Банк данных вопросов.

Из контрольной работы №1

Найдите транзакцию BTC с наивысшей комиссионной ставкой из блока 910918
Ответ:
76f5bb4613530ad1d7acd8750b9c90cce7c958f16e3f86418ecb124c27e9f5eb

К какому криптографическому примитиву относятся цифровые подписи?
Ответ: Асимметричные элементы

Консенсус – процесс согласования финального состояния данных между узлами, которые доверяют друг другу
Ответ: Неверно

Блокчейн – это централизованная система
Ответ: Неверно

Византийский узел – узел демонстрирующий некорректное поведение
Ответ: Верно

Когда транзакция получена и подтверждена специальными участниками сети блокчейн – майнерами, её включают в блок, и начинается осуществление майнинга
Ответ: Верно

На рисунке представлена схема генерации адреса в блокчейне Биткойн. На схема под цифрой 8:
Ответ: Контрольная сумма

В кошельке Ethereum для шифрования данных, хранящихся локально, используется 256-битный AES в режиме счетчика
Ответ: Неверно

Узел – отдельный игрок (компьютер), все узлы могут отправлять и получать сообщения. У каждого узла есть память, но отсутствует процессор
Ответ: Неверно

Одно из преимуществ блокчейна – это интеллектуальная собственность
Ответ: Верно

При отправке данных получателю, шифрование этих данных происходит закрытым ключом отправителя
Ответ: Неверно

Среднее время формирования блока в блокчейне Биткойна согласно протокола (мин)
Ответ: 10

Важнейшей особенностью технологии блокчейн является цепочка блоков
Ответ: Неверно

Основные проблема (проблемы) при проектировании распределенных систем:
Ответ: координация между узлами и устойчивость к сбоям

Заголовок блока также содержит транзакции
Ответ: Неверно

Определите хеш блока BTC, в котором находится транзакция 07893f760645c78fa001a46cb8ca9dafd8c2954aeb24860ccfbd5d7ff4a7fb52
Ответ:
00000000000000000016de6abf09ac9b1726dfd74e7ded706f9daa0d6a50b5a

Согласно CAP теореме устойчивость к разделению достигается с помощью алгоритма консенсуса
Ответ: Неверно

Базисное дерево Меркла применяется в блокчейне Ethereum для хранения пар ключ-значение, где корень хешируется с помощью алгоритма RIPEMD и включается в заголовок блока
Ответ: Неверно

В системах шифрования с открытым ключом содержатся такие механизмы безопасности, как:
Ответ: обмен ключами, цифровые подписи, идентификация, шифрование и дешифрование данных

Распределенная система - вычислительная парадигма
Ответ: Верно

В блокчейнах жертвуют доступностью ради согласованности и устойчивости к разделению
Ответ: Неверно

На этом уровне блокчейновой технологии используются протоколы распространения информации:
Ответ: сеть P2P

Считается ли вызов смарт-контракта инициализацией в общей схеме создания блоков?
Ответ: Верно

В кошельке Биткойна для шифрования данных, хранящихся локально, используется SHA-256
Ответ: Неверно

Проблема(проблемы) блокчейна
Ответ: масштабируемость, конфиденциальность, безопасность

На рисунке представлена схема работы алгоритма POS. На схеме под цифрой 4:
Ответ: Доля

Для создания эффективной системы e-cash необходимо соблюдать два фундаментальных требования: подотчетность и
Ответ: анонимность

На рисунке представлен процесс майнинга в блокчейне Биткойн. Под цифрой 6 на рисунке:
Ответ: Увеличение нонса

Укажите хеш блока, в котором находится транзакция TRX 8f9be7999b79a87d82f5a88336c08e77574d61de62855747eb07dcb92dc76075
Ответ:
00000000046afbaaa7bc15baa674c0353f1ac76efc13074d954800199f43e273

Масштабируемость относится к …
Ответ: ограничению БЛЧ

Распределенный реестр обязательно состоит из блоков транзакций как и блокчейн
Ответ: Неверно

В каком году впервые произошло применение блокчейна за пределами криптовалют
Ответ: 2013

Узел в блокчейне поддерживает:
Ответ: цепочку блоков, ВМ, конечный автомат и адрес

Представлена схема работы алгоритма POW. На рисунке под цифрой 5:
Ответ: Полученный хеш

Укажите год, в котором Хэл Финни изобретает многоразовую систему POW
Ответ: 2004

Известно, что транзакция 0x887f9604e5cd6a133a8cf91c9d41505723ce6a6831a053a82b26c6d89b40d79d находится в блоке 23184422. Определите хеш предыдущего блока ETH

Ответ:
0xe7483e816f3d58ff65d62c44cd8065042eb0a7a01239789514f743ca84915b98

Рассчитайте приблизительную комиссию транзакции, где в качестве входов транзакции выступают три входных UTXO, а в качестве выхода транзакции адрес контрагента, а также ваш адрес сдачи. Комиссионная ставка - 0,00000004
Ответ: 0,00002088

Это криптографически сильное случайное число. Обычно его используют в хеш-функциях для защиты от радужных или атак с перебором по словарю
Ответ: соль

Одновременных согласованности данных и доступности не существует на практике
Ответ: Верно

Блокчейн описывает структуру данных, в которой хранится постоянная история транзакций
Ответ: Верно

Из контрольной работы №2

Вопрос 1
Какой из перечисленных подходов НЕ относится к основным концепциям решений второго уровня (Layer-2)?
Ответ: Увеличение размера блоков базового блокчейна

Вопрос 2
Какое поле в структуре заголовка блока биткойна напрямую обеспечивает криптографическую связь с предыдущим блоком, формируя тем самым непрерывную цепочку (blockchain)?
Ответ: Хеш заголовка предыдущего блока (Previous block header hash)

Вопрос 3
Какую функцию выполняет "серия журналов" (logs), которая является частью субсостояния транзакции?

Ответ: Она работает как механизм уведомления, отслеживая и регистрируя события для внешних по отношению к блокчейну систем (пример: фронтенд приложений)

Вопрос 4
Пользователь Алексей создал транзакцию на 250 байт с суммой входов 1.0 BTC и суммой выходов 0.999 BTC. Его друг Борис, чтобы сэкономить, отправил транзакцию с нулевой комиссией. Через 3 часа транзакция Бориса все еще не подтверждена, а транзакция Алексея была обработана за 15 минут. Какой из выводов является НЕВЕРНЫМ?
Ответ: Транзакция Бориса не была обработана, потому что она является невалидной и была отклонена узлами сети из-за отсутствия комиссии

Вопрос 5
Какой тип кошелька позволяет сгенерировать неограниченное количество ключей для получения средств из единого начального значения (сида), представленного в виде мнемонической фразы, при этом обеспечивая древовидную структуру для организаций ключей и упрощения резервного копирования?
Ответ: Иерархический детерминированный (HD) кошелек

Вопрос 6
Эти типы блокчейна децентрализованы и открыты для всех, разрешение широкого участия в сетевой деятельности и обеспечение прозрачности посредством широкого распространения и механизмов достижения консенсуса
Ответ: Public

Вопрос 7
Какой элемент транзакции указывает на её положение внутри блока в блокчейне?
Ответ: Included in block

Вопрос 8
Этот метод в смарт-контракте возвращает владельца, который имеет право передавать указанный токен другому владельцу
Ответ: getApproved

Вопрос 9
Какое поле в заголовке блока Ethereum содержит хеш корневого узла структуры данных, которая хранит информацию о состоянии всех учетных записей (балансы, nonce, код контрактов и хранилище) после обработки всех транзакций в этом блоке?
Ответ: Корневой узел состояния (State root)

Вопрос 10
Представьте, что смарт-контракт для автоматизации выплат по страхованию урожая должен получать данные о количестве осадков в определённом регионе. Для этого используются специальные метеостанции с датчиками. Какой тип оракула наиболее подходит для этого сценария и почему?
Ответ: Аппаратный оракул, так как он предназначен для получения данных непосредственно с физических устройств и датчиков

Вопрос 11
Этот метод в смарт-контракте позволяет другому адресу передавать токены от Вашего имени (с Вашего адреса). Данный метод применяется в случае, когда участник разрешил конкретному адресу отправлять токены от своего имени.
Ответ: transferFrom

Вопрос 12
Какая модель обработки транзакции содержит параллелизм (Hyperledger Fabric):
Ответ: Execute, Ordering, Validate

Вопрос 13
Какое свойство смарт-контракта является критически важным для обеспечения того, чтобы все узлы в распределенной сети блокчейна пришли к единому и неизменному результату его выполнения, тем самым поддерживая консенсус?
Ответ: Детерминированность

Вопрос 14
Какую функцию выполняет «пул транзакций» (пул памяти) в сети Биткойн?
Ответ: Это буфер в оперативной памяти узла для временного

хранения неподтвержденных транзакций, ожидающих включения в блок

Вопрос 15
Чем характеризуется транзакция типа "coinbase"?
Ответ: Не имеет ввода (input), так как создает новые монеты

Вопрос 16
Что относится к ключевым функциям, которые обеспечивают Layer-1 блокчейны как фундаментальные протоколы?
Ответ: Обеспечение алгоритма консенсуса, поддержание инфляционной модели, функционирование прикладных языков программирования

Вопрос 17
Какова основная экономическая роль майнеров в сети Ethereum?
Ответ: Быть мотивированными финансовым вознаграждением (Ether) за проверку корректности и подлинности блоков транзакций

Вопрос 18
Согласно правилам валидации блока в Ethereum, какое из перечисленных условий приведет к немедленному отклонению блока?
Ответ: Временная метка блока меньше (раньше), чем временная метка его родительского блока

Вопрос 19
Каков ключевой компромисс или основная выгода для майнера, решившего работать в майТРА2нинг-пуле, по сравнению с соло-майнингом?
Ответ: Участник пула получает регулярный и предсказуемый доход, даже если именно его вычислительная мощность не нашла решение для блока

Вопрос 20
Представьте, что майнер анализирует три транзакции (А, Б, В) из своего пула памяти, чтобы включить их в следующий блок. Согласно правилам валидации, какая из этих транзакций будет однозначно отклонена узлами сети и НЕ будет включена в блок?

Ответы: Транзакция А: Имеет сумму входов 1.5 BTC и сумму выходов 1.7 BTC. Цифровые подписи верны, и её входы ранее не тратились,

Транзакция В: Все её входы уже были использованы в другой транзакции, которая попала в предыдущий блок,

Транзакция Д: Цифровые подписи для её входов не соответствуют ожидаемым скриптам и являются недействительными

Вопрос 21
Недостаток Account Based Model
Ответ: отсутствие параллелизма

Вопрос 22
Какое из перечисленных условий является обязательным для первоначальной проверки валидности транзакции в Ethereum?
Ответ: Nonce (одноразовый код) транзакции должен точно соответствовать текущему значению nonce в учетной записи отправителя

Вопрос 23
Какое поле в транзакции Ethereum гарантирует, что каждая транзакция, отправленная с определённого адреса, будет уникальной и защищённой от повторного воспроизведения (replay attacks)?
Ответ: Nonce-число

Вопрос 24
В чем заключается ключевое отличие алгоритма консенсуса GHOST, используемого в Ethereum, от подхода "самой длинной цепочки", применяемого в Биткойне?
Ответ: GHOST учитывает вычислительную работу, затраченную на создание ommer-блоков, формируя "самую весомую" цепочку, а не просто самую длинную

Вопрос 25
Как генерируется уникальный адрес для вновь создаваемого смарт-контракта в Ethereum?
Ответ: Это младшие 160 бит хеша Keccak от RLP-кодированной структуры, содержащей адрес отправителя и его Nonce-число

Вопрос 26
Закрытый ключ биткойна используется для:
Ответ: создания цифровой подписи транзакций и подтверждения владения биткойнами

Вопрос 27
Каков правильный порядок этапов жизненного цикла транзакции в сети Биткойн?
Ответ: Подписание -> Трансляция в сеть -> Помещение в пул памяти -> Майнинг -> Получение подтверждений

Вопрос 28
Согласно структуре данных транзакции, какое поле отвечает за определение самого раннего момента времени, когда транзакция может быть признана действительной и включена в блок?
Ответ: Время блокировки (Lock time)

Вопрос 29
Какова основная функция корня Меркла, который хранится в заголовке каждого блока блокчейна?
Ответ: Выступать криптографическим «отпечатком пальца», который представляет все транзакции в блоке и гарантирует их целостность

Вопрос 30
Какова основная функция оракула в экосистеме смарт-контрактов?
Ответ: Служить интерфейсом для доставки внешних данных из реального мира в смарт-контракт

Вопрос 31
В чем заключается ключевое различие между транзакцией и сообщением в Ethereum?
Ответ: Транзакции создаются и подписываются внешними агентами (пользователями), тогда как сообщения создаются и отправляются смарт-контрактами в среде выполнения

Вопрос 32
Каково основное назначение транзакции coinbase?

Ответ: Для создания новых монет и она всегда является первой в блоке

Вопрос 33
Представьте, что майнер успешно нашел Nonce, удовлетворяющий условию Proof-of-Work, и его блок был принят сетью. Согласно тексту, что из перечисленного НЕ является прямым и гарантированным следствием этого события?
Ответ: Сложность майнинга в сети немедленно автоматически повышается, чтобы гарантировать нахождение следующего блока ровно через 10 минут

Вопрос 34
Какое из утверждений точно описывает одно из ключевых различий между памятью (Memory) и хранилищем (Storage) в виртуальной машине Ethereum (EVM)?
Ответ: Память (Memory) является энергозависимой и очищается после выполнения транзакции, а хранилище (Storage) постоянно сохраняется в блокчейне

Вопрос 35
Что такое транзакция в сети Биткойн?
Ответ: Ядро экосистемы, которое может быть простым или сложным и состоит из нескольких элементов

Вопрос 36
Какое количество подтверждений транзакции считается достаточным для надежного предотвращения двойного расходования?
Ответ: Ожидание шести подтверждений является рекомендуемым для предотвращения двойного расходования

Вопрос 37
Чем структура ввода транзакции coinbase ОТЛИЧАЕТСЯ от структуры ввода обычной транзакции?
Ответ: У нее нет указателя на предыдущую транзакцию, а вместо скрипта разблокирования есть поля для данных

Вопрос 38
Согласно механизму функции перехода состояний в Ethereum, что

происходит с комиссией (газом) за транзакцию, если её выполнение завершается неудачно из-за нехватки газа (OOG - Out of Gas)?
Ответ: Все изменения состояния отменяются, но уплаченная комиссия не возвращается и достаётся майнеру

Вопрос 39
Согласно процессу генерации, что представляет собой адрес в сети Ethereum и как он получается?
Ответ: Адрес — это последние 20 байт хеша Keccak-256, вычисленного от открытого ключа

Вопрос 40
Какое из следующих утверждений о транзакции, которая отправляет монеты другому пользователю, является ВЕРНЫМ?
Ответ: Она должна быть подписана закрытым ключом отправителя и иметь ссылку на предыдущую транзакцию

Из контрольной работы №3

Какое из следующих утверждений НЕВЕРНО описывает связь между сетью Lightning и блокчейном (блочной цепью)?
Ответ: Все платежи в сети Lightning записываются как транзакции в базовом блокчейне

Чем принципиально отличается процесс отправки платежа в Lightning Network от проведения транзакции в базовом блокчейне Bitcoin?
Ответ: Платежи в Lightning Network маршрутизируются только между парами узлов, а не широко вещаются всей сети

Какая технология, используемая в Lightning Network для обеспечения конфиденциальности, напрямую сравнивается с протоколом сети Tor?
Ответ: Луковичная маршрутизация

Какой из перечисленных признаков сети Lightning НЕВЕРЕН
Ответ: Для проведения платежей в Lightning Network требуется ожидание подтверждения хотя бы одного блока в базовом блокчейне

Какую ключевую роль выполняет комбинация транзакций «внутри цепи» и «вне цепи» для создания сети Lightning?
Ответ: Она формирует дополнительный «слой» платежей поверх Bitcoin, который становится более быстрым, дешевым и приватным способом его использования

Какое утверждение наиболее точно описывает финансовую основу платежного канала Lightning Network?
Ответ: Это мультиподписной адрес «2 из 2» в блокчейне Bitcoin, контроль над средствами на котором требует подписи обоих участников канала

Какой криптографический механизм гарантирует, что участник канала не сможет мошеннически вернуть и использовать устаревшее (отозванное) состояние баланса в свою пользу?
Ответ: Механизм штрафов, встроенный в смарт-контракт (скрипт) Bitcoin, который наказывает такого участника

В чём заключается ключевое преимущество использования последовательности неподтверждённых (хранимых «вне цепи») транзакций для обновления баланса в платежном канале?
Ответ: Это эквивалентно перемещению средств между участниками без записи каждой операции в публичный блокчейн Bitcoin

Что является основным экономическим стимулом для майнеров Bitcoin участвовать в объединённом майнинге (merge-mining) сети RSK?
Ответ: Они получают дополнительное вознаграждение в виде комиссий за транзакции в сети RSK, практически без увеличения своих операционных затрат

В чем заключается принципиальное различие между процессом проведения платежа в блокчейне Bitcoin и в сети Lightning Network?
Ответ: Bitcoin-транзакции «отправляются» широковещательной рассылкой, а Lightning-платежи «маршрутизируются» по цепочке каналов

Какое из перечисленных свойств платежного канала Lightning Network является НЕВЕРНЫМ?
Ответ: Для совершения платежа внутри открытого канала требуется дождаться как минимум одного подтверждения в блокчейне Bitcoin

Какое свойство луковичной маршрутизации (Onion Routing) в Lightning Network является самым важным для обеспечения высокой степени конфиденциальности?
Ответ: Промежуточный узел не знает, кто инициатор и конечный получатель платежа, зная только своих соседей в цепочке

Какой из перечисленных механизмов в протоколе луковичной маршрутизации Lightning Network позволяет безопасно находить рабочий путь для платежа методом проб и ошибок, не раскрывая стратегию поиска внешним наблюдателям и промежуточным узлам?
Ответ: Маршрутизация сообщений об ошибках обратно инициатору по тому же луковичному протоколу, делая их неотличимыми от обычных платежных пакетов

Что из перечисленного является правильным соответствием между элементами экосистемы Bitcoin и Lightning Network ?
Ответ: Bitcoin-адрес является аналогом Lightning-счёта (invoice), а Bitcoin-транзакция является аналогом Lightning-платежа

С точки зрения лучших практик конфиденциальности, какое поведение, технически возможное в Bitcoin, считается нежелательным, но при этом полностью невозможно в базовом протоколе Lightning (без использования специальных механизмов)?
Ответ: Использование одного и того же адреса/счёта для получения множества платежей от разных отправителей

Какой общий, фундаментальный принцип работы является ключевым и для Bitcoin, и для Lightning Network?
Ответ: Пользователь доверяет только математике, криптографии и надежности ПО, а не конкретным людям или институтам

Что из перечисленного является НЕВЕРНЫМ утверждением об общих чертах Bitcoin и Lightning Network?
Ответ: Lightning Network имеет собственный лимит эмиссии, отличный от 21 миллиона BTC

Как модель безопасности Lightning Network соотносится с моделью безопасности Bitcoin?
Ответ: Безопасность Lightning Network сводится к безопасности Bitcoin, обеспечивая в целом тот же уровень защиты

Какое из утверждений о конфиденциальности в Lightning Network является верным?
Ответ: Узлы Lightning имеют постоянную идентичность (ID узла и IP-адрес), что создает риски для анонимности, в отличие от узлов Bitcoin, которые можно легко менять

Почему крупные платежи в Lightning Network могут быть менее приватными и более уязвимыми для наблюдения?
Ответ: У них может быть меньше вариантов маршрутизации, что позволяет злоумышленнику, контролирующему узлы с высокой ликвидностью, наблюдать за большинством таких платежей

Какой строительный блок (примитив) Биткойна гарантирует, что транзакция, действительная сегодня и с неизрасходованными входами, будет принята сетью в будущем, даже через длительный срок, при условии неизменности правил консенсуса?
Ответ: Без срока действия (Nonexpiration)

Какой вектор атаки на доступность и конфиденциальность характерен для Lightning Network, но отсутствует или менее очевиден в базовом протоколе Bitcoin?
Ответ: Злоумышленник может отправлять множество платежей, не завершая их, надолго блокируя капитал честных пользователей в HTLC-контрактах

Атака на конфиденциальность, при которой злоумышленник не находится на пути платежа (противник вне пути). Какой ключевой метод он

использует для сбора исходных данных о состоянии сети перед проведением анализа?
Ответ: Последовательное «прощупывание» (probing) сети для определения индивидуальных остатков в платежных каналах и создания «снимков» её состояния в разные моменты времени

Какая из перечисленных утечек информации позволяет злоумышленнику на пути платежа (противнику на пути) сузить круг возможных отправителей и получателей, основываясь на технических параметрах платежа?
Ответ: Он может исключить из «анонимностного множества» все узлы, ёмкость каналов которых меньше суммы маршрутизируемого платежа

Какой фундаментальный принцип, лежащий в основе слепой цифровой подписи, позволяет использовать её для обеспечения анонимности в блокчейнах?
Ответ: Сообщение маскируется (скрывается) перед отправкой на подпись, что позволяет подписывающей стороне подписать его, не зная содержания, сохраняя при этом возможность последующей верификации подписи с оригинальным сообщением

Какое ключевое преимущество пороговой подписи (threshold signature) по сравнению с обычной мультиподписью (multisig) делает её особенно полезной для публичных блокчейнов с точки зрения приватности и эффективности?
Ответ: Для проверяющего (ноды сети) она выглядит как одна обычная подпись от одного ключа, что снижает размер транзакции, ускоряет проверку и скрывает состав группы подписантов

В чём заключается ключевое принципиальное отличие полностью гомоморфного шифрования (Fully Homomorphic Encryption, FHE) от частично гомоморфного шифрования (Partially Homomorphic Encryption, PHE)?
Ответ: FHE позволяет выполнять неограниченное количество произвольных операций (как сложение, так и умножение) над

зашифрованными данными, в то время как PHE поддерживает только один тип операций (либо сложение, либо умножение)

Какой подход к организации распределённой сети сознательно жертвует степенью децентрализации для достижения высокой пропускной способности и скорости обработки транзакций?
Ответ: Скоростной подход (например, сети на базе Delegated Proof-of-Stake), где строгий отбор и небольшое количество нод обеспечивают эффективность, но снижают децентрализацию

Какой уровень блокчейн-архитектуры (L0, L1, L2, L3) отвечает непосредственно за обеспечение базовой безопасности, децентрализации и создания консенсуса, выступая фундаментом для всех остальных надстроек?
Ответ: Уровень L1 — базовые блокчейны (такие как Bitcoin или Ethereum), которые обеспечивают безопасность и децентрализацию, являясь основой для других уровней

Какое ключевое отличие сайдчейна (sidechain) от решения уровня L2, такого как каналы состояния (state channels), с точки зрения их архитектурной независимости?
Ответ: Сайдчейн является полностью независимым блокчейном со своими правилами консенсуса и параметрами, но связан с основной цепью через двусторонний мост, тогда как каналы состояния — это лишь протоколы взаимодействия поверх базового блокчейна

Если участник сети создаст транзакцию, где сумма биткойнов на выходах окажется больше суммы на входах (без учета комиссии), то какое фундаментальное правило/примитив Биткойна будет нарушено и предотвратит подтверждение такой транзакции?
Ответ: Подотчетность (Accounting)

Какое фундаментальное отличие между ZK-роллапами и оптимистическими роллапами лежит в основе их механизма обеспечения безопасности и подтверждения транзакций?

Ответ: ZK-роллапы для каждой партии транзакций генерируют криптографическое доказательство корректности (SNARK/STARK), которое мгновенно верифицируется в L1, в то время как оптимистические роллапы полагаются на честность операторов и используют оспаривающий период (challenge period), в течение которого транзакции можно оспорить

Какая из перечисленных гарантий Биткойна напрямую обеспечивается доказательством работы (PoW) и затратами энергии, делая перезапись истории блокчейна экономически нецелесообразной по мере роста количества подтверждений?
Ответ: Неизменяемость (Immutability)

В основе работы платежных каналов лежит комбинация нескольких строительных блоков. Какую ключевую роль в этой комбинации играет блок «Блокировка по времени» (Timelock)?
Ответ: Позволяет сторонам создавать обновленные состояния канала (транзакции обязательств) с более короткими временными задержками, чем у исходной расчетной транзакции

Какой ключевой механизм в Lightning Network гарантирует, что промежуточный участник (например, Боб) получит плату за маршрутизацию платежа и при этом не потеряет свои средства, если следующий в цепочке узел (Кэрол) не сможет завершить операцию?
Ответ: Последовательное уменьшение тайм-аута (времени блокировки) для HTLC при движении от отправителя к получателю

В примере с маршрутизацией платежа от Алисы к Эрику, какую сумму в итоге получит Эрик и почему она отличается от суммы, которую инициировала Алиса?
Ответ: Эрик получит 1 биткойн, потому что сумма HTLC, которую ему предлагает Диана, равна именно 1 BTC, а разница (0,003 BTC) остается у промежуточных узлов как их комиссия

Что из перечисленного является ПРАВИЛЬНЫМ описанием роли секрета R и его хеша H в процессе маршрутизируемого платежа в Lightning Network?
Ответ: Хеш H служит публичным идентификатором платежа. Его создает получатель (Эрик) и передает отправителю. Раскрытие секрета R получателем в обмен на HTLC позволяет каждому предыдущему участнику цепочки последовательно забрать свои заблокированные средства

На этом уровне блокчейновой технологии используются протоколы распространения информации:
Ответ: сеть P2P

Узел в блокчейне поддерживает:
Ответ: цепочку блоков, ВМ, конечный автомат и адрес

Масштабируемость относится к …
Ответ: ограничению БЛЧ