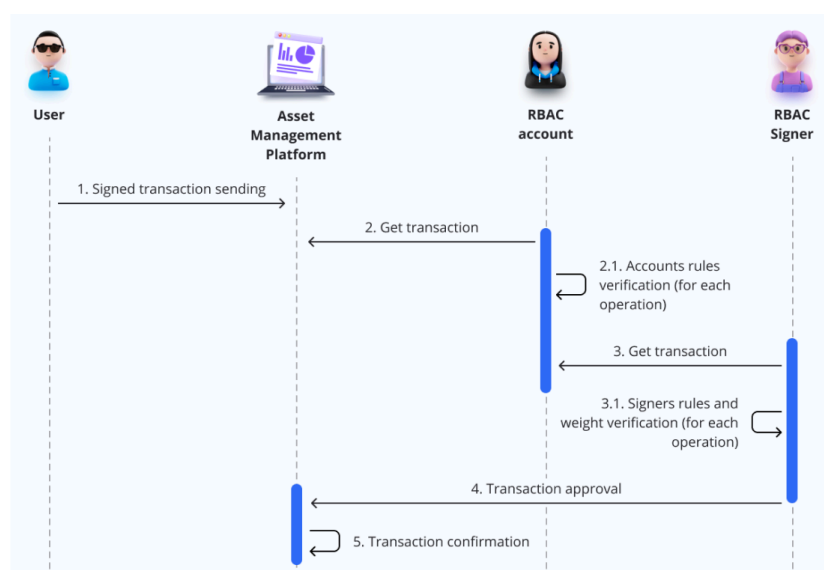
8.1 Механизм проверки транзакций

При публикации транзакции в сети система должна проверить все операции, содержащиеся в транзакции. Для проверки используются два вспомогательных модуля: модуль RBAC Account и модуль RBAC Signer.

Весь процесс проверки транзакций можно описать с помощью диаграммы последовательности, включающей создание транзакции пользователем, проверку модулем RBAC Account, дальнейшую проверку модулем RBAC Signer и окончательную проверку транзакции, ведущую к изменениям в состоянии реестра.

Транзакция, содержащая операцию платежа:

Ниже представлена диаграмма последовательности, иллюстрирующая процесс проверки операции платежа с участием двух учетных записей: отправителя и получателя.



Для успешного выполнения транзакции должны быть выполнены следующие условия:

- Учетная запись отправителя должна иметь правило, разрешающее передачу конкретного актива.
- Подписант учетной записи отправителя должен иметь правило, разрешающее передачу конкретного актива.
- Учетная запись получателя должна иметь правило, позволяющее ей принимать передачи соответствующего актива.
- Пользователь инициирует транзакцию с операцией платежа, передавая актив на баланс учетной записи получателя. Модуль RBAC Account принимает и проверяет транзакцию, убеждаясь, что учетные записи отправителя и получателя имеют необходимые разрешения.
- Если проверки RBAC Account положительны, RBAC Signer принимает на себя управление, подтверждая, что подписант учетной записи отправителя имеет полномочия и достаточный общий вес подписантов для транзакции.

После успешной проверки транзакция подтверждается, и состояние реестра обновляется соответственно.

8.3 Интеграция с необходимыми платежными решениями и шлюзами

Платформа управления активами приоритизирует функции депозитов и снятия средств, что требует модуля интеграции с внешними системами. Этот модуль выступает посредником между платформой и внешними финансовыми системами, обеспечивая удобство пользователей за счет различных способов платежа для внесения и снятия средств.

Минимальные требования:

Интеграция с платежными системами, такими как кредитные карты (UzCard/Humo/Mastercard/Visa) и электронные платежные системы, также необходимо обеспечить пополнение кошелька через банковские переводы.

В случаях транзакций с цифровой валютой или крипто активами модуль интеграции отслеживает внешние учетные системы, иницируя выпуск или погашение токенов на основе полученных данных.

Безопасность и соответствие стандартам:

Платформа обеспечивает защиту данных пользователей, с передачей конфиденциальной информации напрямую от пользователя к сервису. Уникальные идентификаторы предотвращают повторную обработку одного и того же запроса на депозит. Подтверждение выпуска поступает от PSIM или администратора платформы, аутентифицированного с помощью цифровых подписей.

Во время вывода средств погашение токенов происходит после получения средств на внешний счет. Если платежный сервис отклоняет транзакцию, токены разблокируются для повторной попытки снятия.

8.4 Мониторинг, Защита и Управление Комиссиями

Платформа интегрируется с внешними службами соблюдения нормативных требований, проверяя каждую транзакцию на предмет происхождения средств или получателя. Она использует протоколы защиты высокого уровня, такие как многофакторная аутентификация и криптографическая подпись для всех транзакций.

Инструменты управления комиссиями позволяют создавать индивидуальные правила наложения комиссий с параметрами для счетов, активов и типов операций. Комиссии могут быть представлены в фиксированном и (или) в процентном виде комиссий в зависимости от предполагаемых сценариев.

Протокол консенсуса:

9.1 Byzantine Fault Tolerance

«Проблема византийских генералов» была задумана в 1982 году как логическая дилемма, иллюстрирующая, как группа византийских генералов может иметь проблемы со связью при попытке договориться о своем следующем шаге.

Дилемма предполагает, что у каждого генерала есть своя армия и что каждая группа расположена в разных частях города, который они собираются атаковать. Генералам необходимо договориться о наступлении или отступлении. Неважно, нападут они или отступят, главное чтобы все генералы достигли консенсуса, то есть договорились об общем решении и согласовали его исполнение.

Таким образом, мы можем рассмотреть следующие требования: каждому генералу предстоит решить: атаковать или отступить (да или нет). После того, как решение принято, его нельзя изменить. Все генералы должны принять одно и то же решение и выполнить его синхронно.

Вышеупомянутые проблемы связи связаны с тем, что один генерал может общаться с другим только посредством сообщений, которые пересылает курьер. Следовательно, главная дилемма «Проблемы византийских генералов» заключается в том, что сообщения могут быть каким-то образом задержаны, уничтожены или потеряны.

Кроме того, даже если сообщение успешно доставлено, один или несколько генералов могут решить (по какой-либо причине) действовать злонамеренно и отправить мошенническое сообщение, чтобы сбить с толку других генералов, что может привести к полному провалу.

Если мы применим эту дилемму к контексту блокчейна, то каждый генерал представляет собой узел сети, и узлы должны достичь консенсуса относительно текущего состояния системы. Другими словами, большинство участников распределенной сети должны согласовать и выполнить одно и то же действие, чтобы избежать полного провала.

Следовательно, единственный способ достичь консенсуса в таких типах распределенных систем — это иметь как минимум $2/3$ или более надежных и честных сетевых узлов. Это означает, что если большая часть сети решит действовать злонамеренно, система будет подвержена сбоям и атакам (например, атаке 51%).

Византийская отказоустойчивость (BFT) — это свойство системы, которая способна противостоять классу сбоев, полученному из проблемы византийских генералов. Это означает, что система BFT может продолжать работу, даже если некоторые узлы выходят из строя или действуют злонамеренно.

Платформа Lockton Finance использует разновидность BFT консенсуса:

FBA (Federated Byzantine Agreement) — это система консенсуса, которая

обеспечивает безопасность и согласованность данных в децентрализованной сети путем формирования кворумов. В отличие от традиционных систем консенсуса, FBA позволяет узлам самостоятельно выбирать другие узлы, которым они доверяют, для создания перекрывающихся групп, называемых кворум-срезами.

Эти срезы обеспечивают гибкость и безопасность сети, позволяя достичь согласия даже при наличии злонамеренных узлов. FBA консенсус обеспечивает высокую производительность и масштабируемость.

10.1 Внесение фиатных средств

Провайдер эмиссии токена (платформа) должен иметь учетную запись во внешней системе. Эта учетная запись будет использоваться для привязки токенов, которые позже будут выпущены на платформе.

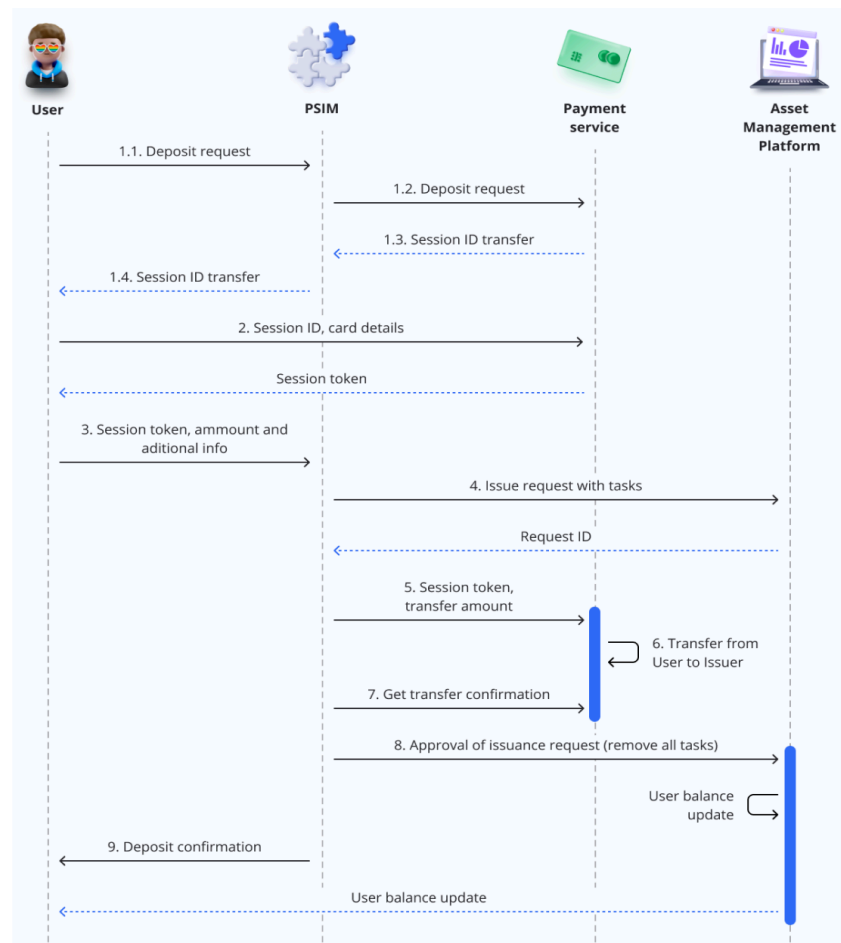
На платформе должен быть создан соответствующий токен и настроены соответствующие ограничения токена.

Должна быть создана учетная запись администратора (или группа учетных записей администратора) с правами на выпуск токена и подтверждена выдача соответствующего токена.

Процесс внесения фиатных средств выглядит следующим образом:

- Пользователь получает идентификатор сеанса
- Пользователь отправляет запрос на депозит в PSIM. В запросе указывается желаемый депозитный актив.
- PSIM проверяет возможность внесения заявленного актива и отправляет запрос на депозит в Платёжный сервис (внешнюю систему).
- Платежный сервис генерирует уникальный идентификатор сеанса и отправляет его в PSIM.
- PSIM передает полученный идентификатор Пользователю.
- Пользователь связывается с Платежным сервисом, отправляет ему идентификатор сеанса, полученный ранее, и сообщает данные, относящиеся к его учетной записи во внешней системе (номер карты, счет и т. д.).
- Платежный сервис обрабатывает данные карты и отправляет Пользователю новый уникальный идентификатор — токен сеанса, который связан с данными внешней учетной записи пользователя.
- Пользователь отправляет полученный токен сеанса, количество токенов и другие сведения, связанные с их получением, в PSIM.
- PSIM отправляет запрос на выпуск токенов на платформу управления активами. Запрос содержит набор задач, которые необходимо обработать перед фактической выдачей и сумму. AMP получает запрос, генерирует уникальный идентификатор запроса и возвращает его в PSIM.
- PSIM отправляет информацию о сумме перевода и токене сеанса (который привязан к учетной записи пользователя во внешней системе) в Платежный сервис.

- Платежный сервис обрабатывает запрос и осуществляет перевод со счета пользователя на внешний счет эмитента (платформы) токена.
- PSIM получает подтверждение перевода от Платежного сервиса.
- PSIM подтверждает запрос на выпуск на платформе управления активами. Баланс пользователя на платформе обновляется в соответствии с реквизитами подтвержденного запроса.
- PSIM сообщает Пользователю, что депозит подтвержден. Чтобы убедиться в этом, пользователь может войти на платформу и получить информацию о своем балансе.



10.2 Внесение цифровых активов

Ввод и вывод цифровых валют и крипто активов также осуществляется с помощью PSIM. Однако в этом случае стоит разделить этот модуль на четыре компонента:

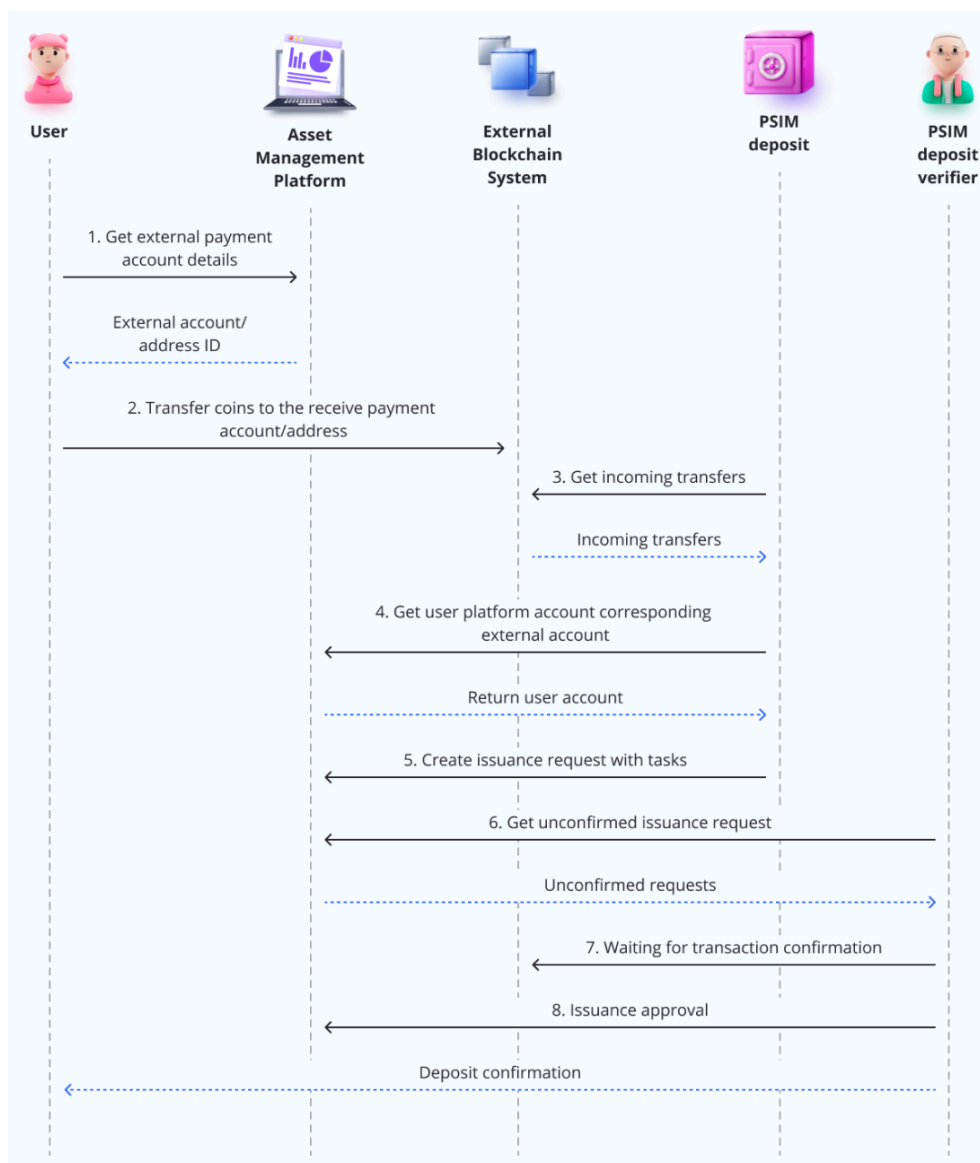
Депозит PSIM, Верификатор депозита PSIM, Вывод PSIM, Верификатор вывода PSIM.

Для размещения цифровых валют и крипто активов на платформе должен быть обеспечен набор следующих требований:

- Системный администратор предварительно создал соответствующий актив. Актив имеет достаточную доступную для выпуска сумму.
- Системному администратору необходимо создать пул идентификаторов учетных записей внешней системы в конфигурации ядра платформы управления активами.
- Разрешения учетной записи пользователя должны разрешать получение необходимого актива. Пользователь запрашивает новый адрес для привязки к его учетной записи.

Процесс размещения выглядит следующим образом:

- Пользователь отправляет запрос на Платформу управления активами для получения платежного счета/адреса во внешней системе.
- Пользователь переводит необходимое количество активов на полученный аккаунт/адрес.
- PSIM Deposit отслеживает входящие переводы и счета/адреса их отправителей.
- PSIM Deposit запрашивает Платформу управления активами для получения учетной записи пользователя с внешней учетной записью, с которой был сделан депозит.
- После получения данных учетной записи пользователя PSIM Deposit создает запрос на выпуск и отправляет его в ядро платформы управления активами.
- PSIM Deposit Verifier отслеживает неподтвержденные запросы на выпуск на платформе.
- После получения запроса PSIM Deposit Verifier отслеживает внешнюю сеть и ожидает необходимого количества подтверждений транзакции.
- При достижении необходимого количества подтверждений PSIM Deposit Verifier подтверждает выдачу токенов на баланс пользователя, и пользователь получает информацию об успешном пополнении депозита.



12.1 Вывод фиатных средств

Для осуществления вывода необходимо обеспечить комплекс следующих требований:

- Пользователь должен иметь учетную запись во внешней системе. Этот счет будет использоваться для вывода средств.
- Соответствующий токен должен быть доступен для вывода.

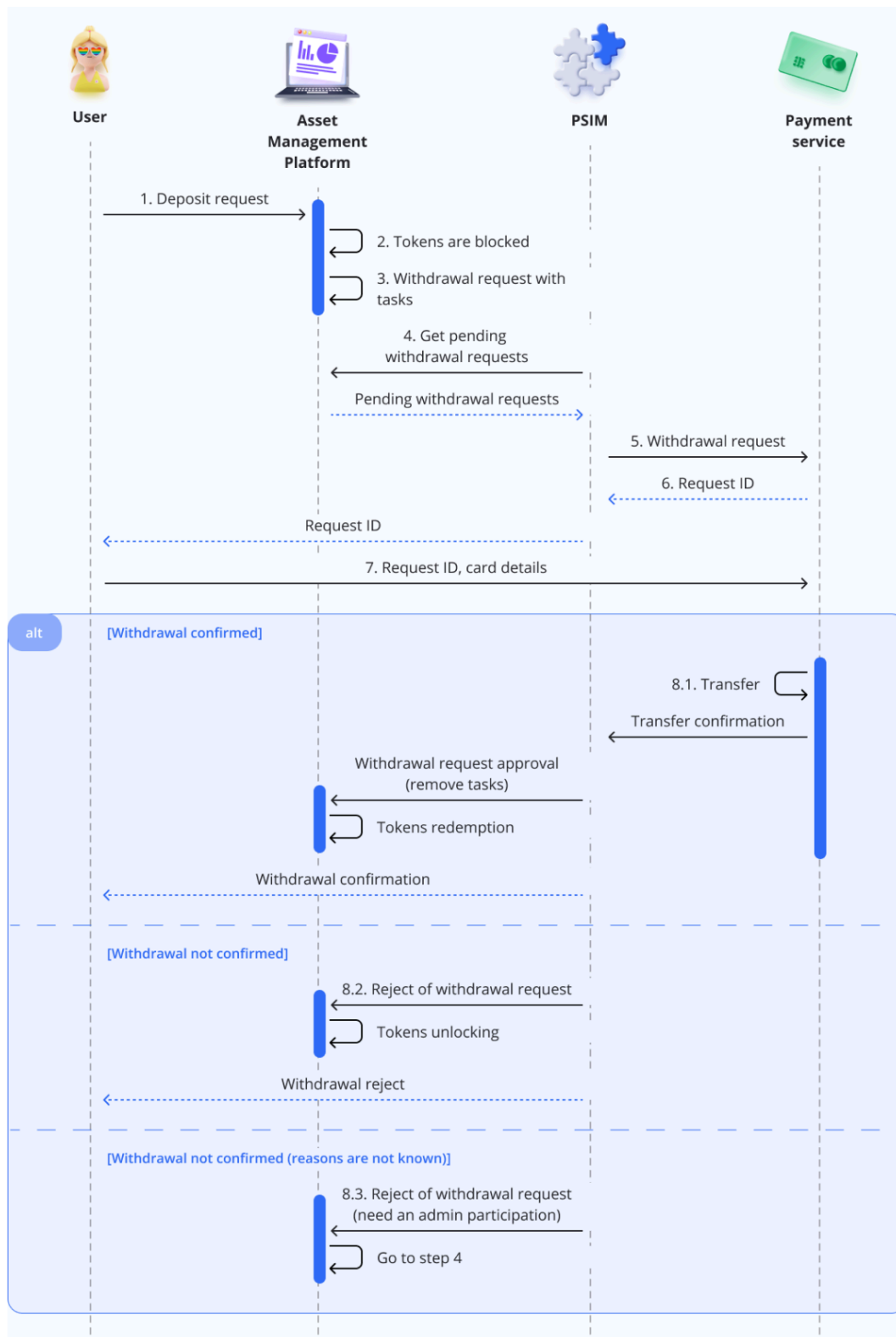
Процесс вывода выглядит следующим образом:

- Пользователь отправляет запрос на вывод средств на Платформу управления активами. Запрос должен содержать информацию об аккаунте пользователя, сумме для вывода, активе для вывода и т. д.
- Соответствующее количество токенов заблокировано на платформе управления активами.

- АМР создает запрос на вывод средств, который может содержать определенные задачи, которые должны выполнить администраторы платформы.
- PSIM отслеживает подобные события на платформе и получает информацию о необработанных запросах.
- PSIM отправляет в Платёжный сервис информацию о запросе на вывод средств (сумма перевода, счёт эмитента).
- Платежная система генерирует уникальное значение идентификатора запроса и передает его в PSIM. PSIM передает полученное значение Пользователю.
- Пользователь отправляет в Платёжный сервис идентификатор запроса и данные о своём счёте (номер карты, реквизиты и т.п.).

Платежная система обрабатывает запрос. В этом случае возможны три сценария:

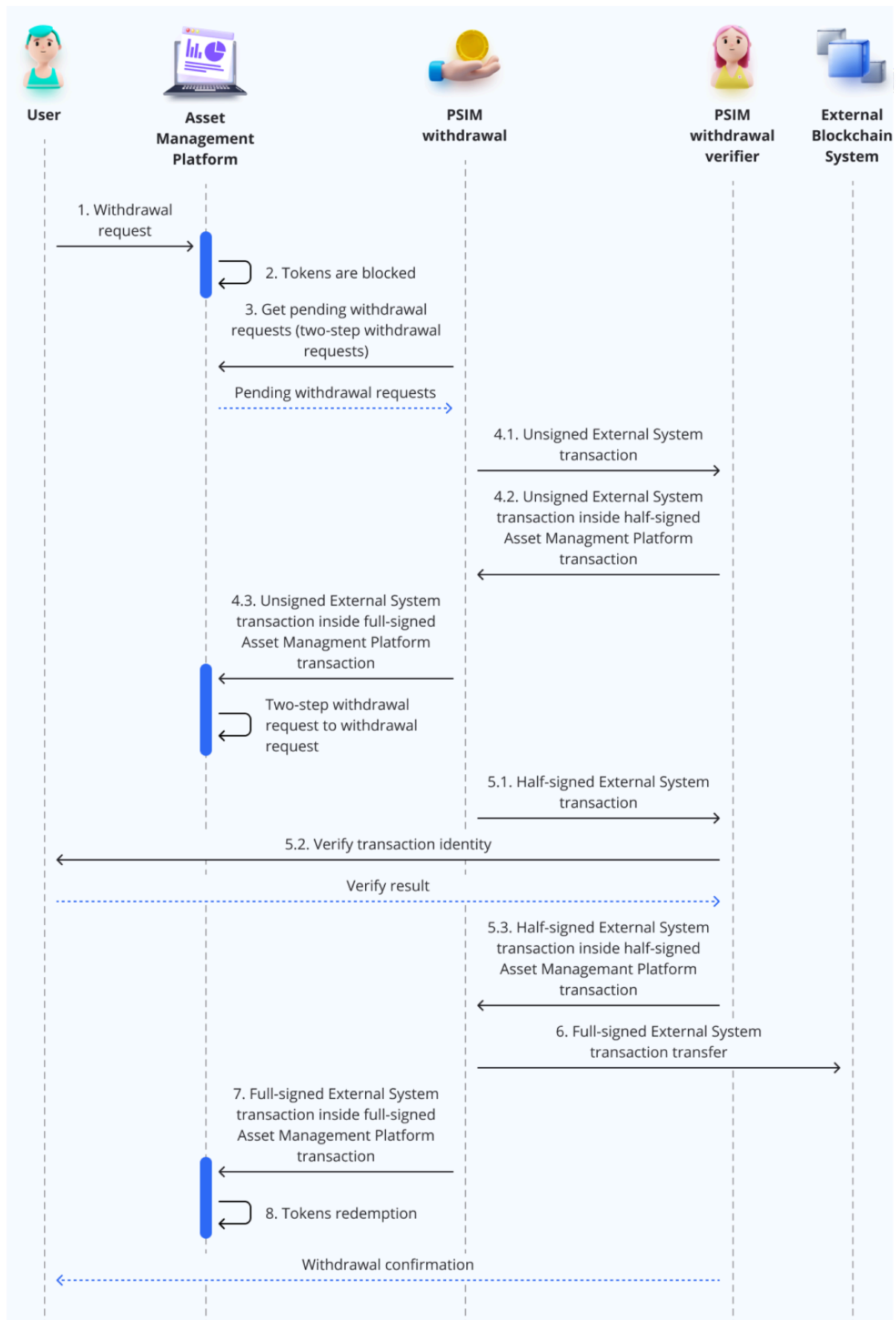
- Вывод подтвержден. Если Платежный сервис подтверждает вывод, он перечисляет необходимые средства клиенту и отправляет подтверждение вывода в PSIM, который, в свою очередь, подтверждает вывод на платформе; в результате токены, заблокированные на балансе пользователя, погашаются.
- Вывод не подтвержден по известным причинам. Если Платежный сервис отказывается подтвердить запрос (например, технически неспособен по каким-либо причинам или пользователь указал неверные данные), то PSIM обращается к системе с просьбой выполнить операцию отклонения вывода. В результате токены, которые были заблокированы на балансе пользователя, снова доступны пользователю.
- Вывод не подтвержден, а причины неизвестны. Если запрос на вывод средств не был подтвержден платежным сервисом и PSIM не получил никаких подробностей о причине отклонения, то PSIM требует от уполномоченного администратора принять решение относительно следующих действий.



12.2 Вывод цифровых валют и криптоактивов

Процесс вывода выглядит следующим образом:

- Пользователь отправляет запрос на Платформу управления активами. Запрос на вывод содержит идентификатор баланса, с которого следует вывести средства, сумму для вывода, актив для вывода и т.д.
- Соответствующее количество токенов блокируется на балансе пользователя.
- PSIM Withdrawal замечает ожидающий запрос на вывод средств и начинает его обработку. Обратите внимание, что для подтверждения запроса необходимо выполнить две итерации (при этом мультиподпись используется как для отправки транзакций Asset Management Platform, так и для внешней системы).
- Функция вывода средств PSIM отправляет неподписанную транзакцию внешней системы компоненту средства проверки вывода средств PSIM.
- Верификатор вывода средств PSIM получает транзакцию внешней системы и помещает ее в транзакцию AMP. Затем он подписывает транзакцию AMP и отправляет ее обратно в PSIM Withdrawal. Напомним еще раз: чтобы транзакция AMP была гарантирована, она должна быть подписана вторым ключом.
- PSIM Withdrawal получает полуподписанную транзакцию AMP, проверяет ее и подписывает своим ключом. После этого он отправляет на платформу подписанную транзакцию AMP (с неподписанной транзакцией внешней системы внутри). После этого первая итерация завершается (двухэтапный запрос на вывод средств меняется на запрос на вывод средств).
- Вывод средств PSIM подписывает транзакцию внешней системы и отправляет ее верификатору вывода средств PSIM.
- Средство проверки вывода средств PSIM получает полуподписанную транзакцию внешней системы и отправляет на платформу запрос на проверку идентичности полученной транзакции с той, которая была помещена в первую транзакцию AMP.
- Если транзакция совпадает, верификатор вывода средств PSIM подписывает ее своим ключом и помещает в новую транзакцию AMP. Он также подписывает эту транзакцию AMP и отправляет ее на вывод средств PSIM.
- PSIM Withdrawal получает полуподписанную транзакцию AMP с полностью подписанной транзакцией внешней системы. После этого он отправляет транзакцию внешней системы во внешнюю сеть для подтверждения.
- PSIM Withdrawal подписывает транзакцию AMP (делая ее полностью подписанной) и передает ее на платформу, тем самым завершая процесс вывода.
- Платформа управления активами получает подписанную транзакцию и выкупает заблокированные токены.



Модуль идентификации (КУС):

13.1 Служба идентификации — это модуль, соответствующий требованиям GDPR, который хранит данные, собранные в ходе процедуры КУС (знай своего клиента). Чтобы получить доступ к данным, пользователю или администратору необходимо предоставить цифровую подпись, которая сверяется с самым последним состоянием реестра. Такой подход обеспечивает высокий уровень безопасности. Этот модуль также хранит закрытые ключи пользователей, зашифрованные на стороне клиента.

Это не позволяет злоумышленнику получить доступ к учетным записям системы, даже имея полный доступ к хранилищу.

Крипто депозитарий предполагает наличие отдельного модуля, отвечающего за хранение данных КУС (знай своего клиента), и он называется Identity Storage.

Тот кто имеет разрешение на работу с Identity Storage, указывается через ключи, предоставляемые системным администраторам — для подтверждения своего разрешения администратор предоставляет соответствующую подпись.

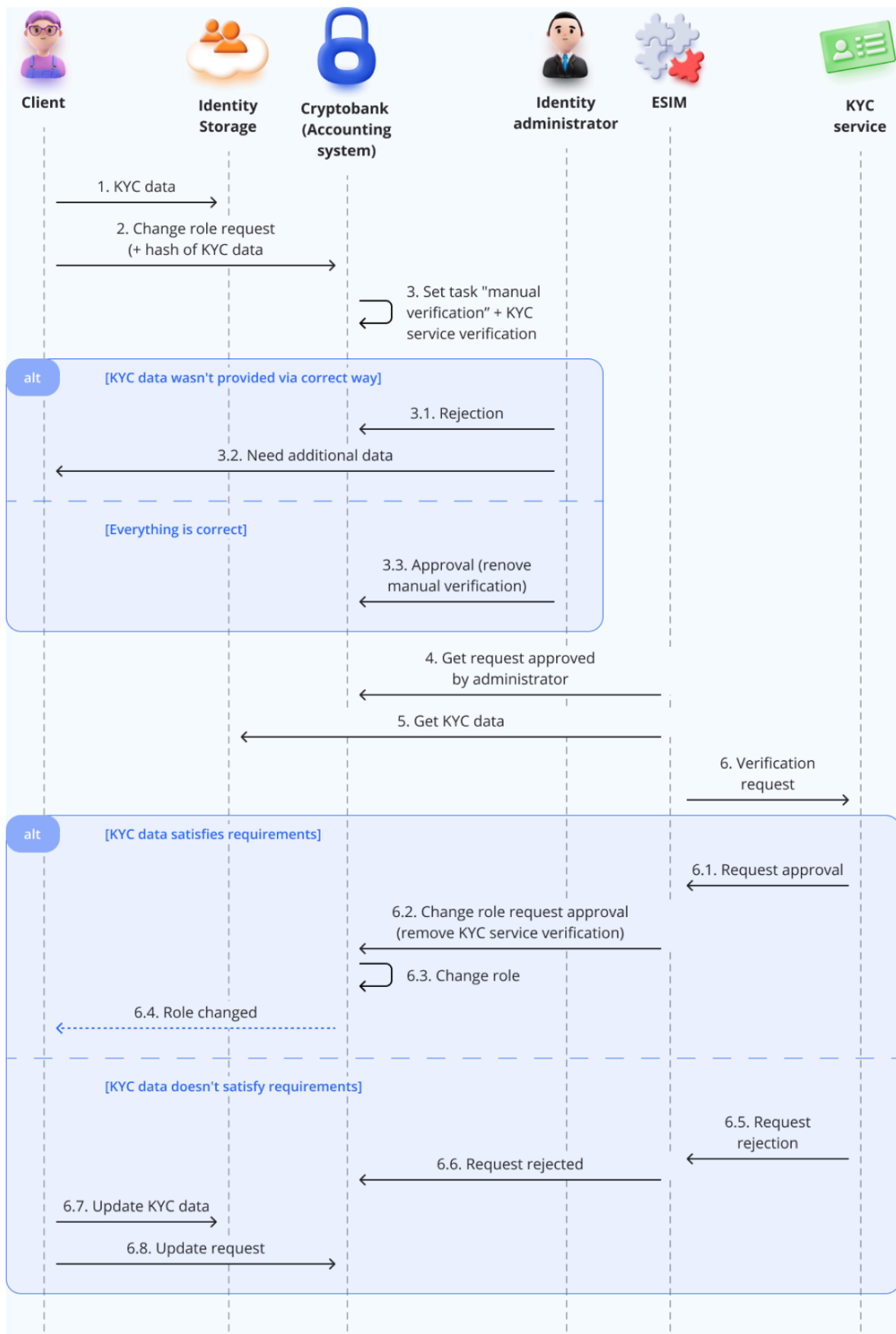
Для интеграции системы учета с внешними комплаенс-решениями необходимо использовать «мостовой» модуль.

Идентификация КУС начинается с отправки пользовательских данных в хранилище.

На следующем этапе учетной системе предлагается изменить роль пользователя.

При поступлении в учетную систему запроса, статус запроса на ручную проверку данных администратором (для проверки полноты полученных данных) изменяется. Если данные неполные, пользователю отправляется сообщение с просьбой предоставить правильные данные. Когда все данные полностью заполнены, администратор проверяет их правильность. Затем модуль ESIM получает подтверждение о полноте данных и отправляет их в службу идентификации.

Если данные некорректны (плохое качество, не те данные), пользователю отправляется сообщение о том, что необходимо отправить правильные данные, процесс идентификации перезапускается. Если пользователь подтвержден, служба аутентификации отправляет ответ модулю ESIM, который, в свою очередь, отправляет ответ в учетную систему. Система учета изменяет роль пользователей. Идентификация завершена.



6. СВЕДЕНИЯ О РАЗРАБОТЧИКЕ:

- Название: Distributed Lab
- Общее описание бэкграунда
 - Distributed Lab — это украинская IT-компания, которая специализируется на создании решений в области блокчейн-технологий. Основанная в 2014 году, компания фокусируется на разработке финансовых технологий, используя блокчейн как основу для создания прозрачных, безопасных и эффективных систем.

Основные направления деятельности Distributed Lab включают:

- Блокчейн-платформы: Компания разрабатывает индивидуальные блокчейн-решения, предназначенные для удовлетворения специфических потребностей бизнеса. Это включает создание частных блокчейнов, интегрированных с существующими корпоративными системами.
 - Консалтинг: Distributed Lab предоставляет консультационные услуги в области блокчейн-технологий, помогая компаниям понять потенциал этой технологии и как она может быть интегрирована в их текущие операции.
 - Образовательные программы: Компания ставит перед собой задачу образования и распространения знаний о блокчейн-технологии и криптовалютах. Они проводят обучающие курсы, семинары и мастер-классы для различных групп специалистов.
 - Исследования и разработки: Distributed Lab участвует в исследовательских проектах, связанных с передовыми разработками в сфере блокчейна и финтеха. Они стремятся быть на переднем крае инноваций в этой области.
 - Команда Distributed Lab состоит из специалистов с глубокими знаниями в области криптографии, теории игр, децентрализованных протоколов, а также имеет опыт работы с классическими финансовыми системами.
- Ключевые члены команды
 - Pavel Kravchenko
Co-Founder, CEO
pavel@distributedlab.com
 - Oleksandr Kurbatov
Crypto Research Lead
alex@distributedlab.com
 - Volodymyr Dubinin

Co-Founder, COO
volodymyr@distributedlab.com

- Yaroslav Panasenko
Chief Technical Officer
yp@distributedlab.com
- Реализованные проекты (которые можно показать)
 - <https://github.com/distributed-lab>

7. ИНФОРМАЦИЯ ОБ ЭМИТЕНТЕ

ООО Lockton Hub, свидетельство о государственной регистрации №2180726 от 29.05.2023 г.

ИНН: 310 516 640

Адрес: г.Ташкент, Шайхонтохурский р-н, улица Фурката, дом 3а

Директор: Шипилов Д.

Лицензия НАПП: # CD 00001

- **Шипилов Денис Борисович.**
<https://www.linkedin.com/in/denis-shipilov-05ab1821b>
- info@lockton.uz ; +998772572277