УДК 004.7.371:3.614

# ТЕХНОЛОГИЯ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ «СЕТИ БЛОКЧЕЙН»

Вишняков В.А., Юй Ч.Ю.

*Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь*

vish@bsuir.by

В докладе описывается лабораторный цикл при постановке дисциплины «Сети блокчейн» на кафедре ИКТ БГУИР. Обсуждается использование инфокоммуникационных технологий в рамках сети блокчейн для обеспечения хранения данных, исследуется комбинация различных подходов для развертывания смарт-контрактов. Представлены концепция и технологии, связанные с блокчейн Ethereum 2, помогающие понять фундаментальную логику и ее операционные механизмы. Описаны четыре лабораторные работы, две из них по разработке и развертыванию смарт-контрактов.

Ключевые слова: сеть блокчейн; лабораторные работы; Metamask; Remix, Truffle; Solidity; умный контракт.

*Введение.* Сеть блокчейн – это одноранговая сеть (P2P), образованная несколькими компьютерами (узлами), соединяющимися друг с другом по распределенному протоколу [1]. В сети блокчейн обеспечивает децентрализованное хранение данных и управление ими посредством совместного использования и ведения распределенной бухгалтерской книги, известной как цепочка блоков. По сути, блокчейн – это общедоступная распределенная база данных, способная хранить постоянно растущий зашифрованный реестр. Данные связаны друг с другом в виде блоков, причем каждый блок содержит серию записей транзакций. Эта технология обладает такими характеристиками, как децентрализация, открытость, устойчивость к несанкционированному доступу, анонимность и отслеживаемость [2].

*Краткие сведения по блокчейн*. Любой участвующий пользователь или устройство в блокчейн-сети называется узлом. Эти узлы обладают характеристиками открытости, распределения и автономии, образуя плоскую топологию для связи без центральной точки.

Подтверждение транзакции происходит, когда пользователь инициирует транзакцию, транслируя ее по всей сети. Другие узлы сети подтверждают действительность транзакции с помощью алгоритмов консенсуса. Как только набор транзакций подтвержден, они упаковываются в новый блок в процессе, известном как майнинг, а конкретные узлы, выполняющие операции проверки блока, называются майнерами. Каждый блок виден каждому участнику сети, и до тех пор, пока он не будет проверен и подтвержден более чем 51 % одноранговых узлов, эти блоки не могут быть добавлены, заменены или подделаны, обеспечивая безопасность блокчейна.

Каждая блокчейн-сеть выполняет различные операции, основанные на наборе определенных правил, известных как консенсус. В настоящее время существуют два основных механизма консенсуса: Proof of Work (PoW) и Proof of Stake (PoS). Доказательство работы диктует, что узел должен решить сложную математическую задачу нахождения хэша нового блока с несколькми нулями в начале быстрее, чем другие узлы, чтобы квалифицироваться как майнер. Proof of Stake оптимизирует механизм Proof of Work, гарантируя, что узлы с высокой вычислительной мощностью не обязательно станут майнерами; вместо этого узлы должны участвовать в сети и владеть определенным количеством токенов, чтобы претендовать на генерацию и утверждение блоков. Сети могут быть классифицированы как общедоступные или частные в зависимости от приложений и механизмов доступа. Известные блокчейн-сети включают Bitcoin, Ethereum, Hyperledger и другие.

*Лабораторные работы.* Разработаны четыре лабораторные работы по курсу «Сети блокчейн». Первая работа знакомит студентов с установкой сети Ethereum. Вторая лабораторная работа посвящена установке кошелька Ethereum и работе с ним. В третьей и четвертой лабораторных работах, связанных с разработкой и написанием смарт-контрактов, производится выбор блокчейн-платформы, развертывание смарт-контрактов и тестирование разными средствами.

*Выбор среды.* Учитывая потребность в прозрачных и программируемых автоматизированных решениях для хранения данных, выбрана версия блокчейн 2.0. Блокчейн 2.0 объединяет Ethereum со смарт-контрактами для достижения более широкого спектра сценариев и обработки приложений за пределами финансового сектора, поддерживая консенсус PoS. Ethereum [3] – это блокчейн-платформа с открытым исходным кодом, которая включает в себя проверенные технологии и механизмы из Blockchain 1.0, такие как асимметричное шифрование, вычисление хэша, механизмы консенсуса и протоколы P2P. Она также внедряет свои инновации, включая виртуальную машину и смарт-контракты. Сеть Ethereum нацелена на поддержку разработки и развертывания смарт-контрактов и децентрализованных приложений (dApps). Solidity, язык программирования в Ethereum для написания смарт-контрактов, является объектно-ориентированным языком, похожим на JavaScript, поддерживающим разработку программного кода по Тьюрингу (с организацией разветвлений и циклов).

*Смарт-контракты* – это автоматизированные контракты, выполняемые в сети блокчейн, содержащие заранее определенные правила и условия. Они пишутся на специальных языках программирования и хранятся по адресам смарт-контрактов в блокчейне. С контрактной точки зрения смарт-контракты можно рассматривать как «автономных агентов», предназначенных для выполнения протоколов путем реагирования на определенную информацию или коды транзакций. С вычислительной точки зрения «смарт-контракты» – это программы, способные выполнять множество заданных пользователем функций перехода состояний, включая выполнение и хранение информации. В отличие от традиционных контрактов, смарт-контракты направлены не только на выполнение общих условий контракта, но и на минимизацию злонамеренных и случайных исключений, снижая зависимость от доверенных посредников.

В 3-й и 4-й лабораторных работах авторы использовали смарт-контракты двумя способами. В первом подходе использовался кошелек Metamask Ethereum и среда разработки смарт-контрактов Remix для развертывания смарт-контрактов и взаимодействия с ними. Во

втором подходе использовалась платформа разработки Truffle, основанная на среде Node.js для создания, тестирования и развертывания смарт-контрактов Ethereum. Рассмотрим их подробнее.

*Исследование.* Тематическое исследование в лабораторной работе 3: используется кошелек Metamask Ethereum и среда разработки смарт-контрактов Remix. Пусть компания разрабатывает простое децентрализованное приложение для записи информации о домашних животных. Это приложение позволяет владельцам домашних животных записывать основную информацию о своих питомцах и надежно хранить эту информацию в смарт-контрактах на блокчейне. Выполняются следующие шаги:

1. Установка MetaMask кошелька Ethereum.
2. Получение токенов Ethereum с помощью Infura faucet в тестовой сети Sepolia.
3. Открытие онлайн-среды разработки Solidity IDE, Remix.
4. Создание исходного файла Solidity.
5. Написание текста смарт-контракта на языке Solidity.
6. Компилирование смарт-контракта.
7. Развернуть смарт-контракт, выбрав в среду развертывания Metamask.
8. Ответить на запросы MetaMask и перечислить плату за развертывание смарт-контракта.
9. Взаимодействование со смарт-контрактом.

Тематическое исследование в лабораторной работе 4: разработка блокчейна с использованием Truffle и Node.js. Студенты разрабатывают простое децентрализованное приложение для хранения аудио, направленное на обеспечение неизменности и прозрачности аудиофайлов с использованием технологии блокчейн. Они и могут загружать хэш-значения аудиофайлов в смарт-контракт и извлекать эти хэш-значения с помощью смарт-контракта. Целью приложения является предоставление децентрализованного, прозрачного решения для хранения аудио, позволяющего пользователям проверять целостность файлов. Выполняются следующие шаги:

1. Установка и инициализация Truffle.
2. Создание нового проекта Truffle.
3. Написание смарт-контракта.
4. Написание сценария миграции.
5. Настройка Truffle для подключения к локальной сети.
6. Составление смарт-контракта.
7. Программирование смарт-контракта в локальной сети.
8. Проверка развертывания с помощью средства Ganache.
9. Взаимодействие и работа со смарт-контрактом.

*Заключение.* Разработаны четыре лабораторные работы по курсу «Сети блокчейн». Первая работа знакомит студентов с установкой сети Ethereum. Вторая лабораторная работа посвящена установке кошелька Ethereum и работе с ним. В третьей и четвертой лабораторных работах, связанных с разработкой и написанием смарт-контрактов, производится выбор блокчейн-платформы, развертывание смарт-контрактов и тестирование разными средствами.

Дальнейшие четыре лабораторные работы будут связаны с использованием сети блокчейн для хранения и восстановления цифровых документов, а также сохранения пользовательских данных в сетях ИТ-диагностики.

**Литература**

1. Вишняков, В. А. Технология блокчейн в образовании и ИТ-медицине: модели, алгоритмы, программные средства : [монография] / В. А. Вишняков, Д. А. Качан. – Минск : РИВШ, 2023. – 184 с.

2. Zhou Wenli. Survey of P2P technologies. / Zhou Wenli,Wu Xiaofei. // Computer Engineering and Design, – Vol.27(1). – 2006. – P.76–79.

3. Buterin V. Ethereum: platform review. // Opportunities and Challenges for Private and Consortium Blockchains. 2016. – 45 p.

# TECHNOLOGY OF LABORATORY WORK IN THE DISCIPLINE «BLOCKCHAIN NETWORKS»

Vishnyakou U.A., Yu. C.Y.

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

The report describes a laboratory course in the formulation of the discipline «Blockchain Networks» at the Department of ICT of BSUIR. The use of infocommunication technologies within the blockchain network for data storage is discussed, a combination of different approaches for the deployment of smart contracts is investigated. The concept and technologies related to the Ethereum blockchain are presented, helping to understand the fundamental logic and its operational mechanisms, this is useful for the proper design, development and deployment of smart contracts.

Keywords: blockchain network; laboratory work; Metamask; Remix, Truffle; Solidity; smart contract.