Полная программа

Разработка децентрализованных приложений

Разработка децентрализованных приложений

Длительность курса: 150 часов

Модуль 1. Введение в технологию блокчейн и механизмы консенсуса

Тема 1

Обзор технологии, исторический контекст и эволюция блокчейна

Цель занятия

понимать базовые принципы работы блокчейна и его ключевые характеристики;
анализировать исторические предпосылки появления технологии и её эволюцию;
различать основные этапы развития блокчейна (от Bitcoin до современных платформ);
применять полученные знания для оценки потенциала блокчейна в различных сферах

Краткое содержание

основные понятия: блокчейн, децентрализация, криптография, распределённый реестр;
исторический контекст: от идеи цифровых денег до создания Bitcoin;
эволюция блокчейна: Bitcoin, Ethereum, смарт-контракты, dApps;
ключевые события и тренды в развитии технологии.

Тема 2

Децентрализация, неизменяемость, механизмы консенсуса // ДЗ

Цель занятия

понять принципы децентрализации и её роль в безопасности блокчейна;
анализировать свойства неизменяемости данных и их значение для аудита и доверия;
различать основные механизмы консенсуса и их применение в разных блокчейн-сетях;
оценивать устойчивость сети к атакам в зависимости от выбранного консенсуса.

Краткое содержание

децентрализация: узлы, пиринговые сети, устойчивость к цензуре;
неизменяемость: хеши, криптографические доказательства, защита от подделки;
механизмы консенсуса: базовые принципы, роль майнеров/валидаторов;
примеры уязвимостей и атак (51%, Sybil-атака).

Домашние задания

Подготовка и хранение простого смарт-контракта

Цель

Закрепить базовые навыки разработки смарт-контрактов:
- настроить рабочее окружение,
- создать минимальный контракт,
- протестировать контракт и задеплоить его в локальную сеть.

Результат: Вы получите первый рабочий проект смарт-контракта с тестами и README.

Тема 3

Доказательство работы (PoW), доказательство доли (PoS), делегированное доказательство доли (DPoS) // ДЗ

Цель занятия

понимать принцип работы алгоритма Proof of Work (PoW) и его роль в безопасности сети;
анализировать преимущества и недостатки Proof of Stake (PoS) по сравнению с PoW;
понимать механизм Delegated Proof of Stake (DPoS) и его применение в высокопроизводительных блокчейнах;
сравнивать энергозатратность, децентрализацию и скорость обработки транзакций в PoW, PoS и DPoS.

Краткое содержание

Proof of Work (PoW): майнинг, хешрейт, сложность сети; проблемы.
Proof of Stake (PoS): стейкинг, валидаторы, слэшинг; преимущества.
Delegated Proof of Stake (DPoS): голосование за делегатов, высокая пропускная способность; критика.

Домашние задания

Исследование и сравнение алгоритмов консенсуса (PoW, PoS, DPoS)

Цель

Цель:
-закрепить понимание принципов работы механизмов консенсуса Proof of Work и Proof of Stake;
-сформировать навык анализа последствий изменения данных в блокчейн-цепочке;
-отработать сравнительный анализ алгоритмов консенсуса по прикладным критериям.

Результат:
-выполнен эксперимент с изменением данных блока в модели Proof of Work и зафиксировано влияние на хэш и целостность цепочки;
-подготовлено краткое описание условий валидатора и принципа выбора валидатора в сети Ethereum после перехода на Proof of Stake;
-собрана таблица сравнения Proof of Work и Proof of Stake по энергопотреблению, скорости транзакций и безопасности;
-подготовлены выводы о различиях и применимости алгоритмов консенсуса.

Тема 4

Доказательство полномочий (PoA), доказательство важности (PoI)

Цель занятия

понимать принцип работы алгоритма Proof of Authority (PoA) и его применение в приватных блокчейнах;
анализировать особенности Proof of Importance (PoI) и его отличия от PoS;
сравнивать PoA и PoI с другими механизмами консенсуса по уровню децентрализации и эффективности;
определять сферы применения PoA (корпоративные решения) и PoI (NEM) в реальных проектах.

Краткое содержание

Proof of Authority (PoA): валидация на основе репутации узлов; использование в приватных/гибридных блокчейнах; высокая скорость, энергоэффективность; недостатки.
Proof of Importance (PoI):учет активности аккаунта, объема транзакций и «социального графа»; отличие от PoS.

Модуль 2. Криптография и безопасность в блокчейне, структуры данных

Тема 1

Криптографические принципы в блокчейне. Угрозы безопасности блокчейна и меры противодействия.

Цель занятия

объяснять роль криптографии в обеспечении безопасности блокчейна;
идентифицировать основные угрозы (атаки 51%, Sybil, double-spending);
применять методы защиты: криптографические алгоритмы, механизмы консенсуса;
анализировать реальные случаи взломов блокчейн-проектов.

Краткое содержание

базовые криптографические концепции: конфиденциальность, целостность, аутентификация;
угрозы: атаки на консенсус, смарт-контракты, приватность;
защитные меры: мультиподписи, аудит кода, форки.

Тема 2

Хэш-функции, цифровые подписи и криптография с открытым ключом // ДЗ

Цель занятия

применять хэш-функции (SHA-256, Keccak) для проверки целостности данных;
генерировать и верифицировать цифровые подписи (ECDSA);
различать симметричную и асимметричную криптографию;
использовать открытые/закрытые ключи в транзакциях.

Краткое содержание

свойства хэш-функций: детерминированность, устойчивость к коллизиям;
алгоритмы: RSA vs ECDSA, генерация ключей;
примеры: хэширование, шифрование, подпись

Домашние задания

Хэширование и подписи в контракте

Цель

Закрепить работу с криптографическими примитивами в смарт-контрактах.

Результат: Вы доработаете ваш проект из задания "Подготовка и хранение простого смарт-контракта":
- добавите проверку владельца через `msg.sender`,
- реализуете работу с хэшами,
- научитесь использовать цифровые подписи для проверки подлинности данных.

Тема 3

Деревья Меркла и их роль в блокчейне. Блоки, транзакции и модель данных блокчейна.

Цель занятия

строить деревья Меркла для оптимизации проверки данных;
анализировать структуру блока: хэдер, тело, nonce;
разбирать модель UTXO (Bitcoin) и account-based (Ethereum);
объяснять роль nonce и сложности в майнинге.

Краткое содержание

деревья Меркла: принцип работы, use-case в лёгких клиентах;
сравнение UTXO и account-based моделей;
поля блока: version, timestamp, merkl

Тема 4

Проблемы хранения и масштабируемости блокчейна

Цель занятия

оценивать ограничения размера блокчейна (storage, bandwidth);
сравнивать решения для масштабируемости: шардинг, Layer 2 (Rollups), sidechains;
анализировать компромиссы между децентрализацией и производительностью.

Краткое содержание

проблемы: рост размера цепи, скорость синхронизации;
решения: Pruning, State Channels, Optimistic/ZK-Rollups;
примеры: Ethereum 2.0, Polygon, Lightning Network.

Модуль 3. Функциональная совместимость блокчейнов и решения для масштабирования

Тема 1

Протоколы межсетевого взаимодействия (например, Polkadot, Cosmos)

Цель занятия

объяснять концепцию интероперабельности блокчейнов;
сравнивать архитектуры на примере Polkadot (парачейны) и Cosmos (зоны и хабы);
понимать механизмы кросс-чейн передачи данных (IBC, XCMP);
анализировать преимущества и риски гетерогенных сетей.

Краткое содержание

Polkadot: релейная цепь, парачейны, номинаторы;
Cosmos: Tendermint, Cosmos SDK, Inter-Blockchain Communication (IBC);
use-case: децентрализованные биржи (Osmosis), кросс-чейн DeFi.

Тема 2

Решения для масштабирования уровня L2 (например, Lightning Network, Plasma)

Цель занятия

различать подходы L2: state channels, sidechains, Rollups;
понимать устройство Lightning Network;
оценивать компромиссы Optimistic vs ZK-Rollups;
понять принцип Plasma и его ограничения.

Краткое содержание

Lightning Network: off-chain транзакции, hash-time locks;
Rollups: Arbitrum (Optimistic) vs zkSync (ZK);
примеры: снижение комиссий в Ethereum, мгновенные платежи.

Тема 3

Технологии повышения конфиденциальности (например, доказательства с нулевым разглашением, кольцевые подписи)

Цель занятия

понимать работу доказательств с нулевым разглашением (ZKP) для верификации данных;
понимать алгоритм кольцевых подписей (например Monero или другой);
сравнить zk-SNARKs и zk-STARKs;
анализировать анонимность в сети (Zcash, Tornado Cash).

Краткое содержание

ZKP: базовые принципы
кольцевые подписи: принцип работы

Тема 4

Проблемы и будущие направления масштабируемости блокчейна

Цель занятия

выявлять узкие места в современных решениях (централизация валидаторов в Rollups);
прогнозировать тренды: модульные блокчейны (Celestia), DAG-структуры;
понимать гибридные подходы для баланса безопасности и скорости.

Краткое содержание

проблемы: стоимость данных в L2, ликвидность в мостах;
новые парадигмы: sovereign rollups, EigenLayer;
кейсы: Near Protocol's sharding, Ethereum danksharding.

Модуль 4. Конфиденциальность и анонимность в блокчейне

Тема 1

Анонимность и псевдонимность в блокчейне // ДЗ

Цель занятия

различать понятия анонимности и псевдонимности в контексте блокчейна;
анализировать методы деанонимизации транзакций;
оценивать уровень приватности в различных блокчейнах;
понять базовые методы повышения анонимности.

Краткое содержание

псевдонимность Bitcoin: адреса как псевдонимы, анализ цепочек транзакций;
технологии настоящей анонимности: кольцевые подписи (Monero), zk-SNARKs (Zcash);
инструменты анализа блокчейна: как деанонимизируют пользователей;
практические методы защиты приватности.

Домашние задания

Криптография и безопасность в блокчейне

Цель

Закрепить практические навыки работы с хэш-функциями и цифровыми подписями, а также понять базовые угрозы безопасности блокчейнов на примере локальной симуляции.

Результат:
- реализуете хэширование и ЭЦП в коде,
- соберёте простейшую модель блока и цепочки,
- смоделируете и проанализируете риски и способы противодействия.

Тема 2

Вопросы конфиденциальности в корпоративных блокчейн-решениях

Цель занятия

понять необходимость конфиденциальности в корпоративных блокчейнах;
освоить технологии защиты: конфиденциальные смарт-контракты, нулевое разглашение;
оценивать компромиссы между прозрачностью и конфиденциальностью;
анализировать кейсы использования.

Краткое содержание

приватные транзакции и конфиденциальные данные в корпоративных блокчейнах;
технологии: zero-knowledge proofs (ZKP), secure multi-party computation (sMPC);
регулирование и compliance: GDPR и блокчейн;

Модуль 5. Механика узлов в публичных, частных и корпоративных блокчейнах

Тема 1

Запуск узла Bitcoin // ДЗ

Цель занятия

понимать архитектуру сети Bitcoin и роль полных узлов;
разворачивать Bitcoin Core-узел с нуля;
настраивать конфигурационные файлы и параметры синхронизации;
анализировать потребление ресурсов (CPU, RAM, дисковое пространство).

Краткое содержание

различия между полными узлами и майнерами;
требования к оборудованию и ПО;
процесс загрузки и верификации блокчейна;
базовые команды для мониторинга узла.

Домашние задания

Взаимодействие с Bitcoin: публичный API/собственная нода

Цель

Закрепить практические навыки работы с сетью Bitcoin через JSON-RPC API.

Результат:
- создадите набор скриптов для чтения данных из блокчейна и отслеживания транзакций,
- освоите работу с публичными API и взаимодействие с собственной нодой (при достаточных ресурсах),
- получите понимание инфраструктуры Bitcoin

Тема 2

Запуск узла Ethereum // ДЗ

Цель занятия

различать типы узлов Ethereum (архивные, полные, легкие);
настраивать шлюз для синхронизации с сетью;
подключаться к тестовой сети и mainnet;
мониторить статус синхронизации и использование ресурсов.

Краткое содержание

клиенты Ethereum
режимы синхронизации (snap, fast, full);
работа с JSON-RPI API;
использование Infura как альтернативы локальному узлу.

Домашние задания

Запуск и базовое взаимодействие с узлом Ethereum

Цель

Закрепить практические навыки запуска и настройки узла Ethereum, а также взаимодействия с сетью через JSON-RPC API.

Результат:
- вы поднимете локальный узел (или настроите подключение к Infura),
- напишете скрипт для получения данных из блокчейна Ethereum,
- получите базовый опыт мониторинга состояния сети.

Тема 3

Запуск узла Solana // ДЗ

Цель занятия

понимать архитектуру Solana и роль валидаторов;
настраивать валидаторный узел с помощью solana CLI;
участвовать в тестовой сети (testnet);
анализировать требования к оборудованию (SSD, GPU).

Краткое содержание

отличия Solana от Ethereum (PoH, Tower BFT);
настройка валидатора и делегирование стейка;
мониторинг производительности и логирование.

Домашние задания

Запуск узла Solana и базовое взаимодействие с сетью

Цель

Закрепить практические навыки запуска узла Solana и работы с сетью через Web3.js.

Результат:
- вы поднимете локальный узел или подключитеськ публичному RPC Devnet,
- напишете скрипты для взаимодействия с сетью (создание аккаунтов, транзакции, мониторинг),
- получите базовый опыт работы с экосистемой Solana.

Тема 4

Запуск узла Near // ДЗ

Цель занятия

разворачивать NEAR-узел (RPC или валидатор);
участвовать в staking pool;
настраивать мониторинг через Near CLI;
анализировать экономику газа в NEAR.

Краткое содержание

шардинг в NEAR (Nightshade);
разница между валидаторами и RPC-узлами;
управление аккаунтом через near-cli.

Домашние задания

Запуск узла NEAR и базовое взаимодействие с сетью

Цель

Закрепить практические навыки запуска узла NEAR и взаимодействия с сетью через RPC и NEAR-CLI.

Результат:
- вы развернёте узел NEAR (или подключитесь к testnet RPC),
- освоите базовые команды NEAR-CLI,
- напишете скрипт для отправки транзакций и мониторинга аккаунта.

Тема 5

Запуск узла Ton // ДЗ

Цель занятия

понимать архитектуру TON;
настраивать полный узел или lite-клиент;
взаимодействовать с сетью через Ton CLI;
анализировать скорость синхронизации.

Краткое содержание

компоненты TON: validator, collator, storage provider;
настройка конфигурации для mainnet/testnet;
использование TonAPI для запросов.

Домашние задания

Запуск узла TON и базовое взаимодействие с сетью

Цель

Закрепить практические навыки работы с сетью TON: подключение к публичному RPC или запуск собственного узла, взаимодействие с аккаунтами и транзакциями.

Результат:
- вы подключитесь к тестовой сети TON или развернёте локальный узел,
- создадите аккаунт и выполните транзакцию,
- освоите базовые инструменты TON Web API.

Тема 6

Запуск узла Hyperledger // ДЗ

Цель занятия

разворачивать Fabric-сеть с несколькими peer-узлами;
настраивать каналы и chaincode;
управлять членством через MSP (Membership Service Provider);
анализировать различия с публичными блокчейнами.

Краткое содержание

архитектура Hyperledger Fabric: ordering service, CA;
развертывание сети;
приватные данные и gossip-протокол.

Домашние задания

Развертывание сети Hyperledger Fabric и базовое взаимодействие

Цель

Закрепить практические навыки развертывания сети Hyperledger Fabric и работы с транзакциями в частном блокчейне.

Результат:
- вы развернёте тестовую сеть Hyperledger Fabric с помощью Docker,
- выполните базовые операции (создание канала, деплой смарт-контракта),
- напишете скрипт для отправки транзакций и чтения данных.

Модуль 6. Bitcoin сервисы и смартконтракты

Тема 1

Запуск ordinals на узле bitcioin

Цель занятия

понимать концепцию Ordinals и их отличие от традиционных Bitcoin-транзакций;
настраивать Bitcoin-узел для работы с Ordinals;
создавать и инскрайбить цифровые артефакты;
анализировать влияние Ordinals на сеть Bitcoin.

Краткое содержание

технология Ordinals: инскрайбинг данных в сатоши;
требования к узлу (версия Bitcoin Core, настройки);
инструменты: ord CLI, кошельки для работы с Ordinals;
примеры использования.

Тема 2

Пишем смартконтракт на Solidity и деплоим в блокчейн ethereum, часть 1

Цель занятия

разрабатывать смарт-контракты на Solidity (ERC-20, ERC-721);
тестировать код с помощью Hardhat/Truffle;
деплоить контракты в testnet и mainnet;
взаимодействовать с контрактами через web3.js/ethers.js.

Краткое содержание

структура контракта: функции, модификаторы, события;
безопасность: reentrancy, overflow/underflow;
gas оптимизация;
использование OpenZeppelin Libraries.

Тема 3

Пишем смартконтракт на Solidity и деплоим в блокчейн ethereum, часть 2

Цель занятия

разрабатывать смарт-контракты на Solidity (ERC-20, ERC-721);
тестировать код с помощью Hardhat/Truffle;
деплоить контракты в testnet и mainnet;
взаимодействовать с контрактами через web3.js/ethers.js.

Краткое содержание

структура контракта: функции, модификаторы, события;
безопасность: reentrancy, overflow/underflow;
gas оптимизация;
использование OpenZeppelin Libraries.

Тема 4

Пишем смартконтракт на Rust и деплоим в блокчейн solana, часть 1 // ДЗ

Цель занятия

настраивать среду разработки;
разрабатывать программы Solana (аналог смарт-контрактов);
работать с PDA (Program Derived Addresses);
деплоить в devnet и взаимодействовать через TypeScript.

Краткое содержание

модель аккаунтов в Solana;
обработка CPI (Cross-Program Invocations);
тестирование с помощью Anchor Tests.

Домашние задания

Пишем смарт-контракт на Rust и деплоим в Solana (часть 1)

Цель

Закрепить базовые навыки разработки программ Solana на Rust с использованием Anchor.

Результат:
- вы настроите среду разработки,
- разработаете простую программу на Rust,
- работаете с PDA (Program Derived Addresses),
- деплоите программу в Devnet и вызываете её через TypeScript.

Тема 5

Пишем смартконтракт на Rust и деплоим в блокчейн solana, часть 2 // ДЗ

Цель занятия

настраивать среду разработки;
разрабатывать программы Solana (аналог смарт-контрактов);
работать с PDA (Program Derived Addresses);
деплоить в devnet и взаимодействовать через TypeScript.

Краткое содержание

модель аккаунтов в Solana;
обработка CPI (Cross-Program Invocations);
тестирование с помощью Anchor Tests.

Домашние задания

Пишем смарт-контракт на Rust и деплоим в Solana (часть 2)

Цель

Закрепить углублённые навыки разработки программ Solana на Rust с использованием Anchor.

Результат:
- получить опыт работы с моделью аккаунтов в Solana,
- реализовать межпрограммные вызовы (CPI),
- написать тесты через Anchor Tests,
- задеплоить контракт в Devnet и вызывать его через TypeScript.

Тема 6

Пишем смартконтракт на Rust и деплоим в блокчейн near, часть 1 // ДЗ

Цель занятия

использовать NEAR SDK для Rust;
разрабатывать контракты с persistent storage;
работать с кросс-контрактными вызовами;
деплоить в testnet и mainnet.

Краткое содержание

модель аккаунтов и storage staking;
callback-функции;
gas и performance оптимизация.

Домашние задания

Пишем смартконтракт на Rust и деплоим в блокчейн NEAR (часть 1)

Цель

Закрепить базовые навыки разработки смарт-контрактов NEAR на Rust.

Результат :
- вы настроите NEAR SDK для Rust,
- разработаете контракт с persistent storage,
- выполните деплой в testnet,
- вызовете контракт через NEAR-CLI и/или JavaScript SDK.

Тема 7

Пишем смартконтракт на Rust и деплоим в блокчейн near, часть 2 // ДЗ

Цель занятия

использовать NEAR SDK для Rust;
разрабатывать контракты с persistent storage;
работать с кросс-контрактными вызовами;
деплоить в testnet и mainnet.

Краткое содержание

смартконтракт на языке Rust для Near

Домашние задания

Пишем смартконтракт на Rust и деплоим в блокчейн NEAR (часть 2)

Цель

Закрепить расширенные навыки разработки смарт-контрактов NEAR на Rust.

Результат
- вы поработаете с моделью аккаунтов и storage staking,
- реализуете callback-функции,
- оптимизируете контракт по расходу gas,
- выполните деплой в testnet, при желании в mainnet.

Тема 8

Пишем смартконтракт на FuncC и деплоим в блокчейн ton, часть 1

Цель занятия

настраивать среду разработки для FunC;
разрабатывать смарт-контракты для TON Blockchain;
работать с TVM (TON Virtual Machine);
деплоить контракты через TonCLI.

Краткое содержание

структура контракта в TON;
сообщения и их обработка;
управление gas в TON.

Тема 9

Пишем смартконтракт на FuncC и деплоим в блокчейн ton, часть 2

Цель занятия

настраивать среду разработки для FunC;
разрабатывать смарт-контракты для TON Blockchain;
работать с TVM (TON Virtual Machine);
деплоить контракты через TonCLI.

Краткое содержание

структура контракта в TON;
сообщения и их обработка;
управление gas в TON.

Тема 10

Пишем смартконтракт на JS и деплоим в блокчейн hyperledger, часть 1

Цель занятия

разрабатывать chaincode (аналог смарт-контрактов) на JavaScript;
настраивать приватные каналы в Hyperledger Fabric;
тестировать chaincode в локальной сети.

Краткое содержание

архитектура chaincode;
работа с CouchDB как state database;
управление доступом.

Тема 11

Пишем смартконтракт на JS и деплоим в блокчейн hyperledger, часть 2 // ДЗ

Цель занятия

разрабатывать chaincode (аналог смарт-контрактов) на JavaScript;
настраивать приватные каналы в Hyperledger Fabric;
тестировать chaincode в локальной сети.

Краткое содержание

архитектура chaincode;
работа с CouchDB как state database;
управление доступом.

Домашние задания

Конфиденциальность и анонимность в блокчейне

Модуль 7. Проектирование и дизайн

Тема 1

Дизайн пользовательского интерфейса (UI) и пользовательского опыта (UX) // ДЗ

Цель занятия

применять принципы UI/UX-дизайна к dApps;
проектировать пользовательские потоки для работы с криптокошельками;
оптимизировать интерфейсы под мобильные и веб-версии;
анализировать лучшие практики ведущих DeFi/NFT-проектов.

Краткое содержание

особенности UX в Web3: работа с транзакциями, gas fee, подписями;
инструменты: Figma, Adobe XD для прототипирования;
кейсы: Uniswap, MetaMask, OpenSea;
доступность и инклюзивность в dApps.

Домашние задания

Дизайн пользовательского интерфейса (UI) и пользовательского опыта (UX) в dApps

Цель

Закрепить умение анализировать пользовательский опыт в существующих Web3-приложениях.

Результат:
- поймёте особенности UX в dApps (кошельки, gas fee, подписи),
- умеете находить проблемы интерфейсов,
- предлагаете улучшения для повышения удобства и доступности.

Тема 2

Тестирование и развертывание

Цель занятия

разрабатывать стратегии тестирования (unit, integration, e2e);
настраивать CI/CD для dApps;
деплоить фронтенд;
работать с инструментами мониторинга.

Краткое содержание

тестирование смарт-контрактов;
деплой;
мониторинг транзакций и ошибок;
пост-релизная аналитика.

Модуль 8. Проектная работа

Тема 1

Выбор темы и организация проектной работы

Цель занятия

выбрать и обсудить тему проектной работы;
спланировать работу над проектом;
ознакомиться с регламентом работы над проектом.

Краткое содержание

правила работы над проектом и специфика проведения итоговой защиты;
требования к результату проекта и итоговой документации.

Тема 2

Защита проектных работ

Цель занятия

защитить проект и получить рекомендации экспертов.

Краткое содержание

презентация проектов перед комиссией;
вопросы и комментарии по проектам.

Домашние задания

Проект