МОБИЛЬНЫЙ ДЕЦЕНТРАЛИЗОВАННЫЙ НЕКАСТОДИАЛЬНЫЙ КРИПТОВАЛЮТНЫЙ КОШЕЛЕК НА ПЛАТФОРМЕ IOS

Козко Р.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Фадеева Е.Е. – ассистент

Данная статья посвящена мобильным криптовалютным кошелькам как удобному, быстрому и надежному инструменту для хранения и использования криптовалют на мобильных устройствах. В ней рассмотрены основные принципы работы мобильных криптовалютных кошельков и предоставлен путь реализации децентрализованного некастодиального кошелька на платформе iOS.

В последние годы в связи с развитием технологий блокчейн криптовалюта стала одной из наиболее обсуждаемых и быстро развивающихся технологий в мире. Она представляет собой цифровую валюту, которая может быть использована для относительно быстрых и безопасных транзакций в любой точке мира, обходя при этом традиционные финансовые институты. Криптовалюта уже получила широкое распространение и привлекает внимание не только инвесторов и обычных пользователей, но и крупных корпораций и правительств. В связи с быстрым развитием технологий и ростом интереса к криптовалюте, ее актуальность в наше время неоспорима, а роль криптовалютных кошельков в обеспечении безопасности и удобства хранения цифровых активов становится все более важной.

Принцип работы криптовалютных кошельков и криптовалюты в целом основан на использовании публичных и приватных ключей. Приватный ключ используется для создания публичного ключа и отправки криптовалюты, тогда как публичный ключ используется для получения криптовалюты и является уникальным адресом. Когда пользователь отправляет криптовалюту, он подписывает транзакцию приватным ключом и она отправляется в сеть блокчейн, где она подтверждается валидаторами и записывается в блок.

Для разработки мобильного криптовалютного кошелька необходимо решить следующие задачи:

Выбрать или написать собственную библиотеку для управления криптовалютой. Написание собственной библиотеки занимает огромное количество времени и ресурсов, в то время как существует достаточное количество открытых и популярных решений.

Выбрать способ хранения мнемонической фразы. По способу управления приватными ключами криптовалютные кошельки делятся на кастодиальные и некастодиальные [1]. В зависимости от типа мнемоническая фраза может хранится на неком сервере или непосредственно на устройстве. Так как рассматривается создание некастодиального кошелька на платформе iOS, то мнемоника должна хранится непосредственно на мобильном устройстве в защищенном хранилище Keychain, доступ к которому осуществляется через соответствующий интерфейс;

Обеспечить доступ к блокчейну и как следствие отправку подписанной транзакции, синхронизацию балансов и других данных. Доступ к блокчейну осуществляется через специализированные узлы. Доступ к ним может быть как через серверную, так и напрямую из мобильного приложения в основном по протоколу RPC [2]. Так как рассматривается создание децентрализованного кошелька, то необходимо найти и реализовать взаимодействие с узлами для всех поддерживаемых блокчейнов непосредственно в мобильном приложении;

Обеспечить подсчет наиболее удачных комиссий. Необходимо реализовать алгоритмы подсчёта комиссий на основе данных с узлов и из других открытых API для каждого из поддерживаемых блокчейнов;

Синхронизировать список транзакций. Для каждого из поддерживаемых блокчейнов реализовать синхронизацию транзакций пользователя из эксплореров;

Предоставить информацию о текущих курсах криптовалют. Необходимо периодически синхронизировать данные о курсах;

Выбрать базу данных для хранения и удобного использования синхронизированный данных;

Создать наиболее удобный и минимизирующий количество возможных ошибок пользовательский интерфейс.

Таким образом, можно отметить, что мобильные криптовалютные кошельки являются неотъемлемой частью криптовалютной экосистемы, а их реализация требует учета многих аспектов.

Список использованных источников:

1. Custodial vs. Non-Custodial Wallets [Электронный ресурс]. – Режим доступа: https://academy.binance.com/en/articles/custodial-vs-non-custodial-wallets-what-s-the-difference – Дата доступа: 06.04.2023.

2. Remote Procedure Call [Электронный ресурс]. – Режим доступа: https://www.techtarget.com/searchapparchitecture/definition/Remote-Procedure-Call-RPC – Дата доступа: 06.04.2023.