Asuoki Messenger

Константин Ключников

13 апреля 2022 года

Цель этого текста - дать первое описание Asuoki Messenger и рассказать о его работе.

Вступление

Asuoki Messenger - это мессенджер, ориентированный на безопасность и конфиденциальность личных данных пользователя при общении через интернет. В основе мессенджера лежит технология блокчейн, которая обеспечивает функцию общения напрямую, без серверов и других 3-их устройств.

Содержание

1. Краткое объяснение работы мессенджера.

Asuoki Messenger – это комбинация возможных мер защиты личной информации в интернете. Она дает возможность общаться в интернете напрямую, без серверов, при этом, сохраняя анонимность и защиту личных данных. Комбинация состоит из следующих компонентов:

- Asuoki Blockchain – блокчейн (см. главу 2), основанный на консенсусе PoA или Proof-of-authority, позволяющий контролировать тех, кто находится внутри сети.
- Криптосистема Asuoki Messenger – криптосистема с открытым ключом (см. главу 3), которая служит для получения/отправки сообщений и последующей их шифровке/дешифровке.
- Способ взаимодействия с блокчейном — это способ, обеспечивающий отправку и отображение полученных сообщений, которые может прочитать пользователь. (см. главу 4).

При прочтении текста вы можете увидеть, что для облегчения повествования используется обозначение Алисы и Боба. Это два разных пользователя, которые созданы для того, чтобы на практике показать, что будет делать программа в определенных ситуациях.

2. Asuoki Blockchain

2.1. Описание.

Asuoki Blockchain – это способ общения двух компьютеров в интернете напрямую, без посредников. Между пользователями создается блокчейн-соединение, позволяющее отправлять и получать сообщения, которые будут храниться в блоках блокчейна.

Сам блокчейн является частным — это означает, что попасть в него могут только, кошельки (пользователи), которые прописаны в файле конфигурации обоих узлов.

2.2. Proof-of-authority консенсус

Proof-of-authority (PoA) — это консенсус, который предложил в 2014 году один из создателей Ethereum Гэвин Вуд. Он основан не на вычислительных способностях компьютера (PoW) или на количестве монет на кошельке (PoS), а на «заслуге» и рейтинге валидатора.

В Asuoki Messenger PoA используется для создания закрытого блокчейн-соединения между компьютерами в сети. У узла 1 (Пользователь Алиса) при формировании нового чата для общения, генерируется новый файл конфигурации, в котором прописан кошелек узла 2 (Пользователь Боб), с которым он будет общаться. Попытка злоумышленника попасть внутрь блокчейн-соединения будет неудачной, так как его узел (кошелек ETH) не прописан в файле конфигурации Алисы и Боба.

Для того чтобы злоумышленник смог проникнуть ему нужно:

- Взломать компьютер Алисы и Боба и переписать файлы конфигурации, при этом сам блокчейн, сбросится до генезис-блока, что означает потерю всех данных и сообщений.

- Получить доступ к кошельку Алисы или Боба и использовать их ключ для подключения к блокчейн-соединению.

2.3. Способ отправки сообщений через блокчейн.

Сообщения Алисы в зашифрованном виде попадают в новый блок, который считывает узел Боба и поле «input» нового блока, хранящий сообщение. При этом сам блок сохраняется на компьютер, поэтому получить доступ ко всей переписке можно оффлайн с любого из двух компьютеров (Алисы или Боба).

2.4. Формат сообщений

Сообщения, попадающие в новый блок, имеют один и тот же вид:

1. Длина публичного ключа и подписи — поле, служащее для того, чтобы программа автоматически, после проверки, срезала ненужную часть информации и оставляла только зашифрованное сообщение.

2. Публичный ключ - служит для проверки подписи сообщения. Подробнее об этом в 3.3.

3. Подпись зашифрованного сообщения — это подпись зашифрованного сообщения публичным ключом, описанным выше. Подробнее об этом в 3.3.

4. Зашифрованное сообщение с помощью алгоритма RSA – это оригинальное сообщение Алисы Бобу, зашифрованное с помощью алгоритма RSA. Подробнее об этом в 3.2.

Для удобства представления я перевел весь формат сообщений в графический вид:

Длина публичного ключа + подпись	Публичный ключ	Подпись зашифрованного сообщения	Зашифрованное сообщений с помощью алгоритма RSA

2.5. Возможности расширения функционала

В наших планах создать систему, которая позволит Алисе отправлять любые файлы Бобу напрямую, без серверов, будь то фотографии или архивы в несколько гигабайт.

3. Криптосистема Asuoki Messenger

Криптосистема Asuoki Messenger — криптосистема с открытым ключом, использующая алгоритм RSA и алгоритм хеширования переменной Keccak-256.

3.1. Шифрование сообщений

В Asuoki Messenger сообщения шифруются с помощью определенного алгоритма:

- Криптографический алгоритм с открытым ключом RSA – это один из двух алгоритмов, использующихся в Asuoki Messenger.

- Keccak-256 (SHA-3) - алгоритм хеширования переменной разрядности, разработанный группой авторов во главе с Йоаном Дайменом. В Asuoki Messenger используется Keccak-256k1, с помощью которого происходит подпись сообщения.

3.2. Алгоритм RSA

Алгоритм RSA — это криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Процесс шифровки/дешифровки происходит следующим образом:

1. Алиса создает новый чат, используя QR-код Боба, в котором находится публичный ключ Боба.

2. Алиса шифрует сообщение публичным ключом Боба, подписывает с помощью своего приватного ключа (см. 3.3.) и отправляет его Бобу.

3. Боб, при получении сообщения, проверяет его подпись (см. 3.3.) и, если подпись действительна, дешифрует сообщение с помощью своего приватного ключа RSA. После этого он может прочитать дешифрованное сообщение, отправленное Алисой.

3.3. Алгоритм подписи сообщений Keccak-256

В Asuoki Messenger используется Keccak-256k1. Он служит для подписи зашифрованного, с помощью алгоритма RSA сообщения. При отправке Алисой сообщения Бобу, Алиса подписывает зашифрованное алгоритмом RSA сообщение, с помощью своего приватного ключа. При получении сообщения, Боб действует по определенному алгоритму:

1. Боб проверяет было ли оно подписано приватным ключом кошелька Алисы. Делает он это, беря публичный ключ из сообщения (см. 2.3.) и конвертирует его в кошелёк.

    - Боб сверяет полученный адрес кошелька с адресом кошелька Алисы и, если полученным им кошелёк совпадает с кошельком Алисы, он переходит ко второму шагу.

2. Боб проверяет было ли сообщение подписано публичным ключом Алисы.

    - Если проверка оказывается удачной Боб расшифровывает сообщений своим приватным ключом RSA.

    - Если проверка оказывается неудачной, то Бобу выдается сообщение, что кошелёк, с которого была произведена отправка, не является кошельком Алисы и доверять ему нельзя.

4. Взаимодействие с блокчейн-соединением.

Для взаимодействия с сервером в других мессенджерах используется сайт. При отправке сообщений они шифруются с помощью определенных криптографических протоколов/алгоритмов. Однако в Asuoki Messenger мы не отправляем сообщения на сервер. Вместо этого мы отправляем сообщения на прослушивающий канал связи между блокчейн-соединением и сайтом, посредством Web3. При этом нам не нужно будет создавать сайт, доступный для всех в Интернете. Вместо этого мы будем создавать локально запущенный сайт, доступ к которому будет только у компьютера, на котором запущен веб-сервер. Это решает сразу 2 потенциальные угрозы (4.1).

4.1. Потенциальные угрозы и локальный сайт, как их решение.

Как уже упоминалось выше, взаимодействие с блокчейн-соединением происходит через локально созданный веб-сайт. С помощью этого мы предотвращаем несколько видов атак, целью которых является получение доступа к нашей переписке. Дальше будут приведены виды атак и способы их решений:

1. **«Атака посредника»** - это вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. При этом использование локально созданного веб-сервера, решает эту проблему, так как злоумышленник не может просмотреть исходящий трафик от сайта до блокчейн-соединения.

2. **Перехват незашифрованных сообщений между веб-сервером и блокчейн-соединением.** Если веб-сервер (сайт), будет отправлять в программу незашифрованные сообщения, то есть шанс того, что злоумышленник, получив доступ к локальной сети, сможет перехватывать сообщения и считывать их. Для этого сообщения шифруются внутри сайта, при этом в блокчейн-соединение отправляется полностью готовое сообщение к отправке, подходящее к формату сообщения (см. 2.3.). Таким образом, даже если злоумышленник сможет получить доступ к локальной сети, он не сможет перехватывать сообщения в незашифрованном виде.

Поэтому Вы можете не беспокоиться об угрозе взлома сайта и перехвата незашифрованных сообщений, которые подвергают опасности ваши личные данные.

5. Вывод.

Вы прочитали описание, возможно, первого, полностью автономного децентрализованного мессенджера, который создавался не ради использования новой технологии блокчейн ставшей популярной в 2021 году. Он создавался, чтобы дать пользователям возможность полностью контролировать их сообщения и не бояться, что за их мыслями, словами и поступками, может следить любой человек. Я надеюсь, что это изобретение будет долго служить верой и правдой любому человеку, который будет его использовать, и, возможно, с помощью него мы получим свободу, о которой грезим очень давно.