Техническое описание аппаратно-программного комплекса (АПК) криптокастодиального сервиса

Содержание

1. Введение

1.1. Цели и задачи документа

Целью данного документа является предоставление обзора технических аспектов Крипто Кастодиального сервиса (далее Сервиса). Он направлен на описание архитектуры, функций и взаимодействия компонентов данного Сервиса, а также на обеспечение понимания его роли в системе управления криптоактивами.

1.2. Общее представление о Сервисе и его роли в системе

Сервис представляет собой программный комплекс, разработанный для безопасного хранения, управления и передачи криптоактивов. Его роль в системе заключается в обеспечении надежной платформы для управления криптоактивами, минимизации рисков утечки приватных ключей и обеспечении соблюдения требований безопасности и регулирования. Сервис играет ключевую роль в обеспечении безопасности и надежности операций с криптоактивами и может использоваться как внутри компании, так и в качестве коммерческого предложения на рынке финансовых учреждений, криптовалютных бирж, а также для корпоративных и частных пользователей.

2. Описание бизнес-логики

2.1. Основные функции и возможности Сервиса

- Обеспечение безопасности и конфиденциальности приватных ключей.
- Исключение риска вмешательства третьей стороны благодаря многоуровневой системе контроля.
- Прием, хранение и передача криптоактивов.
- Регистрация и верификация пользователей.
- Создание мультиподписных кошельков.
- Управление криптовалютными кошельками.
- Обслуживание кошельков.
- Мониторинг и отчетность по операциям с криптоактивами.
- Интеграция с внешними сервисами и платформами.
- Ведение реестра держателей криптоактивов.

2.2. Бизнес-процессы, обеспечиваемые Сервисом

- Процесс регистрации и верификации пользователей.
- Процесс создания и управления криптовалютными кошельками.
- Процесс выполнения транзакций с криптоактивами.
- Процесс мониторинга и анализа операций с криптоактивами.
- Процесс обеспечения безопасности и конфиденциальности данных.
- Процесс выпуска и передачи токена, разделенного мультиподписью.
- Процесс ведения реестра эмитентов и держателей криптоактивов.
- Процесс предоставления отчетности.

2.3. Интеграция с другими компонентами системы или внешними системами

2.3.1. Интеграция со сканерами блокчейн

Интеграция со сканерами блокчейн представляет собой важный компонент функционирования Сервиса. Этот процесс обеспечивает непрерывное отслеживание и контроль за транзакциями, происходящими в сети блокчейн, и является неотъемлемой частью обеспечения безопасности и прозрачности операций с криптоактивами.

В рамках интеграции со сканерами блокчейн Сервис устанавливает постоянное взаимодействие с различными узлами сети блокчейн, включая узлы Bitcoin, Ethereum, Tron и другими популярными блокчейна, в случае их подключения в Сервис. Это позволяет Сервису оперативно отслеживать поступление новых транзакций, подтверждать проведение платежей и обеспечивать прозрачность в движении криптоактивов.

Основной функцией интеграции со сканерами блокчейн является мониторинг и анализ транзакций с целью выявления и предотвращения мошеннических действий. С помощью

специализированных алгоритмов и аналитических инструментов Сервис может в будущем осуществлять поиск аномалий в транзакционных данных, таких как подозрительные перемещения крупных сумм, связанные с известными адресами мошенников или принятие платежей с адресов, имеющих негативную репутацию.

Благодаря интеграции со сканерами блокчейн Сервис имеет возможность оперативно реагировать на потенциальные угрозы и предпринимать необходимые меры для защиты активов клиентов. Это включает в себя блокировку подозрительных транзакций, уведомление клиентов о возможных рисках и сотрудничество с правоохранительными органами в рамках расследования инцидентов.

Таким образом, интеграция со сканерами блокчейн является неотъемлемой частью функционирования Сервиса, обеспечивая высокий уровень безопасности и прозрачности операций с криптоактивами.

2.3.2. Интеграция с криптовалютными биржами

Интеграция с криптовалютными биржами представляет собой ключевой аспект деятельности Сервиса, направленный на обеспечение оперативного доступа к актуальной информации о курсах токенов и криптоактивов. Это обеспечивает пользователям Сервиса возможность проводить операции с активами по актуальным ценам, минимизируя риски валютных колебаний и обеспечивая эффективное управление своими инвестициями.

Интеграция с криптовалютными биржами осуществляется путем установления соединения с API (интерфейсом программирования приложений) различных биржевых платформ. Сервис может существлять мониторинг текущих котировок и объемов торгов по различным торговым парам, обеспечивая оперативную реакцию на изменения рыночной ситуации. Это позволит предоставлять пользователям актуальную информацию для принятия инвестиционных решений. В случае предоставления дополнительных услуг, помимо безопасного хранения, Сервис будет также оказывать данную функциональность.

Одной из основных функций интеграции с криптовалютными биржами является автоматический обмен USDT на нативную монету блокчейна[1]. Сервис использует данные, полученные с биржевых площадок, для определения оптимальных курсов обмена и предоставляет пользователю возможность проводить транзакции с оплатой комиссии блокчейна путём обмена USDT на нативную валюту. Это обеспечивает мгновенную конвертацию USDT и выполнение операций с максимальной эффективностью, без необходимости иметь на кошельке нативную монету блокчейна для проведения транзакций.

Кроме того, интеграция с криптовалютными биржами может позволить Сервису предоставлять дополнительные услуги, такие как аналитические отчеты о рыночной

[1] На текущий момент реализован обмен USDT TRC-20 на TRX, однако в планах расширить функциональность для поддержки дополнительных обменов.

ситуации, информацию о ликвидности и объемах торгов по различным токенам, а также предупреждения о важных событиях на рынке.
Таким образом, интеграция с криптовалютными биржами играет ключевую роль в обеспечении пользователей сервиса актуальной информацией о рыночной ситуации и обеспечении возможности проведения операций с криптоактивами по оптимальным условиям.

2.3.3. Интеграция с Sumsub

Интеграция с Sumsub представляет собой важный компонент Сервиса, направленный на обеспечение процесса верификации пользователей и организаций.

Sumsub – это сервис, специализирующийся на проверке личности и бизнеса, который предоставляет инструменты для KYC (знай своего клиента) и KYB (знай своего бизнес-партнера). Интеграция с Sumsub позволяет Сервису проводить процедуры верификации с высокой степенью достоверности и обеспечивать соблюдение требований регулирующих органов по борьбе с отмыванием денег и финансированием терроризма.

Процесс интеграции с Sumsub начинается с передачи необходимых данных о пользователе или организации Сервисом. Эти данные включают в себя информацию о личности (имя, фамилия, адрес и т. д.), а также документы, подтверждающие личность (паспорт, водительские права и т. д.). Sumsub затем проводит проверку предоставленных данных с использованием своих алгоритмов и баз данных, а также проводит биометрическую верификацию, если это необходимо.

После завершения процедуры верификации Sumsub предоставляет сервису отчет о результатах проверки, включающий степень соответствия предоставленных данных требованиям KYC/KYB, а также результаты биометрической верификации. Эта информация используется Сервисом для принятия решения о допуске пользователя к использованию Сервиса.

Интеграция с Sumsub обеспечивает высокий уровень безопасности и достоверности процесса верификации, что позволяет Сервису соблюдать требования регулирующих органов и предотвращать незаконную деятельность. Это также повышает уровень доверия пользователей к Сервису и обеспечивает защиту от мошенничества.

2.3.4. Интеграция с Scorechain

Интеграция с Scorechain представляет собой важный компонент Сервиса, направленный на обеспечение безопасности и прозрачности операций с криптоактивами.

Scorechain – это сервис, специализирующийся на анализе транзакций в блокчейне и оценке рисков, связанных с криптоактивами.

Процесс интеграции с Scorechain начинается с передачи данных о транзакциях, проводимых через Сервис, на анализ. Эти данные включают в себя информацию о сумме транзакции, адресе отправителя и получателя, времени проведения операции и другие сведения, необходимые для анализа.

Scorechain осуществляет анализ предоставленных данных с использованием своих алгоритмов и баз данных. В ходе анализа проводится оценка риска, связанного с каждой транзакцией, а также определяется степень чистоты криптоактивов, участвующих в операции.

После завершения анализа Scorechain предоставляет Сервису отчет о результатах анализа, включающий оценку риска каждой транзакции и рекомендации по дальнейшим действиям. Эта информация используется Сервисом для принятия решений о допуске транзакций к исполнению или блокировке в случае выявления рисков.

Интеграция с Scorechain обеспечивает высокий уровень безопасности и прозрачности операций с криптоактивами, что позволяет Сервису эффективно выявлять и предотвращать операции, связанные с незаконной деятельностью или высокими рисками. Это также помогает соблюдать требования по борьбе с финансовыми преступлениями и обеспечивать безопасность пользователей и их активов.

2.3.5. Интеграция с внешними регуляторами

Интеграция с внешними регуляторами является важным аспектом деятельности Сервиса, поскольку обеспечивает соответствие его операций законодательству и нормативным требованиям, устанавливаемым регулирующими органами. Взаимодействие с внешними регуляторами обеспечивает прозрачность и ответственность перед регуляторами, а также обеспечивает защиту интересов пользователей и соблюдение высоких стандартов безопасности.

Процесс интеграции начинается с передачи необходимой информации о клиентах и их операциях из Сервиса в системы, используемые внешними регуляторами для мониторинга и контроля за деятельностью финансовых учреждений и предотвращения финансовых преступлений. Эта информация включает в себя данные о клиентах, их активности, проведенных операциях, а также сведения, необходимые для проведения проверок KYC (знай своего клиента) и AML (предотвращение отмывания денег).

Системы регуляторов анализируют предоставленные данные и проводят соответствующие проверки, чтобы убедиться в соблюдении Сервисом всех требований законодательства и нормативных актов. После завершения проверки регуляторы предоставляют обратную связь о результатах проверки и, при необходимости, выносят рекомендации или требования по исправлению выявленных нарушений или недочетов.

Интеграция с внешними регуляторами обеспечивает прозрачность и законность деятельности Сервиса, а также обеспечивает доверие со стороны клиентов и партнеров. Это

позволяет Сервису эффективно выполнять свои функции и обеспечивать высокий уровень защиты и безопасности операций с криптоактивами.

2.3.6. Интеграция с сервером авторизации, использующим Group IB Fraud Protection

Интеграция с сервером авторизации, использующим Group IB Fraud Protection, представляет собой важное звено в системе безопасности и защиты Сервиса.

Group IB Fraud Protection — это инновационное решение, разработанное для предотвращения мошенничества и обеспечения безопасности финансовых операций.

Процесс интеграции начинается с передачи необходимых данных о клиентах и их активности из Сервиса в систему Group IB Fraud Protection. Эти данные включают в себя информацию о пользователях, их транзакциях, истории активности, а также другие параметры, которые могут быть использованы для анализа и выявления потенциальных мошеннических схем.

Система Group IB Fraud Protection проводит комплексный анализ предоставленных данных с использованием передовых методов машинного обучения, аналитики данных и искусственного интеллекта. Она выявляет аномальные или подозрительные паттерны поведения, а также производит проверку на соответствие нормативным требованиям и стандартам безопасности.

После анализа система Group IB Fraud Protection генерирует отчеты и рекомендации о возможных мошеннических действиях или нарушениях безопасности. Эти данные передаются обратно в Сервис для принятия соответствующих мер по предотвращению и реагированию на потенциальные угрозы.

Интеграция с сервером авторизации, использующим Group IB Fraud Protection, обеспечивает высокий уровень защиты от мошенничества и обеспечивает безопасность операций с криптоактивами для пользователей Сервиса. Это позволяет эффективно предотвращать финансовые потери, защищать личные данные клиентов и обеспечивать надежность и доверие к работе Сервиса.

3. Требования к Сервису

3.1. Функциональные требования

3.1.1. Обеспечение безопасности и конфиденциальности приватных ключей

3.1.1.1. Генерация, хранение и защита приватных ключей от несанкционированного доступа.

Сервис обеспечивает безопасную генерацию, хранение и защиту приватных ключей, необходимых для доступа к криптоактивам пользователей. Для этого используются следующие меры:

1. ***Генерация ключей***
   Приватные ключи создаются с использованием криптографических алгоритмов высокой стойкости, что обеспечивает их уникальность и надежность.
2. ***Хранение ключей***
   Приватные ключи хранятся в защищенном хранилище данных, на который доступ имеют только авторизованные пользователи с необходимыми привилегиями. Для обеспечения максимальной защиты данных, применяются все возможные способы безопасности, включая механизмы шифрования, хеширования и прочие технологии
3. ***Защита от несанкционированного доступа***
   Для предотвращения несанкционированного доступа к приватным ключам применяются многоуровневые меры безопасности, включая аутентификацию, авторизацию и контроль доступа.

3.1.1.2. Шифрование данных для обеспечения конфиденциальности пользовательской информации.

Сервис осуществляет шифрование пользовательских данных для обеспечения их конфиденциальности и защиты от несанкционированного доступа. Для этого применяются следующие методы:

1. ***Шифрование данных***
   Чувствительная информация, такая как личные данные пользователей и информация о транзакциях, шифруется с использованием современных криптографических алгоритмов.
2. ***Использование безопасных протоколов***
   Для передачи зашифрованных данных между основными компонентами Сервиса применяются безопасные протоколы связи, такие как SSL/TLS, что обеспечивает защищенную передачу информации.
3. ***Хранение зашифрованных данных***
   Зашифрованные данные хранятся в защищенном виде в базе данных или файловой системе, с доступом только для авторизованных пользователей и сотрудников Сервиса.
4. ***Ключи шифрования***
   Ключи шифрования хранятся отдельно от зашифрованных данных и защищаются с помощью механизмов управления ключами, что обеспечивает дополнительный уровень безопасности.

3.1.2. Управление кошельками

3.1.2.1. Регистрация новых кошельков.

Пользователи могут открыть новые кошельки. Кошелек обычно используется для быстрых и удобных операций с криптоактивами. Например, пользователь может предпочесть использовать кошелек для ежедневных транзакций. Такой выбор обеспечивает гибкость и удобство использования криптовалютного кошелька в зависимости от индивидуальных требований пользователя.

Пользователи также имеют возможность открывать несколько кошельков на различных блокчейнах. Это позволяет пользователям управлять различными криптоактивами и токенами, которые могут принадлежать к разным блокчейнам, в рамках одного удобного интерфейса. Такой функционал дает пользователям большую гибкость в управлении своими криптоактивами и позволяет им эффективно управлять своим портфелем криптоактивов.

3.1.2.2. Предоставление возможности создания мультиподписных кошельков.

Сервис предоставляет возможность создания мультиподписных кошельков, которые требуют подтверждения транзакций несколькими участниками. Это повышает безопасность операций и обеспечивает дополнительный уровень защиты от несанкционированных транзакций.

Владелец кошелька при создании указывает его участников; каждому участнику генерируются приватный и публичный ключи внутри оффчейн-системы с помощью метода эллиптических кривых. Для проведения операции требуются подписи заданного владельцем кошелька количества участников. При этом все подписи участников процесса подписания одинаковы по статусу: если одна из подписей будет отсутствовать (или минимальное число подписей соподписантов не будет получено), транзакция не отправится в сеть.

3.1.2.3. Возможность просмотра баланса, истории транзакций и другой информации по кошельку.

Пользователи могут легко отслеживать текущий баланс своих кошельков благодаря возможности просмотра. Это позволяет пользователям в реальном времени узнавать о количестве криптоактивов, находящейся на их кошельке. Кроме того, пользователи имеют доступ к истории всех проведенных транзакций, что обеспечивает полную прозрачность и позволяет вести учет всех операций с их активами. Просмотр информации по кошельку также может включать другие детали, такие как статус транзакций, комиссии, временные метки и дополнительные сведения о транзакциях. Это обеспечивает пользователям полный контроль и понимание их финансовых операций в рамках Сервиса.

3.1.2.4. Управление кошельками (включая операции по выводу и переводам, временная блокировка кошелька).

В рамках Сервиса каждому клиенту открывается персональный кошелек, обеспечивающий безопасное и конфиденциальное хранение криптоактивов клиента, а также доступ к ним только с его учетными данными. Персональный кошелек предоставляет клиенту уникальный идентификатор для доступа к его криптоактивам и выполнения различных операций, включая вывод и переводы. Каждый клиент имеет возможность полного управления своими существующими кошельками через Сервис, включая функцию временного ограничения доступа к активам.

Функция временного ограничения доступа к активам позволяет клиентам временно заблокировать возможность расходования криптоактивов со своего кошелька. Подобное ограничение может быть полезным в случае, если клиент временно не желает осуществлять операции с активами или хочет защитить свои средства от случайных или необдуманных расходов. В течение периода временного ограничения, ни сам клиент, ни другие пользователи не смогут осуществлять транзакции с данным кошельком. Это обеспечивает дополнительный уровень безопасности и контроля за финансовыми средствами клиента.

Функция временного ограничения доступа к активам не требует возможности ее отмены в процессе, так как ее цель - предоставить клиенту возможность защитить его средства от расходования в определенный период времени. После окончания указанного периода ограничения доступ к активам автоматически восстанавливается, обеспечивая удобство использования Сервиса и контроль над финансовыми средствами клиента.

3.1.3. Безопасность

3.1.3.1. Шифрование приватных ключей

Обеспечение безопасного хранения приватных ключей пользователей путем их шифрования с использованием алгоритма Advanced Encryption Standard (AES).

Шифрование методом AES гарантирует, что приватные ключи пользователей защищены высокоуровневой криптографической защитой. Ключи шифрования, используемые в процессе шифрования и дешифрования, имеют достаточную длину для обеспечения стойкости к атакам и предотвращения взлома.

Применение шифрования методом AES гарантирует, что даже в случае несанкционированного доступа к данным, приватные ключи пользователей останутся защищенными и недоступными для злоумышленников.

Таким образом, обеспечивается высокий уровень безопасности криптоактивов клиентов и предотвращается возможность их украдения или использования без разрешения владельца.

3.1.3.2. Реализация механизмов аутентификации и авторизации пользователей

Сервис устанавливает ограничения на количество неудачных попыток входа в учетную запись пользователя. Это предотвращает возможные атаки методом подбора паролей или использование брутфорс атак, когда злоумышленник пытается перебирать различные комбинации паролей.

После достижения предельного количества неудачных попыток входа Сервис может временно блокировать доступ к учетной записи или принимать другие меры безопасности, такие как запрос на восстановление пароля или ввод капчи для подтверждения человеческого присутствия.
Сервис устанавливает определенный период неактивности, после которого происходит автоматический выход из учетной записи пользователя. Это предотвращает

несанкционированный доступ в случае, если пользователь оставил свою учетную запись открытой без присмотра.

Период неактивности определяется в соответствии с требованиями безопасности и может быть настроен администратором Сервиса. После истечения этого периода Сервис автоматически завершает сеанс пользователя и требует повторной аутентификации при повторном доступе.

3.1.3.3. Мониторинг и обнаружение подозрительной активности

Интеграция с Group-IB Fraud Protection представляет собой механизм, который активно отслеживает каждую попытку входа в систему с целью выявления подозрительной активности и предотвращения мошеннических действий. При каждой попытке аутентификации система производит детальную диагностику сессии пользователя, используя алгоритмы машинного обучения и искусственного интеллекта для анализа аномальных паттернов и необычного поведения. Вот более подробное описание процесса:

- Анализ каждой попытки входа: Каждая попытка входа в систему подвергается тщательному анализу и проверке на наличие признаков подозрительной активности.
- Диагностика сессии пользователя: В момент входа в систему проводится анализ сессии пользователя, включая множество факторов, таких как история активности, IP-адрес, устройство, использованный браузер и т. д.
- Использование алгоритмов машинного обучения и искусственного интеллекта: Для обнаружения аномалий и необычного поведения система применяет алгоритмы машинного обучения и искусственного интеллекта. Эти алгоритмы способны выявлять аномальные паттерны, которые могут свидетельствовать о попытке несанкционированного доступа или мошенничестве.
- Предотвращение мошеннических действий: В случае обнаружения подозрительной активности система принимает соответствующие меры для предотвращения мошеннических действий, например, блокирует доступ или требует дополнительной аутентификации.

3.1.4. Регистрация и верификация KYC/KYB

3.1.4.1. Процедуры регистрации новых пользователей с последующей верификацией личности пользователей и организаций в соответствии с KYC/KYB требованиями.

Процедуры регистрации новых пользователей с последующей верификацией личности пользователей и организаций в соответствии с требованиями KYC (Know Your Customer) и KYB (Know Your Business) обеспечивают надежную идентификацию и аутентификацию пользователей перед предоставлением доступа к Сервису.

1. Регистрация новых пользователей:
    - Новые пользователи проходят процедуру регистрации, в ходе которой им предоставляются формы для заполнения основной информации, такой как имя, адрес электронной почты, номер телефона и т. д.

- Пользователи также могут предоставить дополнительные сведения в зависимости от типа аккаунта, например, данные организации, с которой они ассоциируются.

2. Верификация личности пользователей:
   - После завершения процесса регистрации пользователи подвергаются проверке для подтверждения их личности. Это включает в себя предоставление документов, подтверждающих личность, таких как паспорт, водительские права или иные документы, в соответствии с требованиями KYC.
3. Верификация организаций в соответствии с требованиями KYB:
   - Для организаций процесс верификации включает в себя проверку их легального статуса, регистрационных документов, уполномоченных лиц и прочих сведений, необходимых для подтверждения их легальности и подлинности.
   - Этот процесс может включать в себя запрос дополнительной информации о компании, проверку реестров и баз данных, а также контакт с представителями компании для подтверждения предоставленной информации.
4. Соблюдение требований KYC/KYB:
   - После успешной верификации личности и организации пользователи получают доступ к Сервису в соответствии с установленными правами доступа.
   - Данные о пользователях и их верификации хранятся в безопасной и защищенной среде, соблюдая все требования по защите конфиденциальности и безопасности данных.

3.1.5. Мониторинг и отчетность по операциям с криптоактивами

3.1.5.1. Ведение журнала операций и транзакций для обеспечения прозрачности и возможности анализа.

Сервис ведет подробный журнал всех операций и транзакций, происходящих в рамках Сервиса. Каждая операция, начиная от входа пользователя в систему и заканчивая завершением транзакций, регистрируется в журнале.

Для каждой операции сохраняется информация о времени ее выполнения, участниках (пользователи, кошельки, адреса и т. д.), типе операции (пополнение, вывод, перевод и т. д.), сумме, статусе и других сопутствующих данных.

Ведение журнала операций обеспечивает прозрачность действий в Сервисе, позволяет отслеживать историю операций для каждого пользователя и облегчает процесс аудита и анализа для выявления любых аномалий или нештатных ситуаций.

3.1.5.2. Предоставление отчетов о текущем состоянии активов и выполненных операциях.

Сервис предоставляет пользователю возможность получать отчеты о текущем состоянии своих активов и выполненных операциях.

Отчеты могут включать информацию о текущем балансе активов на каждом из кошельков, историю операций за определенный период времени, подробности о каждой операции, включая сумму, тип операции, участников и статус.

Пользователи могут настраивать параметры отчетов в соответствии с их потребностями, выбирая период времени, типы операций и другие параметры фильтрации.

Предоставление отчетов дает пользователям полный обзор и контроль над их финансовыми операциями, помогает им следить за динамикой изменения активов и делать информированные решения по управлению своими кошельками.

3.1.6. Интеграция с внутренними и внешними сервисами и компонентами

3.1.6.1. Взаимодействие с внутренними и внешними сервисами посредством API.

В рамках Сервиса был разработан API, который обеспечивает взаимодействие с внутренними и внешними сервисами.

Этот API используется в различных компонентах Сервиса, таких как личный кабинет пользователей и система электронного документооборота.

3.2. Нефункциональные требования

3.2.1. Производительность

3.2.1.1. Высокая скорость обработки транзакций и запросов пользователей

Сервис разработан с учетом оптимизации скорости обработки транзакций и запросов пользователей. Это означает, что система способна обрабатывать большие объемы данных и запросов с высокой скоростью, что обеспечивает отзывчивость и эффективность работы.

Для достижения высокой скорости обработки используются различные методы оптимизации, такие как кэширование данных, параллельная обработка запросов, оптимизация алгоритмов и структур данных, а также масштабируемая архитектура.

3.2.1.2. Минимальные задержки и ожидания при выполнении операций

Сервис стремится минимизировать задержки и ожидания, которые могут возникать при выполнении операций пользователей. Это включает в себя сокращение времени ответа на запросы, минимизацию времени обработки транзакций и операций, а также оптимизацию пользовательского интерфейса для уменьшения времени ожидания.

Для уменьшения задержек применяются различные подходы, включая оптимизацию кода, использование высокопроизводительных технологий и инфраструктуры, распределение нагрузки и динамическое масштабирование ресурсов в зависимости от нагрузки.

3.2.2. Надежность

3.2.2.1. Обеспечение стабильной работы Сервиса без сбоев и перерывов

Сервис построен таким образом что стремится функционировать безупречно и непрерывно, обеспечивая доступность для пользователей в любое время.

Для достижения этой цели применяются меры, такие как использование высокодоступных и отказоустойчивых архитектур, дублирование ресурсов, регулярные тестирования на прочность и нагрузочное тестирование, а также мониторинг состояния системы для быстрого обнаружения и устранения проблем.

3.2.2.2. Восстановление после сбоев и резервное копирование данных

Выполняются регулярные резервные копирования данных, чтобы в случае сбоя можно было восстановить информацию из резервных копий.

Кроме того, разрабатываются и тестируются планы восстановления после сбоев (Disaster Recovery Plans), которые определяют процедуры и шаги по восстановлению работы системы в минимально возможное время.

3.2.3. Доступность

3.2.3.1. Обеспечение доступности Сервиса в течение 24/7

Сервис будет доступен для пользователей в любое время суток, без прерываний или ограничений.

Для обеспечения непрерывной доступности могут использоваться высокодоступные архитектурные решения, дублирование серверов и ресурсов, а также глобальная распределенная сеть серверов для обработки запросов от пользователей из разных регионов мира.

3.2.3.2. Механизмы резервирования и автоматического мониторинга работоспособности

Для обеспечения непрерывной доступности применяются механизмы резервирования, такие как резервное копирование данных, дублирование оборудования и автоматический перенос нагрузки на резервные серверы в случае сбоя.

Также используются системы мониторинга работоспособности, которые постоянно отслеживают состояние Сервиса и оперативно реагируют на любые проблемы или сбои, предотвращая перерывы в доступе для пользователей.

3.2.4. Удобство использования

3.2.4.1. Интуитивно понятный интерфейс для удобства пользователей

Пользователи могут легко и без труда использовать личный кабинет Сервиса благодаря простому и интуитивно понятному интерфейсу.

Для достижения этой цели дизайн интерфейса разрабатывается с учетом принципов юзабилити и пользователям предоставляются интуитивно понятные элементы управления, логические и последовательные шаги при выполнении задач, а также интуитивные механизмы навигации.

3.2.4.2. Подробная документация и руководства пользователя для облегчения работы

Пользователям предоставляется подробное руководство пользования, которое помогает им освоить функциональность сервиса и эффективно использовать его возможности.

Документация включает в себя описание основных функций и возможностей сервиса, пошаговые инструкции по его использованию.

3.2.5. Масштабируемость

3.2.5.1. Возможность масштабирования Сервиса для обработки растущего числа пользователей и операций

Сервис может быть масштабирован горизонтально (добавление новых серверов) для обработки растущего объема пользователей и операций.

Горизонтальное масштабирование предполагает добавление новых серверов или узлов в сеть для распределения нагрузки и увеличения пропускной способности системы.

3.2.5.2. Горизонтальное масштабирование для распределения нагрузки

Сервис способен горизонтально масштабироваться для эффективного распределения нагрузки между несколькими серверами или узлами.

При горизонтальном масштабировании нагрузка автоматически распределяется между несколькими серверами в сети, что позволяет равномерно распределять нагрузку и

обеспечивать стабильную производительность системы при росте числа пользователей и операций.

3.2.6. Соответствие требованиям регуляторов

3.2.6.1. Соблюдение законодательства и регулирований в области финансовых операций и криптоактивов

Сервис полностью соответствует требованиям законодательства и регулирований, касающихся финансовых операций и использования криптоактивов.

Для этого сервис использует средства аутентификации и идентификации пользователей, методы проверки легитимности финансовых операций, а также механизмы анти-мошенничества и предотвращения отмывания денег (AML).

3.2.6.2. Возможность предоставления отчетности и данных о пользователях регуляторам

Наличие механизмов и процедур для предоставления отчетности и данных о пользователях регуляторам и надзорным органам, если это требуется в соответствии с законодательством.

Сервис может вести детальную отчетность о финансовых операциях и активности пользователей, а также обеспечивать доступ к этой информации в случае запроса со стороны регуляторов.

4. Архитектура Сервиса

4.1. Общее описание архитектуры, включая компоненты и их взаимосвязи

Архитектура Сервиса представляет собой распределенную систему, состоящую из различных компонентов, каждый из которых выполняет определенные функции и взаимодействует с другими компонентами для обеспечения работы Сервиса.

Комплекс программно-аппаратных компонентов, обеспечивают безопасное хранение, управление и передачу криптоактивов.

4.1.1. BlackBox

Является центральным элементом управления криптоактивами. Его функционал включает в себя подсистемы шифрования и хранения ключей, определение правил обработки секретных ключей, а также взаимодействие с блокчейном.

Размещенный в специально сегментированной зоне, Black Box блокирует несанкционированный доступ к внутренней сети, действуя в строгом соответствии с

установленными при создании правилами. Этот сервер ответственен за генерацию кошельков, хранение приватных ключей, подписание транзакций и их последующую отправку в блокчейн.

Привилегии доступа к этому серверу строго ограничены, что гарантирует неприкосновенность приватных ключей кошельков и исключает возможность несанкционированных действий со стороны сотрудников. Это обеспечивает высокий уровень безопасности и надежности в управлении криптоактивами в рамках Сервиса.

Его основные свойства:

- Защита от несанкционированного физического доступа к информации;
- Внешние исходящие сетевые правила позволяют связь только с 3мя фиксированными нодами (HTTPS), 2мя управляющими серверами (шифрованный трафик между Domino серверами);
- Хранение ключей от кошелька (авторизация использования, уменьшение риска потери);
- Валидация входящих транзакций;
- Валидация и инициирование исходящих транзакций;
- Защита от внешней цифровой атаки;
- Защита от физической атаки на оборудование;
- Защита от принуждения клиента к подаче приказа на операцию;
- Ведение журналов запросов на операции и самих операций;
- Передача финансовой учетной системе реквизитов транзакции;
- Снабжение владельца актива оперативной информацией по балансу кошелька.

4.1.2. API

API представляет собой интерфейс для взаимодействия внешних серверов с Управляющим сервером Сервиса. Он позволяет осуществлять запросы для создания криптокошельков, выполнения транзакций, а также получения информации о кошельках и транзакциях.

Основные функции API:

- Создание криптокошельков: API предоставляет метод для создания новых криптокошельков. Этот метод генерирует уникальные адреса и возвращает их внешним серверам для дальнейшего использования.
- Проведение операций: С помощью API можно инициировать и проводить различные транзакции, такие как отправка и получение криптоактивов. API обрабатывает запросы, передает их на Управляющий сервер и возвращает статус выполнения операции.
- Получение информации о кошельках: API позволяет внешним системам получать актуальную информацию о балансе и статусе кошельков. Запросы к API возвращают данные, хранящиеся в системе, включая историю транзакций и текущие балансы.

- Получение информации о транзакциях: API предоставляет методы для запроса детальной информации о конкретных транзакциях, включая их статус, сумму, дату и другие важные параметры.

Основные свойства API:

- Безопасность: Все взаимодействия с API осуществляются через зашифрованные каналы связи (HTTPS), что гарантирует защиту данных от перехвата и несанкционированного доступа.
- Аутентификация и авторизация: Для доступа к API требуется использование токенов аутентификации. Каждый запрос проверяется на предмет наличия и валидности токена, что предотвращает несанкционированное использование API.
- Логирование: Все запросы и операции, выполняемые через API, записываются в журналы. Это обеспечивает возможность аудита и анализа действий, выполняемых через API.
- Высокая доступность: API спроектирован с учетом требований к высокой доступности и устойчивости к отказам, что обеспечивает бесперебойное функционирование даже при высокой нагрузке.
- Гибкость и масштабируемость: Архитектура API позволяет легко расширять его функционал и масштабировать в зависимости от потребностей Сервиса и внешних систем.

4.1.3. Управляющий сервер

Управляющий сервер является центральным элементом в архитектуре Сервиса, обеспечивая создание и управление документами по запросу API или в рамках бизнес-процессов документооборота. Эти документы могут касаться создания кошельков, проведения транзакций и других операций, связанных с криптоактивами.

Основные функции Управляющего сервера:

- Создание документов: Управляющий сервер генерирует документы на основе запросов, поступающих через API. Эти документы могут включать заявки на создание криптокошельков, проведение транзакций и другие операции.
- Валидация и проверка подписей: Управляющий сервер проверяет подписи всех входящих запросов для обеспечения их подлинности и целостности. Это предотвращает несанкционированные операции и гарантирует, что все запросы поступают от доверенных источников.
- Поддержка документооборота: В рамках бизнес-процессов документооборота Управляющий сервер управляет созданием, обновлением и хранением документов, связанных с операциями внутри Сервиса.
- Ожидание запроса от BlackBox: После создания документов Управляющий сервер ожидает запроса от BlackBox. Когда BlackBox обращается к Управляющему серверу, он предоставляет необходимые документы для анализа и принятия решения.

Процесс работы:

- Получение запроса через API:

- Запрос поступает от внешнего сервера через API, например, на создание нового криптокошелька или инициирование транзакции.
- Создание документа:
- Управляющий сервер создает соответствующий документ, содержащий все необходимые данные для выполнения запроса.
- Проверка подписи:
- Управляющий сервер проверяет подпись запроса для подтверждения его подлинности и целостности.
- Ожидание запроса от BlackBox:
- Управляющий сервер сохраняет созданный документ и ждет запроса от BlackBox.
- Запрос от BlackBox и принятие решения:
- BlackBox обращается к Управляющему серверу, запрашивая необходимые документы. Основываясь на данных из этих документов, BlackBox вычисляет, следует ли проводить транзакцию в блокчейне. При положительном решении транзакция подписывается и отправляется в блокчейн.

Основные свойства Управляющего сервера:

- Безопасность: Управляющий сервер оснащен механизмами защиты от несанкционированного доступа и цифровых атак, что обеспечивает безопасность и целостность всех обрабатываемых данных.
- Надежность: Сервер спроектирован для обеспечения высокой надежности и устойчивости к отказам, что гарантирует бесперебойное выполнение всех операций.
- Гибкость: Управляющий сервер поддерживает интеграцию с различными бизнес-процессами, что позволяет легко адаптироваться к изменениям в требованиях и масштабировать систему по мере необходимости.
- Логирование: Все операции, выполняемые Управляющим сервером, записываются в журналы, что обеспечивает возможность аудита и анализа действий.

Таким образом, Управляющий сервер играет ключевую роль в обеспечении надежного и безопасного выполнения операций внутри Сервиса, ожидая запросов от BlackBox для принятия окончательных решений по транзакциям и другим операциям.

4.1.4. Сетевая инфраструктура

Поскольку АПК построен на средствах виртуализации, большая часть сетевой инфраструктуры представлена программным обеспечением.
Сетевая инфраструктура включает в себя:

- программные модули операционных систем, отвечающих за сетевое взаимодействие;
- программный модуль сетевого процессора, обеспечивающего реализацию сетевых правил взаимодействия между серверами и службами, основанный на специальной операционной системе Routeros;
- Виртуальные сетевые интерфейсы;
- Драйвера аппаратных сетевых интерфейсов;
- Соединительные кабели.

4.1.5. Аппаратное обеспечение

Для обеспечения надежной и эффективной работы Сервиса, аппаратное обеспечение представлено серверами HP DL380. Эти серверы являются одними из наиболее надежных и мощных в своем классе и широко применяются в корпоративной среде. Их высокая производительность и устойчивость позволяют обрабатывать большие объемы данных и обеспечивать непрерывную работу платформы.

4.1.6. Личный кабинет

В рамках сервиса разработано несколько Личных кабинетов, объединенных единым сервером авторизации, для предоставления различных услуг. Эти услуги включают кастодиальный сервис для институциональных клиентов и сервис по предоставлению крипто-эквайринга для получения платежей в криптоактивах.

Личный кабинет для кастодиального сервиса:
Этот Личный кабинет предоставляет услуги по управлению кастодиальными кошельками для институциональных клиентов, таких как криптобиржи, брокеры, фонды, майнеры и другие юридические лица.

Основные функции:

- Создание кошельков: Позволяет создавать новые криптокошельки с интуитивно понятным интерфейсом.
- Проведение транзакций: Пользователи могут отправлять и получать криптоактивы, отслеживать статус транзакций и управлять своими средствами.
- Просмотр информации: Пользователи могут просматривать баланс своих кошельков, историю транзакций и другие важные данные.

Интеграция с сервисом единого входа:

- Личный кабинет интегрирован с сервисом единого входа (см. 4.1.9.), что обеспечивает регистрацию и верификацию пользователя, а также управление учетными записями.
- Процесс работы с юридическими лицами:
- Создание учетной записи юридического лица: После авторизации физического лица пользователь может создать учетную запись для юридического лица, включающую ввод и верификацию необходимых данных.
- Подписание для вывода средств: Для вывода средств из кастодиального хранения предусмотрен специальный процесс подписания, обеспечивающий дополнительный уровень безопасности и подтверждение операций.
- Оплата сервиса:
- Программа для оплаты услуг сервиса, позволяющая настраивать автоматические платежи с кошелька на регулярной основе (например, раз в месяц или квартал).

Личный кабинет для сервиса крипто-эквайринга:
Этот Личный кабинет предназначен для мерчантов, которым необходимо принимать платежи в виде криптоактивов, например, для интернет-магазинов. Сервис предоставляет

возможности интеграции на сторонние сайты и отображения виджета с адресом кошелька для приема платежей.

Основные функции:

- Интеграция со сторонними сайтами: Предоставление API для крипто-эквайринга, которое позволяет мерчантам интегрировать сервис на свои сайты.
- Отображение виджета: Виджет с адресом кошелька для приема криптовалютных платежей отображается на сайте мерчанта.
- Создание платежей: Пользователи могут создавать платежи через специальный интерфейс, генерируя уникальные адреса кошельков для каждой транзакции.
- Мониторинг и управление: Мерчанты могут отслеживать поступающие платежи, просматривать историю транзакций и управлять своими счетами.

Интеграция с сервисом единого входа:

- Личный кабинет для крипто-эквайринга также интегрирован с сервисом единого входа, что обеспечивает удобство регистрации и верификации пользователя.

Процесс работы с мерчантами:

- Регистрация мерчанта: Мерчанты регистрируются через сервис единого входа и получают доступ к Личному кабинету для крипто-эквайринга.
- Создание платежного виджета: Мерчанты могут настроить и интегрировать платежный виджет на свои сайты, используя предоставленное API.
- Прием платежей: Платежи поступают на уникальные адреса кошельков, генерируемые для каждой транзакции, и отображаются в Личном кабинете.

Основные свойства Личных кабинетов:

- Удобный интерфейс: Личные кабинеты предоставляют пользователям простой и понятный интерфейс для выполнения всех операций.
- Безопасность: Все действия, выполняемые в Личных кабинетах, защищены с помощью современных методов шифрования и механизмов аутентификации.
- Гибкость и масштабируемость: Личные кабинеты могут адаптироваться к изменениям в требованиях пользователей и масштабироваться в зависимости от их потребностей.
- Логирование: Все операции, выполняемые через Личные кабинеты, записываются в журналы, что обеспечивает возможность аудита и анализа действий пользователей.

Таким образом, Личные кабинеты обеспечивают удобное и безопасное управление криптоактитивными кошельками и платежами, предоставляя необходимые функции для различных категорий пользователей и взаимодействуя с сервисом через единый сервер авторизации.

Административная часть:
В сервисе предусмотрена административная часть с пользовательским интерфейсом, предназначенная для разработчиков, использующих API. Этот интерфейс позволяет настраивать параметры интеграции, включая указание URL-адресов для отправки

результатов запросов. Разработчики могут легко управлять этими настройками, обеспечивая автоматическую обработку данных и взаимодействие с их системами в реальном времени. Это обеспечивает гибкость и удобство при интеграции сервиса с внешними приложениями и сервисами.

4.1.7. Учетная система

Учетная система представляет собой мощный инструмент для управления финансовыми данными и активами клиентов. Специально спроектированная для воздействия на различные аспекты бизнес-процессов, эта учетная система призвана обеспечить точность, надежность и эффективность в управлении криптоактивов.

Учетная система полностью автоматизирует обработку данных, снижая риск возможных ошибок и обеспечивая оперативное обновление информации об активах. Это повышает эффективность управления финансовыми данными

Тесная интеграция с технологией блокчейн обеспечивает прозрачность и надежное отслеживание каждой транзакции и изменения в составе активов. Клиенты могут быть уверены в безопасности и достоверности финансовой информации.

Прямой поток данных с блокчейн обеспечивает высокую степень прозрачности транзакций, позволяя клиентам в режиме реального времени отслеживать и анализировать изменения в личном кабинете.

4.1.8. Бизнес-процессинг

Система электронного документооборота с настроенными бизнес-процессами обеспечивает безопасный обмен структурированной информацией и электронными документами.

Электронный документооборот обеспечивает возможность прозрачного отслеживания всех документов и транзакций в системе. Это позволяет получать полную информацию о ходе операций, статусе транзакций и других важных событиях, что способствует улучшению контроля и управления активами.

Электронные документы, подписи и другие цифровые атрибуты поддерживаются с использованием многоуровневых мер безопасности, включая шифрование и цифровые подписи. Настраиваемые бизнес-процессы, интегрированные в документооборот, позволяют автоматизировать многие рутинные операции, такие как проверка данных, обработка запросов и создание отчетов. Это сокращает время выполнения операций и повышает общую эффективность работы. Он также включает в себя функции учета, обработки и обновления данных, что обеспечивает точность и надежность информации о держателях криптоактивов. Это является ключевым аспектом для соблюдения требований и стандартов в сфере криптокастоди.

Специальные бизнес-процессы в рамках системы электронного документооборота:

a. Создание карточки контрагента в базе данных:

Процесс включает в себя сбор и регистрацию основной информации о контрагенте, такой как личные данные, юридическая информация, реквизиты. Создание карточки контрагента обеспечивает удобный доступ к информации и управление клиентской базой данных.

b. KYC/KYB верификация пользователя:

Верификация личности (Know Your Customer) и верификация бизнеса (Know Your Business) — процессы, направленные на проверку подлинности клиента и его деятельности. Включает сбор и анализ документов, а также проведение проверок на соответствие законодательным требованиям.

c. Заключение договора с клиентом:

Электронное оформление договоров с клиентами, включая необходимую юридическую информацию и согласование условий. Процесс обеспечивает прозрачность и легкость ведения документации по заключенным сделкам.

d. Создание кошелька:

Процесс, позволяющий клиентам создавать криптовалютные кошельки для безопасного и удобного хранения своих активов. Включает в себя генерацию уникального адреса кошелька и установку дополнительных безопасностей.

e. Ввод и вывод средств:

Обеспечивает пользователям возможность внесения и вывода средств с их кошельков, включая определение сумм, выбор метода транзакции и подтверждение операций.

f. Процедура подтверждения транзакции при выводе средств в случае увеличения лимита:

Дополнительный этап безопасности, который вступает в силу при достижении определенных лимитов вывода средств. Включает подтверждение пользователя и, возможно, дополнительные шаги аутентификации.

g. Выпуск смартконтракта и токена в соответствии с параметрами, указанными клиентами:

Процесс, позволяющий клиентам создавать свои уникальные смартконтракты и токены в соответствии с заданными параметрами. Включает в себя установку правил и параметров для функционирования токена.

h. Комплаенс и реагирование на подозрительные транзакции:

Реализует меры по соблюдению законодательных требований и обнаружению подозрительных транзакций. Включает в себя мониторинг и анализ операций, а также реагирование в случае выявления аномалий.

Эти специальные бизнес-процессы в системе электронного документооборота обеспечивают полный жизненный цикл взаимодействия с клиентами и управление

криптоактивами, соблюдение законодательных требований и обеспечение безопасности операций.

Интеграция системы мультиподписи в систему электронного документооборота, основанную на HCL Notes, является ключевым элементом, обеспечивающим дополнительный уровень безопасности для операций с криптоактивами. Эта интеграция обеспечивает контроль и подтверждение подписей в рамках документооборота, создавая дополнительный барьер для защиты активов клиентов

4.1.9. ПО дополнительных систем

Сервер авторизации:
Отвечает за регистрацию и авторизацию пользователей в Личные кабинеты, обеспечивая безопасность и удобство доступа к сервисам. Используя технологию OAuth 2.0, сервер авторизации поддерживает стандартизированный и безопасный механизм аутентификации и авторизации, что позволяет легко интегрировать его в сторонние сервисы в будущем.

Основные функции сервера авторизации:

- Регистрация пользователей: Обеспечивает процесс создания учетных записей для новых пользователей, включая проверку и верификацию данных.
- Авторизация пользователей: Обеспечивает безопасный вход в Личные кабинеты, проверяя подлинность учетных данных пользователей.
- Управление сессиями: Контролирует сессии пользователей, обеспечивая их защиту от несанкционированного доступа и поддерживая их активность.
- Интеграция с OAuth 2.0: Использование стандарта OAuth 2.0 обеспечивает возможность безопасного и стандартизированного доступа к ресурсам, что упрощает интеграцию с другими сервисами.

Преимущества использования OAuth 2.0:

- Безопасность: OAuth 2.0 обеспечивает безопасный механизм передачи данных, минимизируя риск утечки учетных данных.
- Гибкость: Позволяет настраивать различные уровни доступа и разрешений для пользователей и приложений.
- Совместимость: Стандартизированный протокол легко интегрируется с множеством сторонних сервисов, расширяя возможности использования сервиса авторизации.

Пример процесса авторизации:

1. Регистрация нового пользователя:
    - Пользователь предоставляет необходимые данные для регистрации.
    - Сервер авторизации проверяет и верифицирует данные.
    - Учетная запись пользователя создается и подтверждается.
2. Вход в Личный кабинет:
    - Пользователь вводит свои учетные данные (логин и пароль).
    - Сервер авторизации проверяет подлинность данных.
    - При успешной авторизации пользователь получает доступ к Личному кабинету.

3. Интеграция с внешним сервисом:
    - Внешний сервис запрашивает доступ к ресурсам пользователя через сервер авторизации.
    - Сервер авторизации предоставляет токен доступа, обеспечивая безопасный и контролируемый доступ к ресурсам.

Таким образом, сервер авторизации играет ключевую роль в обеспечении безопасного и удобного доступа к Личным кабинетам, поддерживая современные стандарты безопасности и предоставляя возможности для будущих интеграций со сторонними сервисами.

Сервер резервного копирования:
Является важной частью инфраструктуры сервиса, обеспечивая надежное и безопасное хранение резервных копий данных. Его основная задача - регулярное создание и хранение резервных копий, а также обеспечение их доступности в случае необходимости восстановления данных.

Основные функции сервера резервного копирования:

- Автоматизированное создание резервных копий: Сервер автоматически создает резервные копии данных с заданной периодичностью, обеспечивая их актуальность и полноту.
- Хранение резервных копий: Созданные копии данных хранятся на сервере резервного копирования в зашифрованном виде, обеспечивая их конфиденциальность и целостность.
- Мониторинг и администрирование: Администраторы могут мониторить состояние резервных копий, проводить их проверку на целостность и производить необходимые административные операции.
- Восстановление данных: В случае потери данных или необходимости восстановления системы, сервер резервного копирования предоставляет возможность быстрого и надежного восстановления данных из резервных копий.

Преимущества использования сервера резервного копирования:

- Безопасность данных: Резервные копии хранятся в зашифрованном виде, что обеспечивает защиту данных от несанкционированного доступа и утечек.
- Надежность: Автоматизированный процесс создания и хранения резервных копий обеспечивает их регулярность и актуальность, минимизируя риск потери данных.
- Гибкость: Сервер резервного копирования может быть настроен под конкретные требования сервиса, включая периодичность создания копий, их хранение и восстановление данных.
- Экономия ресурсов: Эффективное управление ресурсами сервера резервного копирования позволяет оптимизировать использование вычислительных и сетевых ресурсов.

Сервер резервного копирования обеспечивает надежное и безопасное хранение резервных копий данных, обеспечивая бесперебойную работу сервиса и быстрое восстановление данных в случае необходимости.

4.1.10. Блокчейн ноды

Собственные блокчейн ноды играют ключевую роль в интеграции сервиса с различными блокчейн сетями, обеспечивая прямое взаимодействие с целевыми блокчейнами без посредничества сторонних сервисов. Создание и использование собственных блокчейн нод позволяет сервису получать данные, проводить транзакции и выполнять другие операции на блокчейне непосредственно через собственные разработки, что обеспечивает большую гибкость, контроль и независимость.

Основные функции собственных блокчейн нод:

- Прямое взаимодействие с блокчейн сетями: Ноды обеспечивают прямое подключение к целевым блокчейн сетям, позволяя сервису получать данные, отправлять транзакции и выполнять другие операции на блокчейне.
- Гибкость и настраиваемость: Собственные блокчейн ноды могут быть настроены под конкретные потребности и требования сервиса, включая выбор используемых протоколов, параметров сети и других параметров.
- Безопасность: Ноды обеспечивают безопасное взаимодействие с блокчейн сетями, используя современные методы шифрования и защиты данных.
- Контроль и независимость: Создание и использование собственных блокчейн нод позволяет сервису сохранять контроль над своими операциями на блокчейне и не зависеть от сторонних сервисов или провайдеров.

Преимущества использования собственных блокчейн нод:

- Полный контроль: Сервис имеет полный контроль над своими операциями на блокчейне, включая безопасность, пропускную способность и другие аспекты.
- Гибкость и настраиваемость: Возможность настройки и конфигурации собственных блокчейн нод позволяет адаптировать их под уникальные потребности и требования сервиса.
- Независимость: Сервис не зависит от сторонних провайдеров или сервисов блокчейна, что обеспечивает независимость и устойчивость операций на блокчейне.

Создание и использование собственных блокчейн нод позволяет сервису получать максимальную гибкость, контроль и независимость в интеграции с различными блокчейн сетями, обеспечивая эффективное и безопасное взаимодействие с ними.

4.2. Описание технологий и инструментов, используемых в разработке Сервиса

В разработке Сервиса используются современные технологии и инструменты, обеспечивающие его надежную работу, безопасность и эффективность. Ниже приведены основные технологии и инструменты, применяемые в разработке:

1. Криптография:
   В Сервисе применяются современные криптографические алгоритмы для защиты приватных ключей, шифрования данных и обеспечения безопасности транзакций. Это включает в себя использование алгоритмов шифрования, хэширования, эллиптических кривых и других методов криптографии.

2. Инструменты тестирования:
   В процессе разработки Сервиса применяются различные инструменты для автоматизированного тестирования, включая модульное, интеграционное и функциональное тестирование, а также инструменты для обеспечения безопасности кода.
3. Мониторинг и аналитика:
   Для отслеживания работы Сервиса, выявления проблем и анализа производительности используются специализированные инструменты мониторинга и аналитики, отслеживания работоспособности и эффективности.
4. Базы данных:
   Для хранения данных о пользователях, транзакциях и другой информации используются базы данных PostgreSQL.
5. Языки программирования:
   В зависимости от конкретных задач и компонентов сервиса, используются различные языки программирования, такие как, Java, JavaScript, Lotus script (HCL Notes) а также фреймворки, такие как, NodeJS и ExpressJS.

5. Интеграция и взаимодействие

5.1. Описание протоколов и форматов обмена данными

Сервис использует стандартные протоколы и форматы обмена данными для взаимодействия с другими системами и компонентами. В частности, для внешнего API и обмена данными с клиентами и внешними системами используется RESTful API. Для обеспечения безопасности и конфиденциальности данных могут применяться стандартные защищенные протоколы связи, такие как HTTPS.

5.1.1. Внешние API, используемые Сервисом, и как они взаимодействуют с другими системами

Сервис использует внешние API для взаимодействия с различными системами и сервисами. Некоторые из них включают:

- API криптовалютных бирж для получения актуальной информации о курсах токенов USDT-TRX при автообмене.
- API для проверки KYC/KYB (знай своего клиента/знай своего бизнес-партнера) сервиса Sumsub.
- API для мониторинга чистоты криптоактивов сервиса Scorechain.
- Внутренние API для взаимодействия между различными компонентами в рамках архитектуры Сервиса.

5.1.2. Процессы синхронизации и/или обмена данными с другими компонентами.

Сервис реализует процессы синхронизации и обмена данными с другими компонентами системы с помощью асинхронных и синхронных методов обмена информацией. Например:

- Регулярные запросы к внешним API:
    - Сервис осуществляет регулярные запросы к внешним API, например, к криптовалютным биржам, для получения актуальной информации о курсах криптоактивов USDT и TRX для их обмена.
- Автоматизированный обмен данным через внутренние API:
    - Для обмена данными между различными компонентами системы используются внутренние API, которые позволяют передавать информацию между компонентами. К примеру, данные о пользовательских транзакциях передаются из бэкенда в фронтенд для отображения в личном кабинете пользователя.
- Реализация механизмов обмена данными в реальном времени:
    - Для оперативного реагирования на изменения состояния системы, Сервис реализует механизмы обмена данными в реальном времени.

6. Безопасность

Безопасность является важным аспектом работы Сервиса. Ниже представлено описание мер безопасности, механизмов аутентификации и авторизации, а также методов защиты от атак и угроз безопасности.

6.1. Описание мер безопасности, применяемых в Сервисе

Хранение приватных ключей
Приватные ключи хранятся в защищенном хранилище данных - BlackBox, где применяются методы шифрования и хеширования для обеспечения их безопасности.

Расположение в DMZ (Зона Демилитаризации)
BlackBox располагается в сегменте сети, известном как DMZ. Это специально выделенная зона сети, которая находится между внешней сетью интернета и внутренней сетью организации. Такое размещение обеспечивает повышенный уровень безопасности, поскольку BlackBox изолирован от внешних сетевых запросов и имеет ограниченный доступ к внутренним ресурсам организации.

Ограничения внешних запросов
BlackBox не принимает внешние сетевые запросы напрямую. Все запросы на получение и отправку данных, связанные с операциями, исходят только от BlackBox. Это обеспечивает дополнительный уровень безопасности и предотвращает возможные атаки извне на систему хранения и управления приватными ключами.

Многоуровневая система контроля
Применяется многоуровневая система контроля доступа для предотвращения несанкционированного доступа к приватным ключам и другим конфиденциальным данным.

6.2. Защита от атак и угроз безопасности

6.2.1. Мониторинг и обнаружение аномалий

В разделе 3.1.3.3. Мониторинг и обнаружение подозрительной активности3.1.3.3. Мониторинг и обнаружение подозрительной активности описана внедренная система мониторинга и обнаружения аномальной активности, включая интеграцию с сервисом Group IB Hunting Platform.
Для выявления аномальной активности, такой как необычные сетевые запросы или подозрительные попытки входа, применяются алгоритмы машинного обучения и анализа данных. Обнаружение аномалий позволяет оперативно реагировать на потенциальные угрозы безопасности и принимать соответствующие меры для защиты системы. Подключение сервиса Group IB Hunting Platform обеспечивает эффективное выявление и предотвращение угроз безопасности, что гарантирует высокий уровень защиты для пользователей и их данных.

6.2.2. Защита от DDoS-атак

Для защиты от распределенных атак отказа в обслуживании (DDoS) внедрены специализированные средства и механизмы. Эти средства включают в себя использование передовых технологий фильтрации трафика, обнаружения и блокирования атакующих IP-адресов, а также механизмы ограничения доступа для предотвращения перегрузки серверов.
Технологии фильтрации трафика
Используются для выявления и отсеивания аномального или вредоносного сетевого трафика, который может быть характерен для DDoS-атак. Это позволяет минимизировать негативное воздействие на работу Сервиса и сохранить его доступность для легитимных пользователей.
Обнаружение и блокирование атакующих IP-адресов
Происходит на основе анализа поведения трафика и выявления характерных признаков атаки. После идентификации потенциально вредоносных IP-адресов применяются меры блокирования для исключения их влияния на работу Сервиса.
Механизмы ограничения доступа
Предотвращают перегрузку серверов путем установки ограничений на количество запросов или подключений от одного и того же источника. Это позволяет более эффективно управлять нагрузкой и поддерживать стабильную работу Сервиса даже при попытках атаки.

Эти меры обеспечивают непрерывную работу Сервиса даже в условиях массовых сетевых атак, обеспечивая высокий уровень доступности и защиты для пользователей и их данных.

6.2.3. Резервное копирование и восстановление

В разделе 3.2.2. Надежность описано что Система осуществляет регулярное создание резервных копий данных. Это включает информацию о пользовательских аккаунтах, транзакциях и другие важные компоненты.
Этот процесс выполняется периодически с заданной частотой, обеспечивая актуальность резервных данных.

Преимущества регулярного резервного копирования:

1. ***Быстрое восстановление работоспособности***
   В случае атаки, сбоя системы или других чрезвычайных ситуаций, регулярно создаваемые резервные копии позволяют оперативно восстановить работу Сервиса. Это минимизирует временные простои и обеспечивает быстрое восстановление доступности для пользователей.

2. ***Минимальные потери данных***
   Регулярное резервное копирование гарантирует сохранность данных и минимизирует риск потери информации в случае непредвиденных ситуаций. Поскольку данные регулярно обновляются в резервных копиях, потеря информации ограничивается до последней созданной копии.

3. ***Сохранение непрерывности работы Сервиса***
   Регулярное создание резервных копий данных обеспечивает непрерывность работы Сервиса даже в случае возникновения непредвиденных обстоятельств. Это помогает поддерживать уровень Сервиса на высоком уровне и обеспечивать надежность и устойчивость для пользователей.

7. Сопровождение и обновление

7.1. Информация о процедурах обновления и сопровождения Сервиса

7.1.1. Обновление Сервиса

- Планирование обновлений
  - Периодически Сервис планирует обновления для внедрения новых функций, исправления ошибок и улучшения безопасности. Планирование проводится с учетом времени, когда оно оказывает минимальное воздействие на пользователей.

- Тестирование перед обновлением
  - Перед выпуском обновлений проводится тщательное тестирование, чтобы удостовериться в их корректности и отсутствии негативного влияния на работу системы.

- Последовательное внедрение
  - Обновления внедряются последовательно на тестовые и продуктивные среды, чтобы минимизировать возможность возникновения сбоев и недоступности сервиса.

- Резервное копирование данных

- Перед обновлением системы создаются резервные копии данных, чтобы в случае неудачного обновления можно было быстро восстановить работоспособность сервиса.

7.1.2. Сопровождение Сервиса

- Устранение неполадок
  - Специалисты по сопровождению реагируют на возникающие проблемы, исправляют их и вносят соответствующие изменения для предотвращения их повторного возникновения.

- Поддержка пользователей
  - Оказание поддержки пользователем, включая решение проблем и ответы на вопросы, с целью обеспечения непрерывной работы и удовлетворения потребностей пользователей.

- Обновление документации
  - Постоянное обновление документации, включая руководства пользователя и техническую документацию, чтобы отражать последние изменения и обновления в сервисе.

8. Заключение

В целом, Сервис представляет собой важное звено в мире криптоактивов, обеспечивая безопасное и эффективное управление криптоактивами для различных категорий пользователей. Он играет ключевую роль в обеспечении безопасности, надежности и прозрачности операций с криптоактивами.

В процессе анализа Сервиса были выявлены его сильные стороны, такие как эффективная защита приватных ключей, многоуровневая система контроля и мониторинга, а также широкий спектр интеграций с внешними сервисами и биржами криптоактивов. Однако, всегда есть место для улучшений и доработок.

Направления развития и улучшения:

- Расширение функциональности:
  Внедрение новых функций и возможностей, например, улучшенная аналитика операций, автоматизация процессов, интеграция с новыми блокчейнами и криптоактивами.
- Повышение безопасности:
  Непрерывное усовершенствование механизмов безопасности, внедрение новых методов аутентификации и авторизации, а также реагирование на новые угрозы и уязвимости.
- Улучшение пользовательского опыта:

Оптимизация интерфейса пользователя, улучшение процесса регистрации и верификации, а также предоставление более понятной и информативной документации.

С учетом постоянно меняющегося характера криптовалютного рынка и повышающихся требований к безопасности, развитие и улучшение сервиса должны быть непрерывными процессами, направленными на обеспечение высокого уровня удовлетворения потребностей пользователей и обеспечение его конкурентоспособности на рынке.