Научная программа

Разработка децентрализованных приложений

Разработка децентрализованных приложений

Длительность курса: 150 часов

Модуль 1. Введение в технологию блокчейн и механизмы консенсуса

Тема 1.
История создания, общая концепция, принципы и основы технологии Blockchain

Лекция

Перед началом изучения технологии полезным представлять работу в виде распределенной базы данных, которая называется блокчейн. Мы рассмотрим, что такое блокчейн, как устроена и основные ее свойства, а также рассмотрим основные принципы, которые лежат в основе технологии Blockchain, которая является основным и наиболее перспективным направлением развития децентрализованных приложений.

Blockchain, криптовалюта и криптовалюта Bitcoin.

Домашнее задание

Тема 2.
Децентрализованные приложения, смарт-контракты, и для чего нужны

Лекция

Перед началом изучения технологии разработки смарт-контрактов полезно понимать, что такое децентрализованное приложение и в каком месте в экосистеме, в частности, Ethereum, это приложение находится. Мы рассмотрим, что такое децентрализованное приложение и для чего Ethereum и для различных экосистем нужны смарт-контракты, а также рассмотрим основные принципы Blockchain-сети.

Децентрализованные приложения и смарт-контракты.

Домашнее задание

Исследование по теме основных механизмов Blockchain, их основных и дополнительных свойств

Тема 3.
Криптографические основы Blockchain. Алгоритмы хеширования, SHA-256 и другие. Алгоритмы шифрования, ECDSA и другие. Алгоритмы подписи, ECDSA и другие

Лекция

Перед началом изучения технологии полезно понимать, что такое криптографическая подпись, что такое хеширование, зачем нужно шифрование и какие алгоритмы для подписи, шифрования и хеширования используются в Blockchain. Мы рассмотрим, что такое криптографическая подпись, что такое хеширование, зачем нужно шифрование и какие алгоритмы для подписи, шифрования и хеширования используются в Blockchain.

Криптографические примитивы.

Домашнее задание

Тема 4.
Алгоритмы консенсуса. Proof of Work, Proof of Stake, Proof of Authority, Proof of Burn, Proof of Elapsed Time, Proof of Capacity

Лекция

Перед началом изучения технологии полезно понимать, что такое консенсус, что такое Proof of Work, Proof of Stake, Proof of Authority, Proof of Burn, Proof of Elapsed Time, Proof of Capacity, а также рассмотрим, какие алгоритмы консенсуса используются в различных Blockchain-сетях. Мы рассмотрим, что такое консенсус, что такое Proof of Work, Proof of Stake, Proof of Authority, Proof of Burn, Proof of Elapsed Time, Proof of Capacity, а также рассмотрим, какие алгоритмы консенсуса используются в различных Blockchain-сетях.

Алгоритмы консенсуса.

Домашнее задание

Модуль 2. Криптографии и безопасность в блокчейне, структуры данных

Тема 1.
Криптографические примитивы в технологии Blockchain. Алгоритмы хеширования, шифрования и подписи. Криптографическая стойкость. Криптографическая безопасность

Лекция

Перед началом изучения технологии криптографических примитивов, используемых в Blockchain, полезно понимать, какие алгоритмы используются в Blockchain, почему они используются, какие свойства они обеспечивают, что такое криптографическая стойкость, что такое криптографическая безопасность, в чем разница между криптографической стойкостью и криптографической безопасностью.

Криптографические примитивы.

Домашнее задание

Тема 2.
Хеш-функции в технологии Blockchain. Алгоритмы хеширования, SHA-256 и другие. Алгоритмы шифрования, ECDSA и другие. Алгоритмы подписи, ECDSA и другие

Лекция

Перед началом изучения технологии полезно понимать, что такое хеширование, что такое хеш-функции, какие алгоритмы используются в Blockchain, какие они обеспечивают свойства и в каком месте в экосистеме Blockchain-сетей, например, Ethereum, эти алгоритмы используются. Мы рассмотрим, что такое хеширование, что такое хеш-функции, какие алгоритмы используются в Blockchain, какие они обеспечивают свойства и в каком месте в экосистеме Blockchain-сетей, например, Ethereum, эти алгоритмы используются.

Криптографические примитивы.

Домашнее задание

Тема 3.
Структуры данных Blockchain. Merkle Tree, Merkle Patricia Tree (Ethereum), Merkle Mountain Range (Grin), Merkle Sum Tree (Cardano)

Лекция

Перед началом изучения технологии полезно представлять, какие структуры данных используются в Blockchain, почему они используются, какие свойства они обеспечивают, что такое Merkle Tree, что такое Merkle Patricia Tree (Ethereum), что такое Merkle Mountain Range (Grin), что такое Merkle Sum Tree (Cardano), а также рассмотрим, какие структуры данных используются в различных Blockchain-сетях.

Структуры данных Blockchain.

Домашнее задание

Исследование применимости в Blockchain различных для каждой Blockchain

Модуль 3. Функциональная совместимость в Blockchain и решения для масштабирования

Тема 1.
Проблемы масштабирования Blockchain. Sharding, Sidechains, Plasma, Rollup, Lightning Network, Raiden, Plasma Cash

Лекция

Перед началом изучения технологии полезно представлять, какие проблемы масштабирования есть у Blockchain, почему они возникают, какие решения предлагают такие проблемы и в каких Blockchain-сетях, например, Ethereum, эти решения используются. Мы рассмотрим, что такое шардинг, что такое сайдчейны, что такое Plasma, что такое Rollup, что такое Lightning Network, что такое Raiden, что такое Plasma Cash, а также рассмотрим, в каких Blockchain-сетях, например, Ethereum, эти решения используются.

Проблемы масштабирования и решения для масштабирования.

Домашнее задание

Тема 2.
Проблемы масштабирования Ethereum. Sharding, Casper, Plasma, Rollup, Raiden, Plasma Cash

Лекция

Перед началом изучения технологии полезно представлять, какие проблемы масштабирования есть у Ethereum, почему они возникают, какие решения предлагают такие проблемы и в каких Blockchain-сетях, например, Ethereum, эти решения используются. Мы рассмотрим, что такое шардинг, что такое Casper, что такое Plasma, что такое Rollup, что такое Raiden, что такое Plasma Cash, а также рассмотрим, в каких Blockchain-сетях, например, Ethereum, эти решения используются.

Проблемы масштабирования Ethereum.

Домашнее задание

Тема 3.
Проблемы масштабирования Bitcoin. Lightning Network, Segwit, Schnorr signature, Taproot, Bulletproofs, Mimblewimble, Cross-chain Atomic Swaps

Лекция

Перед началом изучения технологии полезно представлять, какие проблемы масштабирования есть у Bitcoin, почему они возникают, какие решения предлагают такие проблемы и в каких Blockchain-сетях, например, Bitcoin, эти решения используются. Мы рассмотрим, что такое Lightning Network, что такое Segwit, что такое Schnorr signature, что такое Taproot, что такое Bulletproofs, что такое Mimblewimble, что такое Cross-chain Atomic Swaps, а также рассмотрим, в каких Blockchain-сетях, например, Bitcoin, эти решения используются.

Проблемы масштабирования Bitcoin.

Домашнее задание

Исследование применимости в Blockchain решений для масштабирования

Модуль 4. Конфиденциальность и анонимность в блокчейне

Тема 1.
Анонимность и конфиденциальность в Blockchain. Zero Knowledge Proof

Лекция

Перед началом изучения технологии полезно представлять, что такое анонимность, что такое конфиденциальность и в чем разница между анонимностью и конфиденциальностью, что такое Zero Knowledge Proof, что такое Zero Knowledge Proof, что такое Zero Knowledge Proof, а также рассмотрим, в каких Blockchain-сетях, например, Zcash, эти решения используются.

Анонимность и конфиденциальность.

Домашнее задание

Криптографии в Blockchain и Ethereum

Тема 2.
Криптографические примитивы, используемые в технологии Blockchain. Zero Knowledge Proof, Ring Signature, Stealth Address, Pedersen Commitment, Homomorphic Encryption

Лекция

Перед началом изучения технологии полезно представлять, какие криптографические примитивы используются в Blockchain, почему они используются, что такое Zero Knowledge Proof, что такое Ring Signature, что такое Stealth Address, что такое Pedersen Commitment, что такое Homomorphic Encryption, а также рассмотрим, в каких Blockchain-сетях, например, Zcash, эти решения используются.

Криптографические примитивы.

Домашнее задание

Тема 3.
Алгоритмы криптографической подписи в Blockchain. Schnorr signature, Multisig, Threshold signature, Blind signature, Ring signature, Stealth Address

Лекция

Перед началом изучения технологии полезно представлять, какие алгоритмы криптографической подписи используются в Blockchain, почему они используются, что такое Schnorr signature, что такое Multisig, что такое Threshold signature, что такое Blind signature, что такое Ring signature, что такое Stealth Address, а также рассмотрим, в каких Blockchain-сетях, например, Bitcoin, эти решения используются.

Криптографические примитивы.

Домашнее задание

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

Тема 1.
Запуск узла Bitcoin-Core

Лекция

Перед началом изучения технологии полезно представлять, что такое узел Bitcoin, что такое Bitcoin-Core, что такое Bitcoin-Core, что такое Bitcoin-Core, что такое Bitcoin-Core, а также рассмотрим, что такое Bitcoin-Core, что такое Bitcoin-Core, что такое Bitcoin-Core, что такое Bitcoin-Core