ChainChat

Blockchain messenger

www.ChainChat.Info

2017

ChainChat

Blockchain messenger

Область проекта

Средства коммуникации в сети Интернет.

Описание проекта

ChainChat - отказоустойчивая платформа на основе блокчейн, для обмена сообщениями с обеспечением приватности и сохранением неизменной истории сообщений.

Обоснование

В современных агрессивных информационных условиях, требуется надежное и независимое от третьих лиц средство доставки сообщений. На данный момент не существует доступного сервиса полностью решающего данную проблему.

Концепция проекта

Проект ChainChat предлагает:

- Обмен текстовыми сообщениями и файлами
- Подписка на широковещательные рассылки
- Хранение неизменной непротиворечивой истории
- Шифрование содержимого сообщений и адресатов
- Функционирование в децентрализованной сети на технологии блокчейн
- Собственная криптовалюта для премиум-функций и поддержки майнеров

Цель проекта

Реализовать систему обмена сообщениями с обеспечением приватности и сохранением неизменной истории. Предоставить документированное API системы для использования сторонними разработчиками.

Задачи проекта

- Проведение рекламной компании:
  - Разработка сайта
  - Участие в конференциях и проведение семинаров
  - Ведение темы на форуме BitCoinTalk.org

- Привлечение финансирования
  - Проведение ICO, продажа токенов
  - Выход на биржи криптовалют

- Проектирование и дизайн:
  - Структура блокчейна
  - Протокол взаимодействия между узлами
  - Разработка приложения (Desktop + Mobile):
  - Разработка мессенджера
  - Разработка кошелька
  - CPU-майнер (solo и pool)

Решения базирующиеся на централизованном подходе

Средства обмена сообщениями, базирующиеся на централизованной обработке и хранении информации, имеют единую точку отказа, поэтому более уязвимы чем децентрализованные решения. Централизованная реализация потенциально подвержена давлению государственных структур или влиятельных коммерческих организаций.

Данный подход, к примеру, используется в VK, Facebook, Telegram, WeChat.

Решения базирующиеся на децентрализованном подходе

Под децентрализованным подходом будем понимать следующее - обработка и хранение информации на большом количестве равноправных узлов, объединенных в общую сеть. При достаточно большом количестве независимых узлов такой подход более надежен чем централизованный, и более предпочтителен для создания независимой площадки обмена и рассылки сообщений.

Примеры:

CryptoCat - приватный p2p чат

Skype, Jitsi - IP-телефония, с возможностью работы в пиринговых сетях

BitTorrent - обмен файлами через p2p

Децентрализованная непротиворечивость

При децентрализованном подходе информация хранится во множестве экземпляров, что приводит к проблеме возможной противоречивости информации. Решение данной проблемы с сохранением децентрализации обеспечивает технология блокчейна. Данная технология предоставляет механизм консенсуса и поэтому обеспечивает децентрализованное хранение непротиворечивой информации.

На каждом узле сети хранится полная копия блокчейна, поэтому каждый имеет доступ ко всем данным. Для обеспечения приватности требуется дополнительное шифрование пользовательских данных в блокчейне.

В настоящий момент имеются несколько прототипов систем обмена сообщениями на базе блокчейна:

ECHO - приватный блокчейн-мессенджер в стадии разработки, не обеспечивает сохранение истории, многие функции под вопросом

Ethychat - чат на платформе Ethereum, не обеспечивает приватность

Технические детали

Аккаунт пользователя - определяется приватным ключом, который хранится только у него. Этим ключом пользователь авторизует свои действия, которые могут быть проверены с помошью его публичного ключа.

Беседа, чат - канал связи, доступ к которому имеет определённая группа пользователей. Доступ к беседе предоставляется через два приватных ключа - один на чтение, другой на запись. Беседа создаётся пользователем, доступ к беседе предоставляется передачей другим пользователям соответствующих приватных ключей (возможно только одного ключа - на чтение).

Широковещательная рассылка - беседа, приватный ключ на чтение которой публично известен.

Подтверждение блоков работает по гибридной схеме Proof of Work + Proof of Stake.

Внутри платформы вводится собственная криптовалюта - ChainChatCash (X3C). Она может использоваться для оплаты премиум-функций (большие сообщения, отправка файлов), для вознаграждения майнеров и владельцев мастер-нодов, а также для механизма Proof of Stake.

Оплата премиум-функций поглощает определённое количество валюты. Эмиссия валюты осуществляется в виде награды за добавление блока, размер награды зависит от общего количества валюты (чем меньше валюты, тем больше награда).

Требования к проекту

Функциональные требования:

- Чтение/Запись блокчейна
- Регистрация пользователя
- Создание приватной беседы, чата
- Создание публичной рассылки
- Отправка/Приём сообщений
- Предоставление API для других мессенджеров

Не функциональные требования:

- Обеспечение качества и надежности производится за счет максимального полного покрытия кода авто тестами.
- Надежность и безопасность обеспечивается криптографическим протоколом ZK-SNARK, Bitcoin Core
- Обеспечение пропускной способности с возможностью масштабирования. Для комфортной работы пользователя время доставки сообщения не должно превышать 3-5 секунд.
- Необходимо обеспечить кроссплатформенность (Windows, Linux)
- Исходный код и документация размещена в системе контроля версий (git)
- Использование библиотек и других сторонних ресурсов только с открытыми лицензиями (GPL)

Профили заинтересованных лиц

Средства массовой информации - положительно заинтересованы в независимой площадке для публикации новостей

Коммерческие компании - положительно заинтересованы в установлении подтверждённых двусторонних соглашений и обмене информации, представляющей коммерческую тайну

Частные лица - положительно заинтересованы в надёжном приватном канале общения

Биржи - положительно заинтересованы в торговле криптовалютой ChainChat

Майнеры - положительно заинтересованы в добыче криптовалюты ChainChat

Государственные структуры – неоднозначно (отрицательно) заинтересованы в криптовалюте и СМИ без контроля с их стороны

Контрольные точки

Написание Whitepaper	02.2018
Создание беседы (треда) на BitCoinTalk.org	03.2018
Анализ актуальности и востребованности	03.2018
Создание минимального прототипа продукта (MVP)	06.2018
Разработка сайта и рекламной стратегии	06.2018
Проведение семинаров и реклама проекта	09.2018
Привлечение финансирования (проведение ICO, продажа токенов)	09.2018
Формирование команды (разработчики ПО, дизайнеры, юристы)	10.2018
Проектирование и дизайн архитектуры (Структура блокчейна, Протокол взаимодействия между узлами)	01.2018
Разработка приложения Desktop + Mobile (Мессенджер, кошелёк, CPU-майнер)	02.2019
Запуск платформы	06.2019
Привлечение пользователей	07.2019
Выход на биржи криптовалют	09.2019
Дальнейшее развитие и поддержка	12.2019