Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Институт экономики и бизнеса

Сковиков А.Г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ТЕХНОЛОГИЯ БЛОКЧЕЙН И КРИПТОВАЛЮТА»

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Технология блокчейн и криптовалюта» / составитель: А.Г. Сковиков. - Ульяновск: УлГУ, 2019.

Настоящие методические указания предназначены для студентов бакалавриата по направлению 38.03.05 «Бизнес-информатика» (степень – бакалавр), изучающих дисциплину «Технология блокчейн и криптовалюта». В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля, кейсы и тесты для самостоятельной работы.

Студентам заочной формы обучения следует использовать данные методические указания при самостоятельном изучении дисциплины. Студентам очной формы обучения они будут полезны при подготовке к практическим занятиям и к зачету по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом Института экономики и бизнеса УлГУ (протокол № 223/09 от 27 июня 2019 г.).

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Старков, А.Н. Цифровая экономика : учебное пособие / А.Н. Старков, Е.В. Сторожева. — Москва : ФЛИНТА, 2017. — 82 с. — ISBN 978-5-9765-3697-5. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/104928.

2. Цифровое будущее или экономика счастья? [Электронный ресурс]/ А.В. Черновалов [и др.].— Электрон. текстовые данные.— М.: Дашков и К, 2018.— 218 с.— Режим доступа: http://www.iprbookshop.ru/85484.html.— ЭБС «IPRbooks».

3. Сковиков, А.Г. Цифровая экономика. Электронный бизнес и электронная коммерция : учебное пособие / А.Г. Сковиков. — Санкт-Петербург : Лань, 2019. — 260 с. — ISBN 978-5-8114-3703-0. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/119637

4. Сковиков, А.Г. Электронная коммерция: учеб. пособ. / А. Г. Сковиков. - Ульяновск: УлГУ, 2017.

5. Сковиков, А.Г. Электронная коммерция [Электронный ресурс] : учебно-методическое пособие для студентов высших учебных заведений, обучающихся по направлению подготовки: 38.04.08 – «Финансы и кредит» / А. Г. Сковиков, Р. М. Байгулов; УлГУ, ИЭиБ. - Электрон. текстовые дан. (1 файл : 4,54 Мб). - Ульяновск : УлГУ, 2018.

6. Сковиков, А. Г. Технология блокчейн и Биткоин [электронный ресурс] / режим доступа: http://www.intuit.ru/studies/courses/1007/229/info.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

ТЕМА 1. ОСНОВНЫЕ ПОНЯТИЯ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

Основные вопросы:

1. Понятие цифровых технологий и цифровой экономики. Предпосылки и последствия прямой и опосредованной цифровизации общественных отношений. Становление цифровой экономики: цифровые "волны".

2. Материальное производство и цифровая экономика. Происходящие глобальные трансформации в мировой экономике, обществе, технологиях.

3. Введение в эллиптическую криптографию.

4. Как хранить и использовать криптовалюты. Горячие и холодные хранилища.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебном пособии [4] на с. 7-8, учебном пособии [5] на с. 25-28.

Вопрос 2 рассмотрен в учебном пособии [4] на с. 9-12, учебном пособии [5] на с. 1-25.

Вопрос 3 рассмотрен в учебном пособии [6] на с. 21-37 (https://www.intuit.ru/studies/courses/3520/762/lecture/32518).

Вопрос 4 изложен в учебном пособии [6] на с. 37-43 (https://www.intuit.ru/studies/courses/3520/762/lecture/32518).

Контрольные вопросы:

1. Что такое информатизация общества?
2. В чем состоит процесс информатизации общества?
3. В чем отличия процессов информатизации и компьютеризации?
4. Что такое информационное общество?
5. Что является средствами информационной технологии?
6. Назовите этапы развития информационных технологий.
7. Как Вы понимаете тезис: Информация как экономическое благо и фактор производства.
8. Раскройте сущность информационно-коммуникационных технологий.
9. В чем состоит влияние информационно-коммуникационных технологий на глобализацию мировой экономики?
10. Раскройте понятие цифровой экономики.
11. Раскройте структуру цифровой экономики. Субъекты, объекты и институты цифровой экономики как системы.
12. Как связаны цифровая экономика и экономический рост.
13. Четвертая промышленная революция и информационная глобализация.
14. Сформулируйте основные характеристики и возможности информационной (сетевой) экономики.
15. Оцените влияние информационной экономики на участников рынка (покупатели, производители, структура коммерческих отношений).
16. В каком смысле Цифровая экономика выступает как дальнейшее развитие информационной (сетевой) экономики и новая стадия глобализации.
17. Экономические основы технологии распределенных реестров хранения информации (блокчейн).
18. Раскройте преимущества и проблемы применения блокчейна.
19. Криптовалюты: история, классификация и правовое регулирование.
20. Раскройте перспективы и риски применения криптовалют в финансовой системе государства.
21. Как происходит трансформация промышленности в цифровой экономике?

Кейсы для самостоятельной работы:

1. Дайте определение следующим базовым терминам и понятиям: Сатоши Накамото, распределенный реестр, блокчейн, криптовалюта, Биткоин, двойная трата, децентрализованные приложения, распределенные системы, приватные блокчейны, публичные блокчейны, децентрализованный консенсус, атака «человек посередине», криптография, пиринговая сеть, транзакция, майнинг, блок, высота блока, электронная подпись, сатоши, полная нода, облегченные кошельки.

Тесты для самостоятельной работы:

Раздел тестов 1.
Задание 1. Формулировка вопроса – один правильный ответ
Кому именно приписывают создание протокола Биткоин?
Ответ 1. Билл Гейтс
Ответ 2. Сатоши Накамото
Ответ 3. Питер Нортон
Ответ 4. Марк Цукерберг
Задание 2. Формулировка вопроса – один правильный ответ
Технология блокчейн обеспечивает …
Ответ 1. автоматизацию бизнес-процесса
Ответ 2. трансформацию бизнес-процесса
Ответ 3. механизацию бизнес-процесса
Ответ 4. информатизацию бизнес-процесса
Задание 3. Формулировка вопроса – один правильный ответ
Технология блокчейн устраняет следующий недостаток современных бизнес-процессов …
Ответ 1. наличие посредников
Ответ 2. невысокая скорость финансовых операций
Ответ 3. трансакционные издержки
Ответ 4. неразвитость информационной инфраструктуры
Раздел тестов 2.
Задание 1. Формулировка вопроса – один правильный ответ
Применение технологии блокчейн в любых сферах будет экономически выгодным и технологически оправданным?
Ответ 1. Да
Ответ 2. Нет
Задание 2. Формулировка вопроса – один правильный ответ
Является ли точным и корректным определение «блокчейн - распределенная база данных»?
Ответ 1. Да
Ответ 2. Нет
Задание 3. Формулировка вопроса – один правильный ответ
Можно ли утверждать, что правовые аспекты применения технологии блокчейх плохо отрегулированы?
Ответ 1. Да
Ответ 2. Нет
Раздел тестов 3.
Задание 1. Формулировка вопроса – несколько правильных ответов
Укажите препятствия на пути развития технологии блокчейн:

Ответ 1. малая пропускная способность сети

Ответ 2. постоянное увеличение размера физического хранилища, в котором хранится цепочка блоков

Ответ 3. саботаж пользователей

Ответ 4. слабая поддержка со стороны производителей аппаратного обеспечения

Задание 2. Формулировка вопроса – несколько правильных ответов

Укажите виды деятельности, благоприятные для внедрения систем на основе блокчейнов:

Ответ 1. бизнес-процессы с очень высокой интенсивностью трафика (информационных потоков)

Ответ 2. системы с высокой конфиденциальностью, например, финансовые отчеты коммерческих предприятий (корпораций)

Ответ 3. регистрация актов гражданского состояния

Ответ 4. кадастровая деятельность

Задание 3. Формулировка вопроса – несколько правильных ответов

Укажите основные тренды цифровой экономики, проявившие себя в технологии блокчейн:

Ответ 1. формируется на стыке нескольких разнонаправленных видов деятельности, науки, экономики

Ответ 2. способствует локализации бизнес-деятельности

Ответ 3. исключает посредников

Ответ 4. существенным образом зависит от человеческого фактора

Раздел тестов 4.

Задание 1. Формулировка вопроса – несколько правильных ответов

Для каких сфер бизнеса не следует использовать блокчейн?

Ответ 1. анализ данных

Ответ 2. внутренний документооборот компании

Ответ 3. децентрализованная торговля

Ответ 4. голосование

Задание 2. Формулировка вопроса – несколько правильных ответов

Для каких сфер бизнеса следует использовать блокчейн?

Ответ 1. в облачных вычислениях

Ответ 2. в производстве потребительских товаров

Ответ 3. в схемах, основанных на публичных реестрах

Ответ 4. в децентрализованном учете и взаиморасчетах

Задание 3. Формулировка вопроса – несколько правильных ответов

Наличие единого, центрального сервера, копирующего свои данные на вспомогательные серверы, говорит о том, что …

Ответ 1. в системе не используется блокчейн

Ответ 2. в системе используется частный блокчейн

Ответ 3. мы имеем дело с распределенной базой данных

Ответ 4. в системе используется публичный блокчейн

Раздел тестов 5.

Задание 1. Формулировка вопроса – один правильный ответ

Какой класс систем является наиболее представительным (большим)?

Ответ 1. распределенные системы

Ответ 2. децентрализованные системы.

Ответ 3. блокчейны

Ответ 4. криптовалюты

Задание 2. Формулировка вопроса – один правильный ответ

В иерархии децентрализованных распределенных систем блокчейнам непосредственно предшествует класс …

Ответ 1. распределенных систем

Ответ 2. централизованных систем
Ответ 3. децентрализованных систем
Ответ 4. криптовалют
Задание 3. Формулировка вопроса – один правильный ответ
Децентрализованные приложения …
Ответ 1. расширяют возможности сети Интернет
Ответ 2. сужают возможности сети Интернет
Ответ 3. работают независимо от сети Интернет
Ответ 4. не изменяют возможности сети Интернет
Раздел тестов 6.
Задание 1. Формулировка вопроса – один правильный ответ
Какую задачу впервые удалось решить с помощью платформы Биткоин?
Ответ 1. двойных трат
Ответ 2. анонимности платежей
Ответ 3. электронных платежей
Ответ 4. масштабируемости платежных систем
Задание 2. Формулировка вопроса – один правильный ответ
Дефляционный характер криптовалюты Биткоин объясняется …
Ответ 1. виртуальным характером монет
Ответ 2. отсутствием центрального, управляющего звена
Ответ 3. строго ограниченным числом монет, подлежащих выпуску
Ответ 4. высокой волатильностью курса
Задание 3. Формулировка вопроса – один правильный ответ
В сети Биткоин полностью открыты …
Ответ 1. протокол Биткоин и программный код базового клиента Bitcoin Core
Ответ 2. только протокол Биткоин
Ответ 3. только программный код базового клиента Bitcoin Core
Ответ 4. только API (Application Programming Interface - интерфейс программных приложений) функции
Раздел тестов 7.
Задание 1. Задание с вводом правильного числового или текстового значения
Сколько всего будет выпущено биткоинов?
Ответ 1. 21 000 000
Задание 2. Задание с вводом правильного числового или текстового значения
Укажите год завершения эмиссии биткоинов …
Ответ 1. 2 140
Задание 3. Задание с вводом правильного числового или текстового значения
Сколько сатоши в одном BTC?
Ответ 1. 100 000 000
Раздел тестов 8.
Задание 1. Формулировка вопроса – один правильный ответ
Можно ли менять данные в блокчейне?
Ответ 1. Да
Ответ 2. Нет
Задание 2. Формулировка вопроса – один правильный ответ
Может ли уменьшаться число блоков в блокчейне?
Ответ 1. Да
Ответ 2. Нет
Задание 3. Формулировка вопроса – один правильный ответ
Можно ли нарушать хронологический порядок при добавлении блоков?
Ответ 1. Да
Ответ 2. Нет

Раздел тестов 9.

Задание 1. Формулировка вопроса – один правильный ответ

В каких блокчейнах генерация новых блоков осуществляется централизованным образом?

Ответ 1. приватных

Ответ 2. публичных

Ответ 3. сайдчейнах

Ответ 4. стейблкоинах

Задание 2. Формулировка вопроса – один правильный ответ

Достоинством закрытых блокчейнов является …

Ответ 1. прозрачность данных и процессов

Ответ 2. полный контроль над системой со стороны всех ее участников

Ответ 3. потенциально высокая пропускная способность системы

Ответ 4. повышенный уровень безопасности и надежности системы

Задание 3. Формулировка вопроса – один правильный ответ

Достоинством открытых блокчейнов является …

Ответ 1. высокий уровень доверия со стороны пользователей

Ответ 2. низкая стоимость транзакций

Ответ 3. высокая скорость подтверждения транзакций

Ответ 4. более контролируемая и прогнозируемая среда для реализации бизнес-функций

Раздел тестов 10.

Задание 1. Формулировка вопроса – один правильный ответ

С помощью какого средства осуществляется управление биткоинами?

Ответ 1. криптографических ключей

Ответ 2. кредитных карт

Ответ 3. банковских счетов

Ответ 4. токенов

Задание 2. Формулировка вопроса – один правильный ответ

Что является необходимым и достаточным условием для работы с платежной системой Биткоин?

Ответ 1. наличие биткоинов

Ответ 2. наличие фиатных денег

Ответ 3. наличие установленного клиента сети Биткоин

Ответ 4. наличие аккаунта на криптовалютной бирже

Задание 3. Формулировка вопроса – один правильный ответ

Биткоин является …

Ответ 1. одноранговой платежной системой

Ответ 2. платежной системой с процессинговыми центрами

Ответ 3. многополярной платежной системой

Ответ 4. клиент-серверной платежной системой

Раздел тестов 11.

Задание 1. Формулировка вопроса – один правильный ответ

Для достижения консенсуса в сети Биткоин используется механизм?

Ответ 1. Proof of Work

Ответ 2. Proof of Stake

Ответ 3. Proof of Capacity

Ответ 4. Proof of Activity

Задание 2. Формулировка вопроса – один правильный ответ

С помощью какого инструмента обеспечивается высочайшая отказоустойчивость сети Биткоин?

Ответ 1. сеть Интернет

Ответ 2. управляющие центры
Ответ 3. децентрализация
Ответ 4. прозрачность взаимодействия
Задание 3. Формулировка вопроса – один правильный ответ
Перевод средств в сети Биткоин считается завершенным …
Ответ 1. только после включения в блокчейн нового блока с соответствующей транзакцией
Ответ 2. сразу после завершения операции в программе-клиенте пользователя
Ответ 3. после отправки соответствующей транзакции в сеть
Ответ 4. по прошествии 12-ти часового периода времени
Раздел тестов 12.
Задание 1. Формулировка вопроса – один правильный ответ
Кто занимается сборкой блоков в сети Биткоин?
Ответ 1. майнеры
Ответ 2. администраторы
Ответ 3. все пользователи сети
Ответ 4. блокировщики
Задание 2. Формулировка вопроса – один правильный ответ
Временной интервал между двумя блоками в блокчейне сети Биткоин составляет в среднем …
Ответ 1. 1 минуту
Ответ 2. 5 минут
Ответ 3. 10 минут
Ответ 4. 30 минут
Задание 3. Формулировка вопроса – один правильный ответ
Каким образом в каждом новом блоке учитывается вся предыстория блокчейна, включая блок генезиса?
Ответ 1. путем вставки в новый блок ссылки на хеш предыдущего блока
Ответ 2. путем электронного подписания каждого нового блока
Ответ 3. путем нумерации блоков
Ответ 4. путем вставки в новый блок ссылок на все предыдущие блоки
Раздел тестов 1.
Задание 1. Формулировка вопроса – один правильный ответ
Закрытые криптографические ключи в сети Биткоин …
Ответ 1. выдаются в удостоверяющих центрах
Ответ 2. генерируются и хранятся в кошельках
Ответ 3. распространяются по сети
Ответ 4. хранятся в блокчейне
Задание 2. Формулировка вопроса – один правильный ответ
Для управления закрытыми криптографическими ключами в сети Биткоин …
Ответ 1. нужно обращаться к администратору сети
Ответ 2. достаточно иметь кошелек
Ответ 3. используют криптопровайдер КриптоПро
Ответ 4. используется блокчейн
Задание 3. Формулировка вопроса – один правильный ответ
Закрытый криптографический ключ в сети Биткоин – это …
Ответ 1. число
Ответ 2. кодовое слово
Ответ 3. механическое устройство
Ответ 4. комбинация цифр и символов
Раздел тестов 2.
Задание 1. Формулировка вопроса – один правильный ответ

Какой тип криптографии используется в платформе Биткоин?

Ответ 1. симметричная

Ответ 2. асимметричная

Ответ 3. гибридная

Ответ 4. стеганография

Задание 2. Формулировка вопроса – один правильный ответ

Если y = f(x) – односторонняя функция, тогда …

Ответ 1. вычислить *x*, зная *y*, невозможно в принципе

Ответ 2. вычислить *x*, зная *y*, очень сложно

Ответ 3. вычислить *y*, зная *x*, очень сложно

Ответ 4. вычислить *y*, зная *x*, невозможно в принципе

Задание 3. Формулировка вопроса – один правильный ответ

Какие ключи используются в криптосистеме с закрытым ключом …

Ответ 1. открытые и закрытые

Ответ 2. симметричные

Ответ 3. сеансовые

Ответ 4. коды аутентичности

Раздел тестов 3.

Задание 1. Формулировка вопроса – несколько правильных ответов

Если проводить аналогию между банковским чеком и транзакцией сети Биткоин, с каким реквизитом чека можно ассоциировать биткоин-адрес?

Ответ 1. имя получателя средств

Ответ 2. название банка

Ответ 3. номер банковского счета

Ответ 4. подпись на банковском чеке

Задание 2. Формулировка вопроса – несколько правильных ответов

С каким элементом традиционной платежной системы ассоциируется закрытый ключ платформы Биткоин?

Ответ 1. пин-кодом банковской карты

Ответ 2. номером банковского счета

Ответ 3. именем получателя средств

Ответ 4. личным кабинетом пользователя на сайте платежной системы

Задание 3. Формулировка вопроса – несколько правильных ответов

С каким элементом традиционной платежной системы ассоциируется открытый ключ платформы Биткоин?

Ответ 1. номером банковского счета

Ответ 2. пин-кодом банковской карты

Ответ 3. подписью на банковском чеке

Ответ 4. банковской ячейкой

Раздел тестов 4.

Задание 1. Формулировка вопроса – несколько правильных ответов

В сети Биткоин для создания криптопары используется …

Ответ 1. умножение на эллиптических кривых

Ответ 2. деление на эллиптических кривых

Ответ 3. логарифмирование на эллиптических кривых

Ответ 4. вычитание на эллиптических кривых

Задание 2. Формулировка вопроса – несколько правильных ответов

Длина закрытого ключа составляет …

Ответ 1. 256 бит

Ответ 2. 512 бит

Ответ 3. 128 бит

Ответ 4. 1024 бита

Задание 3. Формулировка вопроса – несколько правильных ответов

Укажите правильную последовательность вычислений …

Ответ 1. закрытый ключ → открытый ключ → биткоин-адрес

Ответ 2. биткоин-адрес → закрытый ключ → открытый ключ

Ответ 3. открытый ключ → закрытый ключ → биткоин-адрес

Ответ 4. закрытый ключ → биткоин-адрес → открытый ключ

Раздел тестов 5.

Задание 1. Формулировка вопроса – один правильный ответ

Укажите правильную формулу для вычисления биткоин-адреса

Ответ 1. SHA-256(RIPEMD-160(публичный ключ)

Ответ 2. SHA-256(SHA-256 (публичный ключ)

Ответ 3. RIPEMD-160(RIPEMD-160(публичный ключ)

Ответ 4. RIPEMD-160(SHA-256(публичный ключ)

Задание 2. Формулировка вопроса – один правильный ответ

Закрытый ключ …

Ответ 1. вычисляется как точка на эллиптической кривой

Ответ 2. берется из справочника

Ответ 3. вычисляется случайным образом

Ответ 4. берется из блокчейна

Задание 3. Формулировка вопроса – один правильный ответ

С помощью закрытого ключа создается

Ответ 1. электронная подпись

Ответ 2. кошелек

Ответ 3. биткоины

Ответ 4. блок

Раздел тестов 6.

Задание 1. Формулировка вопроса – один правильный ответ

Можно ли восстановить доступ к средствам в сети Биткоин после потери закрытого ключа?

Ответ 1. Да

Ответ 2. Нет

Задание 2. Формулировка вопроса – один правильный ответ

Может ли кто-то, кроме владельца закрытого ключа, контролировать средства, связанные с соответствующим биткоин-адресом?

Ответ 1. Да

Ответ 2. Нет

Задание 3. Формулировка вопроса – один правильный ответ

Можно ли подбросив 256 раз монету и записав результаты опытов в виде последовательности нулей и единиц получить правильный закрытый ключ?

Ответ 1. Да

Ответ 2. Нет

Раздел тестов 7.

Задание 1. Формулировка вопроса – один правильный ответ

В чем именно состоит недостаток традиционных (не квантовых) генераторов случайных чисел?

Ответ 1. недостаточно высокая неопределенность вычислений

Ответ 2. не позволяют генерировать большие числа

Ответ 3. медленно работают

Ответ 4. дорого стоят

Задание 2. Формулировка вопроса – один правильный ответ

Какие генераторы случайных чисел являются самыми лучшими (надежными)

Ответ 1. физические

Ответ 2. табличные

Ответ 3. квантовые

Ответ 4. алгоритмические

Задание 3. Формулировка вопроса – один правильный ответ

Какие генераторы случайных чисел используются в сети Биткоин?

Ответ 1. *штатные генераторы случайных чисел, входящие в состав операционных систем*

Ответ 2. квантовые генераторы

Ответ 3. табличные генераторы

Ответ 4. физические генераторы

Раздел тестов 8.

Задание 1. Формулировка вопроса – один правильный ответ

В эллиптической криптографии закрытый ключ можно получить из открытого ключа только …

Ответ 1. путем перебора всех возможных значений (brute force)

Ответ 2. применяя эксплойтинг

Ответ 3. применяя SQL-инъекции

Ответ 4. используя алгоритмы имитационного моделирования

Задание 2. Формулировка вопроса – один правильный ответ

Криптография на эллиптических кривых основана на

Ответ 1. проблеме дискретного логарифмирования на эллиптических кривых

Ответ 2. использовании нескольких раундов шифрования с разными ключами

Ответ 3. сложности криптоанализа при использовании объемной (многомерной) перестановки

Ответ 4. сложности криптоанализа при использовании усовершенствованного метода многозначной замены

Задание 3. Формулировка вопроса – один правильный ответ

В сети Биткоин используется эллиптическая кривая следующего вида

Ответ 1. $y^2 = x^3\ 7$

Ответ 2. $y^2 = x\ 7$

Ответ 3. $y^3 = x^3\ 7$

Ответ 4. $y^2 = x^2\ 7$

Раздел тестов 9.

Задание 1. Формулировка вопроса – несколько правильных ответов

Укажите параметры криптографического алгоритма сети Биткоин:

Ответ 1. простой модуль

Ответ 2. базовая точка

Ответ 3. скорость схождения

Ответ 4. длина кодового слова

Задание 2. Формулировка вопроса – несколько правильных ответов

Укажите основные свойства эллиптических кривых, используемые в криптографии:

Ответ 1. дискриминант уравнения эллиптической кривой не равен нулю.

Ответ 2. свойство делимости точек эллиптических кривых над конечным полем

Ответ 3. любая наклонная прямая, пересекающая эллиптическую кривую в двух точках, всегда будет пересекать ее также в третьей точке

Ответ 4. любая наклонная прямая, являющаяся касательной к кривой в одной из точек, обязательно пересечет кривую еще ровно в одной точке

Задание 3. Формулировка вопроса – несколько правильных ответов

Какие операции на эллиптических кривых используются в криптографии платформы Биткоин?

Ответ 1. сложение

Ответ 2. деление

Ответ 3. умножение

Ответ 4. вычитание

Раздел тестов 10.

Задание 1. Формулировка вопроса – один правильный ответ

Что является результатом скалярного умножения на эллиптических кривых базовой точки на значение закрытого ключа?

Ответ 1. точка на эллиптической кривой

Ответ 2. целое число

Ответ 3. вещественное число

Ответ 4. прямая линия, пересекающая эллиптическую кривую

Задание 2. Формулировка вопроса – один правильный ответ

Эллиптическая кривая симметричная относительно …?

Ответ 1. ось ординат

Ответ 2. начала координат

Ответ 3. оси абсцисс

Ответ 4. диагонали декартовой системы координат, пересекающей ее в I и III четвертях

Задание 3. Формулировка вопроса – один правильный ответ

В протоколе Биткоин базовая точка …

Ответ 1. однозначно определена и зафиксирована

Ответ 2. является случайной

Ответ 3. задается для каждого пользователя индивидуально

Ответ 4. меняется после добавления в блокчейн определенного числа блоков

Раздел тестов 11.

Задание 1. Задание с вводом правильного числового или текстового значения

Укажите сколько байт потребуется для записи открытого ключа в алгоритмах электронной подписи на эллиптических кривых в uncompressed формате:

Ответ 1. 65

Задание 2. Задание с вводом правильного числового или текстового значения

Укажите (в десятичной системе счисления) какой префикс используется для записи открытого ключа в uncompressed формате:

Ответ 1. 04

Задание 3. Задание с вводом правильного числового или текстового значения

Если 0 - точка в бесконечности и имеются две точки P и Q, имеющие координаты вида P (a, b) и Q (a, -b), тогда чему будет равно сложение на эллиптической кривой этих точек P Q ?

Ответ 1. 0

Раздел тестов 12.

Задание 1. Задание с вводом правильного числового или текстового значения

Сколько символов потребуется для записи биткоин-адреса в кодировке Base58Check?

Ответ 1. 34

Задание 2. Задание с вводом правильного числового или текстового значения

Сколько байт в двоичной записи биткоин-адреса в кодировке Base58Check составляет контрольная сумма?

Ответ 1. 4

Задание 3. Задание с вводом правильного числового или текстового значения

Сколько символов включает алфавит кодировки Base58?

Ответ 1. 58

ТЕМА 2. БЛОКЧЕЙН 1.0. КРИПТОВАЛЮТЫ НА ПРИМЕРЕ БЛОКЧЕЙНА БИТКОЙН

Основные вопросы темы:

1. Мобильная коммерция. Мобильные платежи. Методы платежа в Интернете. Развитие эквайринга. Мобильный и онлайн-эквайринг.

2. . Платежные технологии. Национальная платежная система. Эволюция платёжных систем. Современные платежные системы.

3. Распределенный консенсус. Proof of Work. Proof of Stake. Консенсус биткоина. Майнинг криптовалют. Экономика майнинга. Виды атак в сети блокчейн. Атаки на консенсус.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебном пособии [4] на с. 134-139.

Вопрос 2 рассмотрен в учебном пособии [4] на с. 178-196, учебном пособии [5] на с. 261-290.

Вопрос 3 рассмотрен в учебном пособии [6] на с. 91-116 (https://www.intuit.ru/studies/courses/3520/762/lecture/32526).

Контрольные вопросы:

1. Объясните принципы работы технологии блокчейн
2. Обзор сфер применения технологии блокчейн
3. Опишите основные этапы развития технологии блокчейн
4. Опишите основные этапы развития технологии блокчейн
5. Архитектура блокчейн-проектов
6. Назовите 3 современные криптосистемы
7. Назовите основные платформы для создания блокчейн-проектов, их отличия друг от друга

Кейсы для самостоятельной работы:

1. С помощью сервиса https://www.blockchain.com/ определите основные параметры блока блокчейна Биткоин с высотой 624535, включая хеш блока, время создания, майнера, создавшего блок, число транзакций, размер в битах, значение поля Nonce, биткоин-адрес майнера, сложность майнинга.

Тесты для самостоятельной работы:

Раздел тестов 1.
Задание 1. Формулировка вопроса – несколько правильных ответов

Какие задачи платформы Биткоин решаются с помощью майнинга?

Ответ 1. эмиссия новых коинов
Ответ 2. достижение консенсуса
Ответ 3. зашита от двойных трат

Ответ 4. обеспечение анонимности

Задание 2. Формулировка вопроса – несколько правильных ответов

Выберите из списка способы добычи (эмиссии) коинов, используемые в различных криптовалютах:

Ответ 1. ICO

Ответ 2. треккинг

Ответ 3. майнинг

Ответ 4. форжинг

Задание 3. Формулировка вопроса – несколько правильных ответов

Укажите параметры, прямо или косвенно влияющие на хешрейт криптоплатформы:

Ответ 1. особенности реализации конкретного алгоритма добычи криптовалюты

Ответ 2. особенности телекоммуникационной сети

Ответ 3. популярность криптовалюты

Ответ 4. высота блокчейна

Раздел тестов 2.

Задание 1. Формулировка вопроса – один правильный ответ

Может ли механизм Proof-of-Work защитить систему от спам-рассылок?

Ответ 1. Да

Ответ 2. Нет

Задание 2. Формулировка вопроса – один правильный ответ

Может ли механизм Proof-of-Work защитить систему от DOS-атак?

Ответ 1. Да

Ответ 2. Нет

Задание 3. Формулировка вопроса – один правильный ответ

Может ли механизм Proof-of-Work защитить систему от двойных тракт?

Ответ 1. Да

Ответ 2. Нет

Раздел тестов 3.

Задание 1. Формулировка вопроса – один правильный ответ

Можно ли описать нахождение консенсуса Proof of Work как случайный процесс с низкой вероятностью успеха?

Ответ 1. Да

Ответ 2. Нет

Задание 2. Формулировка вопроса – один правильный ответ

Награда майнерам за созданный блок уменьшается вдвое каждые пять лет?

Ответ 1. Да

Ответ 2. Нет

Задание 3. Формулировка вопроса – один правильный ответ

Механизм Proof of Work технически основан на том, что нужно не просто найти хеш блока, но еще и добиться, чтобы этот хеш отвечал очень жестким дополнительным требованиям?

Ответ 1. Да

Ответ 2. Нет

Раздел тестов 4.

Задание 1. Формулировка вопроса – один правильный ответ

Выстраивая механизм Proof of Work как средство достижения консенсуса в платформе Биткоин, Сатоши Накамото за основу взял идею проекта Hashcash (обеспечение безопасности данных за счет добавления хешей специального вида – со старшими нулевыми битами). Каким образом Сатоши Накамото развил и улучшил этот инструмент?

Ответ 1. добавил механизм самонастраивающейся сложности — изменения требуемого числа нулей, исходя из суммарной вычислительной мощности участников сети

Ответ 2. добавил валидаторов транзакций, которые посредством голосования выбирают держатели BTC

Ответ 3. добавил учет репутации участника, включая его активность

Ответ 4. добавил идею консенсуса, основанную на предоставлении дискового пространства

Задание 2. Формулировка вопроса – один правильный ответ

Согласно протокола Биткоин в 2141 году доход майнеров будет включать:

Ответ 1. комиссию за создание блоков и валидацию транзакций

Ответ 2. только комиссию за создание блоков

Ответ 3. потоянную сумму за поддержку блокчейна сети Биткоин (криптозарплата)

Ответ 4. только комиссию за валидацию транзакций

Задание 3. Формулировка вопроса – один правильный ответ

Сущность алгоритма Proof of Work определяется следующими двумя положениями:

Ответ 1. обязательное решение некоторой вычислительно сложной и длительной по времени задачи и наличие возможности быстрой и легкой проверки результата

Ответ 2. решение должно быть легко масштабируемым и исключающим наличие единого центра управления

Ответ 3. строгое математическое обоснование решения и легкость его практической реализации

Ответ 4. обязательное использование криптографических методов и использование в качестве транспортной системы – Интернет

Раздел тестов 5.

Задание 1. Формулировка вопроса – один правильный ответ

Какова наиважнейшая цель института майнинга?

Ответ 1. реализация концепции децентрализованной процессинговой системы верификации транзакций

Ответ 2. эмиссия новых коинов

Ответ 3. возможность заработка для майнеров

Ответ 4. создание альтернативы для фиатных денег

Задание 2. Формулировка вопроса – один правильный ответ

Если майнер обладает 10% суммарной вычислительной мощности сети Биткоин, то сколько он будет в среднем получать вознаграждения?

Ответ 1. 1%

Ответ 2. 5%

Ответ 3. 8%

Ответ 4. 10%

Задание 3. Формулировка вопроса – один правильный ответ

Могут ли злоумышленники похитить биткоины других пользователей?

Ответ 1. нет

Ответ 2. да, если злонамеренные майнеры получат большинство (так называемая атака 51%)

Ответ 3. да, в результате намеренного форка

Ответ 4. да, в результате реализации атаки Сивиллы

Раздел тестов 6.

Задание 1. Формулировка вопроса – один правильный ответ

Механизм консенсуса, основанный на использовании «доли» в качестве ресурса, определяющего, какая именно нода получает право добычи следующего блока, называется?

Ответ 1. Proof of Stake

Ответ 2. Proof of Importance

Ответ 3. Proof of Activity

Ответ 4. Proof of Capacity

Задание 2. Формулировка вопроса – один правильный ответ

Механизм консенсуса, основанный на использовании баланса, репутации и активности участника в качестве ресурса, определяющего, какая именно нода получает право добычи следующего блока, называется?

Ответ 1. Proof of Stake

Ответ 2. Proof of Importance

Ответ 3. Proof of Activity

Ответ 4. Proof of Capacity

Задание 3. Формулировка вопроса – один правильный ответ

Механизм консенсуса, основанный на использовании дискового пространства участника в качестве ресурса, определяющего, какая именно нода получает право добычи следующего блока, называется?

Ответ 1. Proof of Stake

Ответ 2. Proof of Importance

Ответ 3. Proof of Activity

Ответ 4. Proof of Capacity

Раздел тестов 7.

Задание 1. Формулировка вопроса – один правильный ответ

Какой механизм децентрализованного консенсуса сети Биткоин препятствует распространению недействительных транзакций?

Ответ 1. автономная верификация транзакций каждой полной нодой

Ответ 2. независимая сборка транзакций в новые блоки майнерами с обязательной демонстрацией найденного доказательства работы

Ответ 3. автономная верификация новых блоков каждой полной нодой и добавление блоков в цепочку

Ответ 4. независимый выбор каждой нодой цепочки блоков с максимальной суммарной сложностью доказательств работы

Задание 2. Формулировка вопроса – один правильный ответ

Какой механизм децентрализованного консенсуса сети Биткоин не позволяет майнерам, создающим новые блоки, неправомерно увеличить размер полагающейся им комиссии?

Ответ 1. автономная верификация транзакций каждой полной нодой

Ответ 2. независимая сборка транзакций в новые блоки майнерами с обязательной демонстрацией найденного доказательства работы

Ответ 3. автономная верификация новых блоков каждой полной нодой и добавление блоков в цепочку

Ответ 4. независимый выбор каждой нодой цепочки блоков с максимальной суммарной сложностью доказательств работы

Задание 3. Формулировка вопроса – один правильный ответ

Какой механизм децентрализованного консенсуса сети Биткоин применяется в случаях, когда несколько майнинг нод создают валидные блоки одновременно?

Ответ 1. автономная верификация транзакций каждой полной нодой

Ответ 2. независимая сборка транзакций в новые блоки майнерами с обязательной демонстрацией найденного доказательства работы

Ответ 3. автономная верификация новых блоков каждой полной нодой и добавление блоков в цепочку

Ответ 4. независимый выбор каждой нодой цепочки блоков с максимальной суммарной сложностью доказательств работы

Раздел тестов 8.

Задание 1. Формулировка вопроса – один правильный ответ

Чему равен приоритет транзакции, если ее вход ссылается на нерастраченный выход, сумма которого равна 1BTC, а транзакция, к которой он относится имеет размер

250 байт и расположена в блокчейне на глубине 1000 блоков относительно вершины блокчейна?

Ответ 1. 400 000 000
Ответ 2. 57 600 000
Ответ 3. 150 000 000
Ответ 4. 500 000 000

Задание 2. Формулировка вопроса – один правильный ответ

В 2019 году один из майнеров, в одиночку создавший новый блок, принятый сетью Биткоин, получил ровно 12,56609689 BTC комиссионных. Какая часть этой суммы приходится на комиссионные за обработку транзакций, вошедших в этот блок?

Ответ 1. 12,56609689 BTC
Ответ 2. 0,56609689 BTC
Ответ 3. 0 BTC
Ответ 4. 0,06609689 BTC

Задание 3. Формулировка вопроса – один правильный ответ

Если блок расположен в блокчейне на глубине 1000 блоков относительно вершины блокчейна, его сумма входов равна 5 BTC, а сумма выходов равна 4,5 BTC, чему будет равна сумма комиссионных за обработку транзакций, вошедших в этот блок?

Ответ 1. 0,5 BTC
Ответ 2. 9,5 BTC
Ответ 3. 0 BTC
Ответ 4. 1 BTC

Раздел тестов 9.

Задание 1. Формулировка вопроса – один правильный ответ

Как и в других транзакциях в coinbase-транзакции имеется поле «Разблокирующий скрипт»?

Ответ 1. Да
Ответ 2. Нет

Задание 2. Формулировка вопроса – один правильный ответ

Майнер имеет возможность сохранить какие-то произвольные данные (например, имя, никнейм или слоган) в coinbase-транзакции?

Ответ 1. Да
Ответ 2. Нет

Задание 3. Формулировка вопроса – один правильный ответ

Значение поля «хеш более ранней транзакции» в coinbase-транзакции равно 0 в десятичной системе счисления?

Ответ 1. Да
Ответ 2. Нет

Раздел тестов 10.

Задание 1. Формулировка вопроса – один правильный ответ

С какой переодичностью меняется значение параметра «Сложность» в платформе Биткоин?

Ответ 1. через каждые 2016 блоков
Ответ 2. через каждые 16 блоков
Ответ 3. через каждые 256 блоков
Ответ 4. через каждые 512 блоков

Задание 2. Формулировка вопроса – один правильный ответ

Уменьшение параметра «Целевая сложность (Target)» в платформе Биткоин на 1 бит приведет …

Ответ 1. к увеличению числа возможных решений (хешей) в два раза
Ответ 2. к сокращению числа возможных решений (хешей) в шестнадцать раз
Ответ 3. к увеличению числа возможных решений (хешей) в шестнадцать раз

Ответ 4. к сокращению числа возможных решений (хешей) в два раза

Задание 3. Формулировка вопроса – один правильный ответ

Изменяя какой параметр заголовка блока, майнеры добиваются хеш-функции блока требуемого формата?

Ответ 1. счетчика Nonce

Ответ 2. поля Bits

Ответ 3. параметр Target

Ответ 4. Difficulty

Раздел тестов 11.

Задание 1. Формулировка вопроса – один правильный ответ

Параметры Target и Bits (состоящий из термов order и mantissa) связаны следующим соотношением …

Ответ 1. $\text{Target} = \text{mantissa} \times 2^{((8 \times (\text{order} - 3)))}$

Ответ 2. $\text{Target} = \text{order} \times 2^{((8 \times (\text{mantissa} - 3)))}$

Ответ 3. $\text{Target} = \text{mantissa} \times 2^{((8 \times (\text{mantissa} - 3)))}$

Ответ 4. $\text{Target} = \text{order} \times 2^{((8 \times (\text{order} - 3)))}$

Задание 2. Формулировка вопроса – один правильный ответ

Параметры Difficulty и Target связаны следующим соотношением …

Ответ 1. не связанные величины

Ответ 2. равные величины

Ответ 3. прямо пропорциональные величины

Ответ 4. обратно пропорциональные величины

Задание 3. Формулировка вопроса – один правильный ответ

В платформе Биткоин …

Ответ 1. сначала рассчитывается Bitcoin Difficulty (сложность майнинга), а затем, исходя из сложности, вычисляется текущее значение Target

Ответ 2. сначала рассчитывается Target, а затем вычисляется текущее значение Bitcoin Difficulty (сложность майнинга)

Ответ 3. Target и Bitcoin Difficulty расчитываются одновременно

Ответ 4. Target и Bitcoin Difficulty вычисляются независимо друг от друга

Раздел тестов 12.

Задание 1. Формулировка вопроса – один правильный ответ

Решение Extra Nonce заключается в …

Ответ 1. добавлении к 4 байтам стандартного Nonce дополнительных 8 байт из coinbase-транзакции

Ответ 2. использовании нового формата записи значения счетчика в поле Nonce

Ответ 3. применении нового подхода к вычислению параметра Bitcoin Difficulty

Ответ 4. применении нового подхода к вычислению параметра Target

Задание 2. Формулировка вопроса – один правильный ответ

За какие валидные блоки награда майнерам не назначается?

Ответ 1. блоки, содержащие транзакции без комиссий

Ответ 2. блоки, подготовленные администраторами сети Биткоин

Ответ 3. блоки, подготовленные с помощью эталонного клиента Bitcoin Core

Ответ 4. orphan-блоки

Задание 3. Формулировка вопроса – один правильный ответ

К чему приведет сокращение, зафиксированного в протоколе Биткоин десятиминутного интервала между блоками?

Ответ 1. частому возникновению случайных форков

Ответ 2. уменьшению пропускной способности системы

Ответ 3. сокращению скорости подтверждения транзакций

Ответ 4. увеличению безопасности системы

ТЕМА 3. БЛОКЧЕЙН 2.0. УМНЫЕ КОНТРАКТЫ

Основные вопросы темы:

1. Децентрализованная Автономная Корпорация. DAPP (децентрализованное приложение). Три основных категории DAPP на платформе Ethereum (криптовалюты, приложения, интегрирующие деньги с внешними событиями в реальном мире, децентрализованные автономные организации (DAO)). Плюсы децентрализованных приложений.

Рекомендации по изучению темы:

Вопрос 1 рассмотрен в учебном пособии [6] на с. 7-13.

Контрольные вопросы:

1. Что такое DAO?
2. В чем состоят достоинства и недостатки DAPP?
3. Перечислите признаки успешного децентрализованного приложения?
4. Что такое gas?
5. Что из себя представляет структура смарт-контракта?

Кейсы для самостоятельной работы:

1. Проанализируйте следующий смарт-контракт, призванный помочь Вам разобраться с типами данных языка Solidit..

```
pragma solidity ^0.5.0;
contract SolDataTypes {
bool isReady;
string savedString;
uint savedValue;
uint8[10] boxPrice;
uint8[] dBoxPrice;
address owner;
enum doorState { Open, Closed, Blocked }
doorState myDoor;
function openDoor() public {
    myDoor = doorState.Open;
}
function closeDoor() public {
    myDoor = doorState.Closed;
}
function blockDoor() public {
    myDoor = doorState.Blocked;
}
function getDoorState() public view returns ( doorState ) {
    return myDoor;
}
constructor() public {
    owner = msg.sender;
}
function setDBoxPrice(uint8 price) public {
    dBoxPrice.push(price);
}
```

```
function getDBoxPrices() public view returns( uint8[]memory ) {
    return dBoxPrice;
}
function setBoxPrice(uint idBox, uint8 price) public {
    boxPrice[idBox] = price;
}
function getBoxPrices() public view returns( uint8[10]memory ) {
    return boxPrice;
}
function init() public {
    isReady = true;
}
function isInitialized() public view returns ( bool ) {
    return isReady;
}
function getBalance() public view returns ( uint ) {
    address myAddress = msg.sender;
    uint balance = myAddress.balance;
    return balance;
}
function setString( string memory newString ) public {
    savedString = newString;
}
function getString() public view returns( string memory ) {
    return savedString;
}
function setValue( uint newValue ) public {
    savedValue = newValue;
}
function getValue() public view returns( uint ) {
    return savedValue;
}
```

Тесты для самостоятельной работы:

Раздел тестов 1.

Задание 1. Формулировка вопроса – несколько правильных ответов

Выберите из списка этапы жизненного цикла транзакции в сети Биткоин:

Ответ 1. подписание электронной подписью

Ответ 2. проверка и включение в блок майнером

Ответ 3. микширование

Ответ 4. подсчет статистики

Задание 2. Формулировка вопроса – несколько правильных ответов

Какие элементы платежа, реализованного с помощью транзакции сети Биткоин, роднят его с банковским чеком?

Ответ 1. транзакции проверяются майнерами

Ответ 2. транзакции объединяются в блоки

Ответ 3. транзакции подписываются непосредственно владельцами средств

Ответ 4. транзакции содержат ссылки на средства других транзакций (счетов)

Задание 3. Формулировка вопроса – несколько правильных ответов

Прозрачность блокчейна в том числе заключается в том, что …

Ответ 1. каждый пользователь сети Биткоин всегда может отследить любую цепочку транзакций, фиксирующих движение конкретных биткоинов

Ответ 2. каждый пользователь сети Биткоин может внести изменения в блокчейн

Ответ 3. каждый пользователь сети Биткоин может анализировать транзакции (сделки), которые еще даже не включены в блоки

Ответ 4. каждый пользователь сети Биткоин может определить персональные данные других участников сети

Раздел тестов 2.

Задание 1. Формулировка вопроса – один правильный ответ

Что означает правило шести подтверждений?

Ответ 1. каждую транзакцию должны подтвердить шесть майнеров

Ответ 2. чтобы считать сделку завершенной, следует дождаться включения в блокчейн шести дополнительных блоков (подтверждений).

Ответ 3. дерево Меркла в блоке должно иметь не менее шести ветвей

Ответ 4. каждый блок должны подтвердить шесть майнеров

Задание 2. Формулировка вопроса – один правильный ответ

Что представляет собой атака Сивиллы?

Ответ 1. под контролем злоумышленника оказывается более 50% хешрейта

Ответ 2. узел-жертва ограничена коммуникациями только с узлами, контролируемыми злоумышленником

Ответ 3. отправка большого количества «мусорных» данных (транзакции-спам) на узел пользователя

Ответ 4. взлом хэш-функций

Задание 3. Формулировка вопроса – один правильный ответ

Анонимность расчетов в сети Биткоин …

Ответ 1. ограничена исключительно рамками сети Биткоин

Ответ 2. не обеспечивается даже в рамках сети Биткоин

Ответ 3. распространяется на все финансовые институты, включая криптовалютные биржи

Ответ 4. невозможна в принципе

Раздел тестов 3.

Задание 1. Формулировка вопроса – один правильный ответ

Можно ли для отправки транзакций использовать такие незащищенные средства как Wi-Fi или Bluetooth?

Ответ 1. Да

Ответ 2. Нет

Задание 2. Формулировка вопроса – один правильный ответ

Можно ли для отправки транзакций использовать каналы спутниковой или коротковолновой радиосвязи?

Ответ 1. Да

Ответ 2. Нет

Задание 3. Формулировка вопроса – один правильный ответ

Проверяет ли каждый активный узел все полученные по сети транзакции?

Ответ 1. Да

Ответ 2. Нет

Раздел тестов 4.

Задание 1. Формулировка вопроса – один правильный ответ

Основной формой реализации транзакций в сети Биткоин являются …

Ответ 1. P2SH-транзакции

Ответ 2. P2PKH-транзакции

Ответ 3. мультиподписные транзакции

Ответ 4. P2PK-транзакции

Задание 2. Формулировка вопроса – один правильный ответ

Для разблокирования средства на выходе P2PKH-транзакции …

Ответ 1. достаточно предъявить открытый ключ владельца средств

Ответ 2. необходимо предъявить открытый ключ и электронную подпись владельца средств

Ответ 3. достаточно предъявить электронную подпись владельца средств

Ответ 4. необходим PIN-код к биткоин-адресу, на который были посланы средства

Задание 3. Формулировка вопроса – один правильный ответ

Биткоин-адрес P2SH-транзакции, записанный в кодировке Base58Check, начинается с цифры …

Ответ 1. 3

Ответ 2. 1

Ответ 3. 2

Ответ 4. 4

Раздел тестов 5.

Задание 1. Формулировка вопроса – один правильный ответ

Какой тип транзакций в сети Биткоин позволяет реализовать схему платежа, в которой разблокирующий сценарий известен только получателю средств …

Ответ 1. P2SH-транзакции

Ответ 2. P2PKH-транзакции

Ответ 3. транзакции выход данных (OP_RETURN)

Ответ 4. P2PK-транзакции

Задание 2. Формулировка вопроса – один правильный ответ

В случае с P2SH-платежом какая сторона сделки экономит на комиссионных майнерам больше?

Ответ 1. получателя

Ответ 2. отправителя

Ответ 3. расходы делятся поровну между отправителем и получателем

Ответ 4. в P2SH-транзакции вообще не предусмотрены комиссионные

Задание 3. Формулировка вопроса – один правильный ответ

Какой тип транзакции реализует сценарий мульти-подписного адреса?

Ответ 1. P2SH

Ответ 2. P2PKH

Ответ 3. P2PK

Ответ 4. выход данных (OP_RETURN)

Раздел тестов 6.

Задание 1. Формулировка вопроса – один правильный ответ

Какой максимально возможный по числу участников в сценарии мульти-подписи вариант реализован в сети Биткоин?

Ответ 1. 25-из-25

Ответ 2. 15-из-15

Ответ 3. 10-из-05

Ответ 4. 5-из-5

Задание 2. Формулировка вопроса – один правильный ответ

Что хранится в пуле UTXO?

Ответ 1. биткоины

Ответ 2. неизрасходованные выходы транзакций

Ответ 3. данные пользователей

Ответ 4. цепочка блоков

Задание 3. Формулировка вопроса – один правильный ответ

Что является недостатком модели UTXO?

Ответ 1. плохо работает в предметных областях, где на один актив претендуют сразу несколько владельцев

Ответ 2. не подходит для децентрализованных приложений

Ответ 3. плохо доказуема с точки зрения теоретической информатики

Ответ 4. плохо работает в криптовалютах

Раздел тестов 7.

Задание 1. Формулировка вопроса – один правильный ответ

Поддерживает ли протокол Биткоин такой элемент платежных систем как балансовый счет?

Ответ 1. Да

Ответ 2. Нет

Задание 2. Формулировка вопроса – один правильный ответ

Содержит ли блокчейн сети Биткоин данные о владельцах средств?

Ответ 1. Да

Ответ 2. Нет

Задание 3. Формулировка вопроса – один правильный ответ

Может ли платформа Биткоин работать без пула UTXO?

Ответ 1. Да

Ответ 2. Нет

Раздел тестов 8.

Задание 1. Формулировка вопроса – один правильный ответ

Какое утверждение является справедливым?

Ответ 1. транзакция может содержать только один вход и несколько выходов

Ответ 2. транзакция может содержать несколько входов и несколько выходов

Ответ 3. транзакция может содержать несколько входов и только один выход

Ответ 4. транзакция может содержать только один вход и только один выход

Задание 2. Формулировка вопроса – один правильный ответ

Если Вы располагаете нерастраченным выходом, номинал которого существенно больше чем сумма проводимого Вами платежа, то …

Ответ 1. следует отказаться от сделки

Ответ 2. следует организовать сдачу самому себе

Ответ 3. следует разделить нерастраченный выход на части и воспользоваться в транзакции только определенной долей выхода

Ответ 4. следует обратиться к сервисам микширования транзакций

Задание 3. Формулировка вопроса – один правильный ответ

Кто формирует очередную coinbase-транзакцию?

Ответ 1. майнер, сформировавший новый блок

Ответ 2. один из администраторов сети Биткоин

Ответ 3. Сатоши Накамото

Ответ 4. формирование осуществляется автоматически непосредственно в блокчейне

Раздел тестов 9.

Задание 1. Формулировка вопроса – один правильный ответ

В какой части транзакции структурно размещается блокирующий скрипт?

Ответ 1. в каждом из имеющихся входов

Ответ 2. в каждом из имеющихся выходов

Ответ 3. в поле Locktime

Ответ 4. в UTXO

Задание 2. Формулировка вопроса – один правильный ответ

Как организована ссылка входа транзакции на конкретный нерастраченный выход в блокчейне?

Ответ 1. указывается номер UTXO

Ответ 2. указывается хеш соответствующей транзакции и порядковый номер выхода

Ответ 3. указывается требуемая сумма

Ответ 4. указываются данные владельца

Задание 3. Формулировка вопроса – один правильный ответ

Что из указанного списка содержится во входе транзакции?

Ответ 1. разблокирующий скрипт

Ответ 2. блокирующий скрипт

Ответ 3. сумма

Ответ 4. время (в формате ОС Unix)

Раздел тестов 10.

Задание 1. Формулировка вопроса – один правильный ответ

Какую транзакцию называют сиротой?

Ответ 1. поддельную

Ответ 2. дочернюю транзакцию, полученную нодой раньше родительской

Ответ 3. полученную из другой криптовалютной платформы

Ответ 4. находящуюся в форке

Задание 2. Формулировка вопроса – один правильный ответ

Как в языке сценариев Script передаются параметры между термами?

Ответ 1. как глобальные переменные

Ответ 2. через стек

Ответ 3. используя процедуры

Ответ 4. прямым обращением к сегменту кода в памяти компьютера

Задание 3. Формулировка вопроса – один правильный ответ

Почему создатели платформы Биткоин использовали в качестве языка сценариев неполный по Тьюрингу язык Script?

Ответ 1. из соображений безопасности системы

Ответ 2. для придания транзакциям свойства эластичности

Ответ 3. для лучшей масштабируемости системы

Ответ 4. для увеличения пропускной способности системы

Раздел тестов 11.

Задание 1. Задание с вводом правильного числового или текстового значения

Укажите значение, которое будет получено в результате выполнения сценария: 1 1 OP_ADD 3 OP_EQUAL

Ответ 1. FALSE

Задание 2. Задание с вводом правильного числового или текстового значения

Укажите значение, которое будет получено в результате выполнения сценария: 1 OP_DUP OP_EQUAL

Ответ 1. TRUE

Задание 3. Задание с вводом правильного числового или текстового значения

Укажите значение, которое будет получено в результате выполнения сценария: 2 1 OP_ADD OP_DUP OP_EQUAL

Ответ 1. TRUE

Раздел тестов 12.

Задание 1. Формулировка вопроса – один правильный ответ

Какому типу транзакций соответствует следующий комбинированный сценарий <Signature A> <Public Key A> OP_CHECKSIG ?

Ответ 1. Pay-to-Public-Key-Hash

Ответ 2. Pay-to-Public-Key

Ответ 3. Pay-to-Script-Hash

Ответ 4. OP_RETURN

Задание 2. Формулировка вопроса – один правильный ответ

Укажите ошибку в записи комбинированного сценария P2PKH-транзакции: OP_DUP OP_HASH160 <Public-Key-Hash > OP_EQUALVERIFY OP_CHECKSIG <Signature > <Public-Key >

Ответ 1. допущена ошибка в записи оператора OP_CHECKSIG

Ответ 2. переставлены блокирующий и разблокирующий скрипты

Ответ 3. вместо оператора OP_EQUALVERIFY следует использовать оператор OP_EQUAL

Ответ 4. вместо оператора OP_DUP следует использовать оператор OP_ADD

Задание 3. Формулировка вопроса – один правильный ответ

Инструкция OP_RETURN ...

Ответ 1. позволяет добавить 80 байт данных к выходу транзакции

Ответ 2. прекращает выполнение сценария

Ответ 3. возращает данные из блокчейна

Ответ 4. возращает данные из сценария