Оглавление

[Введение 3](#_Toc136041461)

[Блокчейн-оракул 3](#_Toc136041462)

[Принцип работы 4](#_Toc136041463)

[Виды блокчейн-оракулы 5](#_Toc136041464)

[Проблемы использования блокчейн-оракулов 6](#_Toc136041465)

[Применение 6](#_Toc136041466)

[Проекты, развивающие оракул-блокчейн 7](#_Toc136041467)

[Будущее блокчейн-оракулов 9](#_Toc136041468)

[Создание смарт-контракта 9](#_Toc136041469)

[Библиографический список: 13](#_Toc136041470)

[Листинг смарт-контракта 14](#_Toc136041471)

## Введение

Блокчейн-технология - это распределенная база данных, которая хранит информацию в виде блоков, связанных между собой цепочкой. Она обеспечивает безопасность и прозрачность хранения данных, а также позволяет их быстро и эффективно обрабатывать.

Блокчейн-технология нашла применение в различных отраслях, включая финансы, здравоохранение, логистику, государственное управление и многие другие. В финансовой отрасли блокчейн используется для обеспечения безопасности и прозрачности финансовых транзакций, а также для создания новых видов цифровых валют, таких как биткоин. В здравоохранении блокчейн используется для хранения медицинских данных и обеспечения безопасности их обработки. В логистике блокчейн используется для отслеживания товаров и контроля их перемещения. В государственном управлении блокчейн используется для создания электронных голосований и обеспечения безопасности государственных данных.

В целом, блокчейн-технология имеет огромный потенциал для применения в различных отраслях, и блокчейн-оракул может стать одним из ключевых инструментов для обеспечения безопасности и прозрачности обработки данных в этих отраслях.

## Блокчейн-оракул

Оракулы — это объекты, которые получают и защищают внешние данные для блокчейнов, позволяя смарт-контрактам взаимодействовать с внешними системами.

Говорили, что греко-римские оракулы древности обладали особой силой, позволяющей им действовать как божественный переводчики, чтобы просвещать простых людей относительно склонностей их богов. В мире Web3 и технологий, связанных с блокчейном, оракулы выполняют аналогичные функции, но вместо того, чтобы доверять их словам, оракулы блокчейна подтверждают свои данные доказательствами. То есть оракулы блокчейна управляются данными и защищены криптографическими примитивами, которые обеспечивают максимальную прозрачность и поддающуюся проверке безопасность.

Проще говоря, оракулы — это объекты, которые служат мостами от блокчейн-экосистем к внешним источникам данных. Оракулы обращаются к веб-API или другим внешним источникам для получения свежих данных, поскольку смарт-контракты изначально не выполняют эти функции. Публичные блокчейны записывают транзакции и хранят публичные копии истории реестра блокчейнов. Новые транзакции подтверждаются пакетами или блоками с использованием различных механизмов консенсуса, используемых участниками их узлов, а смарт-контракты позволяют без проблем выполнять транзакции без доверия и фиксировать их в публичном реестре, приведено в [1].

## Принцип работы

Большинство операций в децентрализованных приложениях совершается с помощью смарт-контрактов. Для того, чтобы выполнить некоторые действия — например, рассчитать точное соотношение цены при обмене одной монеты на другую, им нужны данные из внешних источников, таких как платформы-агрегаторы и биржи.

Но смарт-контракт не может получить информацию, которая находится за пределами блокчейна. Тогда на помощь приходит оракул: он запрашивает, проверяет и аутентифицирует все показания внешних источников, а затем отправляет их в смарт-контракт.

Передача котировок криптовалюты — не единственная задача, которую решают оракулы. Их можно использовать для самых разных целей, от предоставления информации об авиарейсах в режиме реального времени до управления «умным домом». Таким образом, блокчейн-оракулы помогают интегрировать блокчейн-технологии в повседневную жизнь и приблизить их массовое принятие, приведено в [2].

## Виды блокчейн-оракулы

Оракулов разделяют по разным критериям: принципу работы, источникам получаемых данных и их направлению, а также по форме организации. Ниже — самые популярные типы.

1. Программные и аппаратные: первые берут данные из цифровых источников: баз данных, серверов, облачных хранилищ, и транслируют ее адресату в реальном времени. Аппаратные собирают данные с помощью физических устройств: «умных» датчиков, чипов, сканеров штрих-кодов, RFID-меток и так далее
2. Входящие и исходящие: оракулы могут иметь конкретную специализацию — или передавать информацию, или получать из внешних источников. Это может быть необходимо для повышения уровня надежности и решения проблемы единой точки отказа.
3. Централизованный и децентрализованный: централизованный оракул управляется единым оператором, который обычно использует его в своем же приложении. Этот тип оракулов появился первым, однако из-за проблем с уязвимостями такой системы криптоиндустрия постепенно перешла на стандарт децентрализованных блокчейн-оракулов. Это системы, объединяющие множество оракулов. Из него выбирается группа нод, каждый оракул которой выполняет свой «участок» запроса. Первым проектом, который реализовал принцип децентрализованных блокчейн-оракулов, стал Chainlink.
4. Контрактно-ориентированные: дорогостоящий и трудоемкий тип, при котором отдельный оракул обслуживает конкретный смарт-контракт. Если необходимо развернуть несколько умных контрактов, то понадобиться разработать равноценное количество оракулов.
5. Кроссчейн-совместимые: сервисы, предназначенные для передачи данных между различными блокчейнами. Решают проблему несовместимости сетей между собой. Могут быть полезны для децентрализованных приложений, использующих кроссчейн-операции, например перевод одного криптоактива в другой.
6. Вычислительные: специальные оракулы, задача которых — производить ресурсоемкие вычисления, которые нецелесообразно выполнять в блокчейне из-за технических и финансовых ограничений, приведено в [3].

## Проблемы использования блокчейн-оракулов

Главная проблема использования блокчейн-оракулов заключается в том, что атаки, взломы и другие воздействия на них напрямую отражаются на работе смарт-контрактов. Например, при помощи атаки Сивиллы злоумышленники могут выдавать себя за большое количество пользователей и манипулировать данными, которые отправляются в контракт.

Кроме того, на данный момент в индустрии нет никаких общепринятых стандартов для разработки блокчейн-оракулов. Если создатель оракула сэкономит на проверке кода аудиторами и допустит несколько серьезных ошибок, последствия будут драматическими, приведено в [2].

## Применение

Сегодня оракулов в криптоиндустрии используют для передачи потоков данных, в частности ценовых фидов. Последние представляют собой таблицу со списком значений цен на разные даты и их источником. Фиды позволяют смарт-контрактам получать котировки криптовалют с централизованных торговых платформ и агрегаторов торгов.

Например, в проекте для блокчейн-оракулов под названием Band по состоянию на июнь 2022 года поддерживаются референсные цены на 75 криптовалют, и у каждой из них свой набор источников. Например, цену Cosmos (ATOM) получают путем агрегирования котировок из CoinGecko, CryptoCompare, CoinMarketCap, Binance, Huobi Pro и Coinbase Pro.

Технологию оракулов используют в алгоритмических стейблкоинах. Один из примеров — Ampleforth. Цена стабильной монеты AMPL поддерживается за счет модели ребалансировки (Rebase). Чтобы удержать привязку к доллару в соотношении 1:1, число стейблкоинов в кошельках держателей постоянно меняется пропорционально рыночной цене AMPL.

Для этого оракулы Chainlink поставляют в протокол Ampleforth агрегированные данные о цене торговой пары AMPL/USD из нескольких агрегаторов. Кроме того, оракулы также передают протоколу текущее значение индекса потребительских цен в США, полученное из официальных источников, что позволяет учитывать при ребалансировке инфляцию доллара.

Источники данных не ограничиваются приложениями, связанными с криптоиндустрией. В зависимости от назначения программы, где они используются, оракулы можно соединить с источником, который предоставляет, например, статистику о погоде или индексе потребительских цен в отдельно взятой стране или генерации случайных чисел, приведено в [3].

## Проекты, развивающие оракул-блокчейн

1. Chainlink — признанный лидер на рынке децентрализованных блокчейн-оракулов. У проекта нет собственного блокчейна, поэтому он разворачивает ноды в сетях, приложения которых обслуживает. На сегодняшний день оракулы Chainlink работают в Ethereum, Solana и EVM-совместимых блокчейнах, а экосистема проекта включает более 1300 приложений и платформ.
2. Band Protocol – второй по величине поставщик оракулов. В отличие от Chainlink, он имеет собственный блокчейн BandChain, который управляется сетью валидаторов. Band работает с приложениями в сетях Celo, Oasis и Cronos, и развивает инструменты для разработчиков WebAssembly, которые позволяют создавать оракулов.
3. Протокол Reality.eth (ранее RealityKeys) получил широкую известность благодаря своему простому, уникальному дизайну и функциональности. Основная его идея заключается в создании новых источников данных для смарт-контрактов, а не в использовании уже существующих. Когда смарт-контракту требуются данные, протоколу задается вопрос, на который могут ответить пользователи. Ответ принимается, если он не оспорен никем другим. Если спор не решен, вопрос передается внешнему арбитру — обычно эту роль играет децентрализованный суд Kleros.
4. Hivemind (ранее Truthcoin) — один из немногих существующих оракулов, который поддерживает блокчейн Биткоина (BTC) и использует сайдчейн для снижения вычислительного воздействия на основную сеть.
5. Kylin Network – децентрализованный блокчейн-оракул и платформа с инфраструктурой данных для DeFi и Web3. Kylin Network работает на базе фреймворка Polkadot Substrate, приведено в [2].
6. Berry Data — система оракулов в сети BNB Chain. При запросе офчейн-данных операторы оракулов Berry Data соревнуются за передачу данных в специальный «банк данных» (Berry data bank), доступный для всех приложений на BNB Chain. В апреле 2022 года насчитывала около 170 интеграций.
7. DIA (Decentralised Information Asset) — кроссчейн-совместимая информационная платформа с открытым исходным кодом, которая которая обеспечивает доступ к проверенным рыночным данным для децентрализованных приложений. В проекте есть свой токен управления DIA, приведено в [3].

## Будущее блокчейн-оракулов

Блокчейн-оракулы значительно упрощают коммуникацию между смарт-контрактами и внешним миром, поэтому они крайне важны для массового принятия блокчейн-технологий.

В последнее время интерес к этой области растет. А значит, в будущем можно ожидать появления новых децентрализованных оракулов, которые потенциально устранят большинство системных рисков блокчейн-экосистемы и сделают ее более безопасным и надежным пространством, приведено в [2].

## Создание смарт-контракта

1. Подключаем сеть Sepolia. В данной работе Sepolia подключалась при помощи сайта ChainList, приведено в [4]. На рисунке 1 изображен выбор нужной валюты на сайте. Данные изображены на рисунке 2.

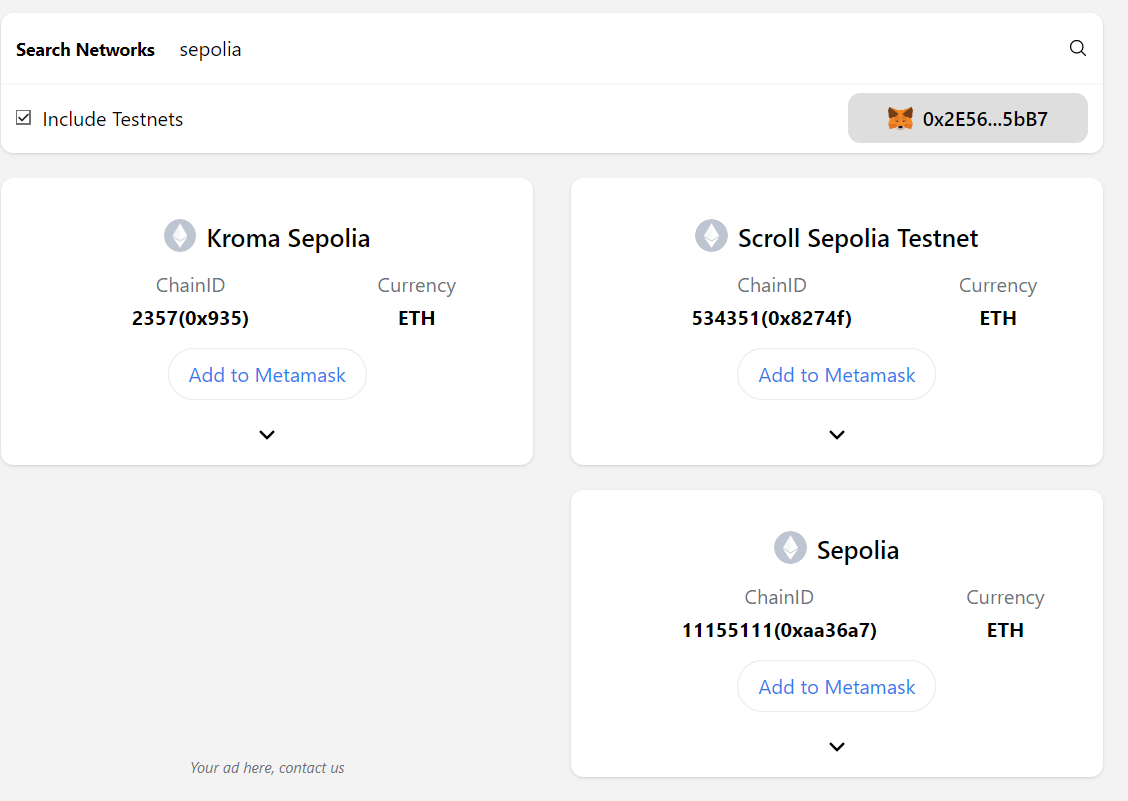


Рис. 1.

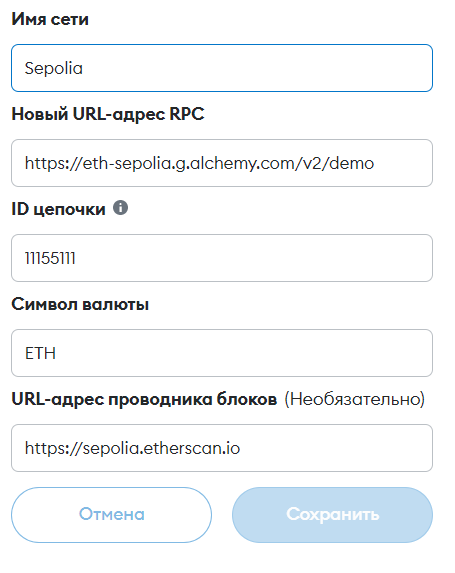


Рис. 2.

1. Добавляем токен LINK в MetaMask.
2. Реализуем смарт-контракт «Курс биткоина в долларах США»:
   1. Импортируем интерфейс блокчейн-оракула:

import "@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol";

* 1. Переходим на сайт ChainLink для получения адреса оракула, приведено в [5]. На рисунке 3 изображен фрагмент сайта, содержащий нужную валюту.

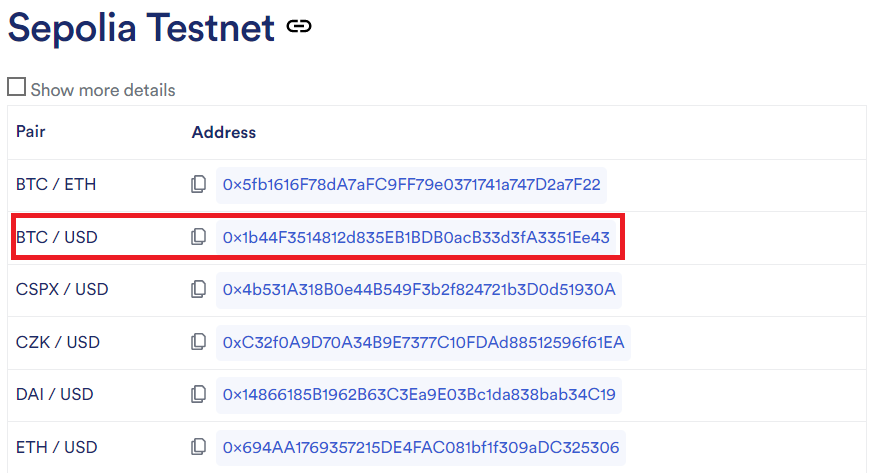


Рис. 3.

* 1. Пишем функцию для получение данных о текущем курсе.

function getBitcoinPrice() public view returns (int) {

// Получаем последнюю цену биткоина от оракула

(, int price, , , ) = priceFeed.latestRoundData();

return price;

}

* 1. Компилируем контракт.
  2. Выбираем среду MetaMask. Под ней должна быть указана валюта – Sepolia, приведено на рисунке 4.



Рис. 4.

* 1. После успешного развертывания контракта и перед запросом функции, пополняем развернутый контракт на 0.1 link, приведено на рисунке 5.

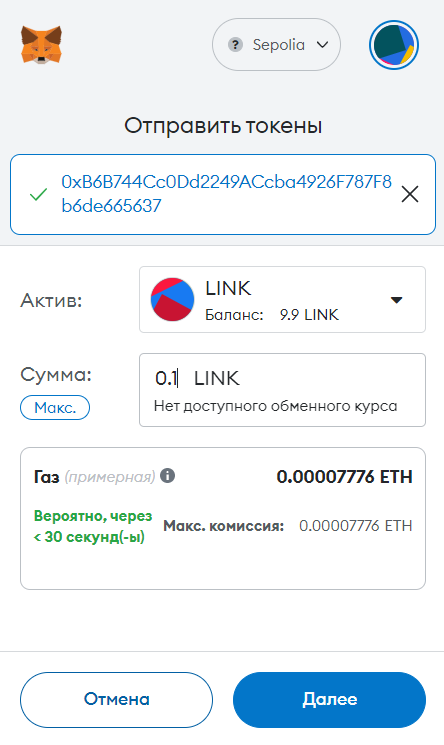


Рис. 5.

* 1. Вызываем функцию.
  2. Сравниваем полученный результат с реальным курсом, приведено на рисунках 6 и 7.



Рис. 6. Полученный результат

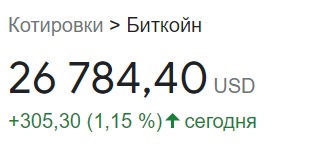


Рис. 7. Реальный курс

Объяснение результата: наш смарт-контракт не поддерживает значение с плавающей запятой.

## Библиографический список:

1. Платформа vc.ru. Что такое Оракулы? Объяснение технологии блокчейн. - URL: <https://vc.ru/crypto/593313-chto-takoe-orakuly-obyasnenie-tehnologii-blokcheyn#:~:text=Оракулы%20—%20это%20объекты%2C%20которые%20получают,контрактам%20взаимодействовать%20с%20внешними%20системами>.
2. Образовательный контент BeInCrypto. Что такое блокчейн-оракул: объясняем простыми словами. – URL: <https://ru.beincrypto.com/learn/what-is-blockchain-oracle/#:~:text=Блокчейн-оракул%20—%20это%20алгоритм%2C,и%20нужным%20ему%20источником%20информации>.
3. Медиакомпания ForkLog. Что такое блокчейн-оракул? – URL: <https://forklog.com/cryptorium/chto-takoe-blockchain-oracle>
4. ChainList. – URL: <https://chainlist.org>
5. ChainLink. – URL: <https://docs.chain.link/data-feeds/price-feeds/addresses>

## Листинг смарт-контракта

pragma solidity ^0.8.7;

// Импортируем интерфейс блокчейн-оракула

import "@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol";

contract BitcoinPriceOracle {

// Создаем переменную для хранения адреса оракула

AggregatorV3Interface internal priceFeed;

// Конструктор контракта

constructor() {

// Устанавливаем адрес оракула для получения данных о курсе биткоина в долларах США

priceFeed = AggregatorV3Interface(0x1b44F3514812d835EB1BDB0acB33d3fA3351Ee43);

}

// Функция для получения текущего курса биткоина

function getBitcoinPrice() public view returns (int) {

// Получаем последнюю цену биткоина от оракула

(, int price, , , ) = priceFeed.latestRoundData();

return price;

}

}