Прохождение внешнего курса 3 часть

Криптография на практике

Кроитору Екатерина НБИ-бд-03-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Рассмотрим что такое криптография на практике. Узнаем для чего нужна цифровая подпись. Как работают электронный платежи и разберем откуда появился блокчейн и как он работает. # Задание

Выполнить тестовую часть курса

2 Теоретическое введение

В асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный ключ сторона хранит у себя. К протоколам асимметричной криптографии относят электронно-цифровую подпись и протокол генерации общего ключа – это этот протокол, который позволяет нам не общаться физически друг с другом, а установить и вычислить общий секретный ключ.

Как правило, в современных протоколах, в современных конфиденциальных коммуникациях используются вместе симметричная криптография и асимметричная криптография. Это сделано, в частности, для того, чтобы сделать конфиденциальную коммуникацию эффективной, так как симметричные примитивы обычно являются более эффективными по времени, чем асимметричные примитивы. Во-вторых, цифровая подпись обеспечивает аутентификацию сообщения, то есть мы можем установить принадлежность подписи владельцу, иными словами, никто другой не смог бы поставить такую подпись под этим сообщением. Ну и последнее, третье – это неотказ от авторства, то есть как только подпись подписана, подписавший её человек не может отказаться от того факта, что он ее подписал. Конечно, в случае кражи секретного ключа, с помощью которого подписывается сообщение, формируется подпись, о корректной безопасности цифровой подписи никакой речи быть не может, поскольку секретный ключ украден. Вообще, этап авторизации покупки зависит от того, какой у нас платеж. Платежи делятся на две категории: первая – это card present или CP, это означает,

что у нас есть физический доступ к нашей карточке, например, когда мы делаем покупки в супермаркете и, оплачивая, мы прикладываем нашу карту к терминалу, либо считываем. Что при этом происходит? При этом терминал, как правило, запрашивает у вас PIN-код. Вы вводите PIN-код, после этого формируется подпись, то есть с помощью вашего PIN-кода на ваш чек, на вашу покупку ставится ваша подпись. У вас как бы есть свой секретный ключ, вшитый в вашу карточку, который генерирует подпись. Эта подпись отправляется банку-эмитенту, он проверяет с помощью вашего публичного ключа, который лежит у банка, эту подпись. Если подпись верна, банк подтверждает транзакцию, вы себя аутентифицировали как владельца этой карты. Для начала разберемся с двумя важными понятиями. Первое: между понятиями крипто (Crypto) и криптовалюта (Cryptocurrency) не стоит знак равенства. Под крипто мы понимаем криптографию как науку, и вы уже знаете довольно много примитивов и терминов из этой области. А вот криптовалюта - это разновидность цифровых денег, которые построены на основе технологии блокчейн. Почему она называется криптовалютой? Потому что для ее корректной работы используются криптографические примитивы. Что я понимаю под корректной работой? Мы все знаем, что деньги должно быть сложно скопировать, и для того, чтобы криптографическую валюту было сложно подделать или скопировать, используются криптографические примитивы. Вторая цель - это обеспечение того, чтобы в криптовалюте одни и те же деньги нельзя было потратить дважды. То есть, когда монеты уже были потрачены или заплачены мной кому-то еще, я не могу эти же самые деньги потратить второй раз. Это свойство также достигается за счет криптографических примитивов. Второе, что нужно понимать - это то, что между биткоином и блокчейном не стоит знак равенства. Несмотря то, что биткоин - это самая популярная криптовалюта на сегодняшний день и первая из криптовалют, это всего лишь одна из возможных криптовалют. Кроме того, это ещё и платежная система, которая использует одноименную валюту. Но у нас есть и другие, не менее интересные криптовалюты, такие как Эфир, Monero, Tether, Zcash, их довольно много на сегодняшний день,

и все они популярны настолько, насколько популярен Биткоин. Однако у них есть свои преимущества относительно Биткоина. Мы не будем в этой лекции углубляться в каждую из них, мы рассмотрим, как работает технология блокчейн.

Зачем вообще она нужна? Основная причина создания криптовалют - это желание работать с децентрализованной платежной системой. Децентрализованная означает, что в этой системе нет какого-то банка как центральной единицы, а значит и нет государственного контроля над средствами. Кому и когда эта идея пришла в голову? Академическая статья о Биткоине вышла 12 января 2009 года и была подписана именем Сатоши Накамото. На самом деле, мы до сих пор не знаем, кто такой Сатоши Накамото, существует ли этот человек на самом деле, это несколько человек или эта компания, но это не важно; важно то, что эта статья положила начало криптографической валюте. В аннотации статьи написано, что она предлагает версию электронных денег. На самом деле электронные деньги как примитив существовали задолго до 2009 года, но важно то, что в этой статье предлагается механизм построения электронных денег, который бы позволил осуществлять онлайн платежи от одного человека к другому без какого-либо финансового института и без какой-либо третьей доверенной стороны, и это положило начало тому, что мы сегодня называем криптографическая валюта. В первой статье была предложена версия криптографической валюты Bitcoin.

3 Выполнение лабораторной работы

В асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ. (рис. 3.1).

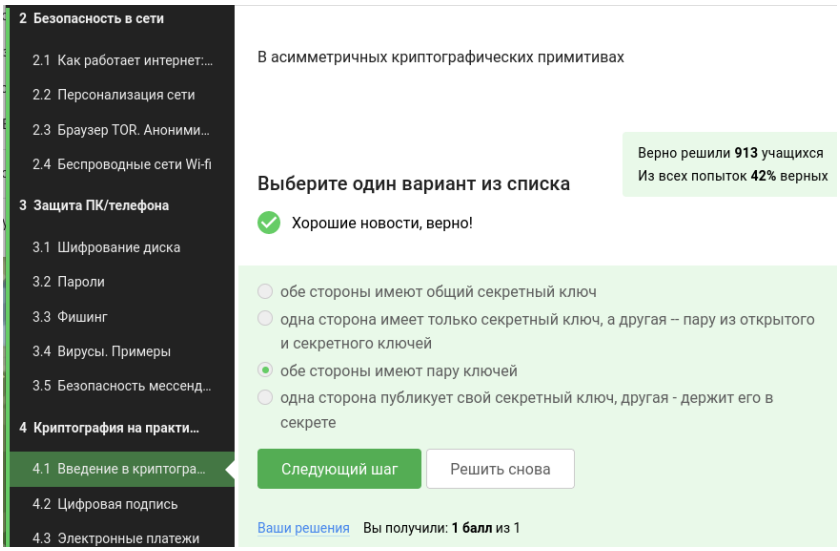

Рис. 3.1: Тест 1

Важное свойство криптографической хэш-функций, то, что делает её криптографической – это стойкость к коллизиям. Что такое коллизия? Коллизия – это два разных входа в хэш-функцию, которые дают одинаковый выход. То есть это две разные строки например x и x’, где $x \neq x'$, такие, что значения хэш-функции на них совпадают, то есть $h(x) = h(x')$. Это важное свойство отличает криптографическую функцию от некриптографической. Можно доказать (мы этого делать с вами не будем), что из этого свойства коллизии следует другое важное свойство,

а именно то, что криптографическую хэш-функцию сложно обратить. То есть, если я вам даю какое-то значение этой функции в точке h(x) и спрашиваю вас, как найти x, то есть вход в эту функцию, для современных криптографических хэш-функций это сделать сложно.

Благодаря этим свойствам, криптографические функции широко применяются в коммуникациях, мы с вами в одной из лекций говорили о том, как криптографическую хэш-функцию можно использовать для хранения паролей. Она также используются для протоколов, подтверждающих целостность данных, ну и современное довольно популярное применение хэш-функции – это доказательство работы. По-другому это называется протоколом proof of work, который используется, например, в таком блокчейне, как биткойн. (рис. 3.2).

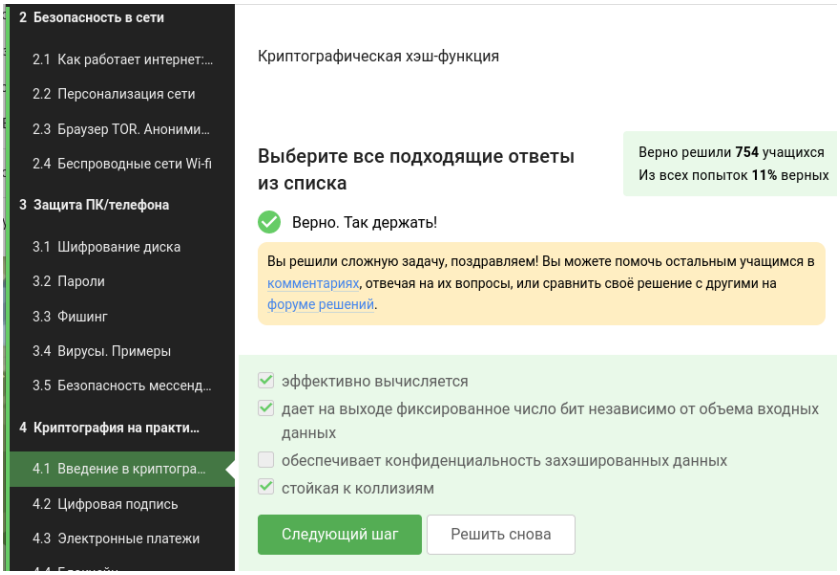

Рис. 3.2: Тест 2

К примерам цифровой подписи относятся интернет-сертификаты, подпись RSA, американский стандарт ECDSA и отечественный стандарт ГОСТ стандарт Р 34.10.2012. (рис. 3.3).

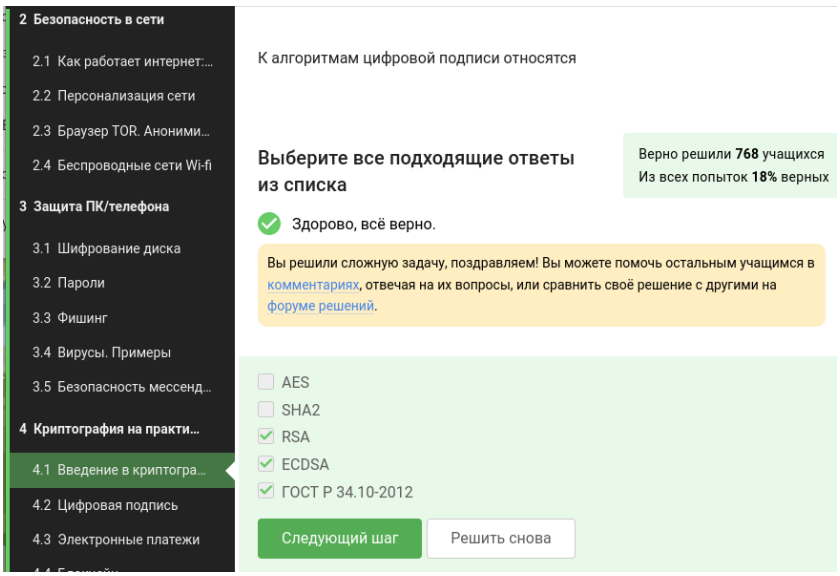

Рис. 3.3: Тест 3

Определяющее свойство симметричной криптографии состоит в том, что она включает себя протоколы, где две или более стороны имеют общие секретные ключи, поэтому она и называется симметричной. К таким протоколам относят симметричное шифрование и некоторые протоколы аутентификации. (рис. 3.4).

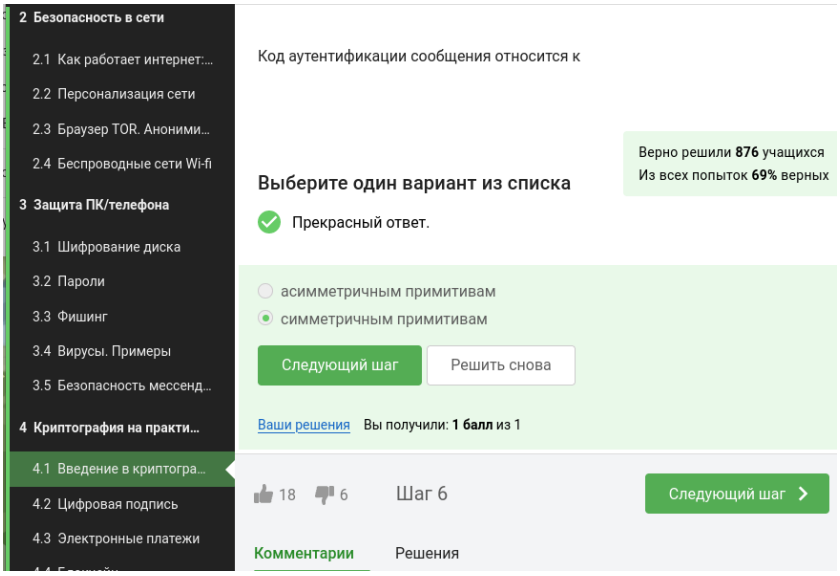

Рис. 3.4: Тест 4

Самым популярным примером протокола обмена ключами является протокол Диффи-Хэллмана, как раз он, либо его модификации используются в современных мессенджерах и в протоколе TLS для того, чтобы мы смогли сгенерировать общий секретный ключ и дальше шифровать наши данные с помощью симметричного алгоритма, то есть с помощью ключа skAB. Если реализовать генерацию общего ключа так, как она описана у Диффи-Хэллмана, мы получим довольно слабый протокол, нестойкий к активным злоумышленникам. (рис. 3.5).

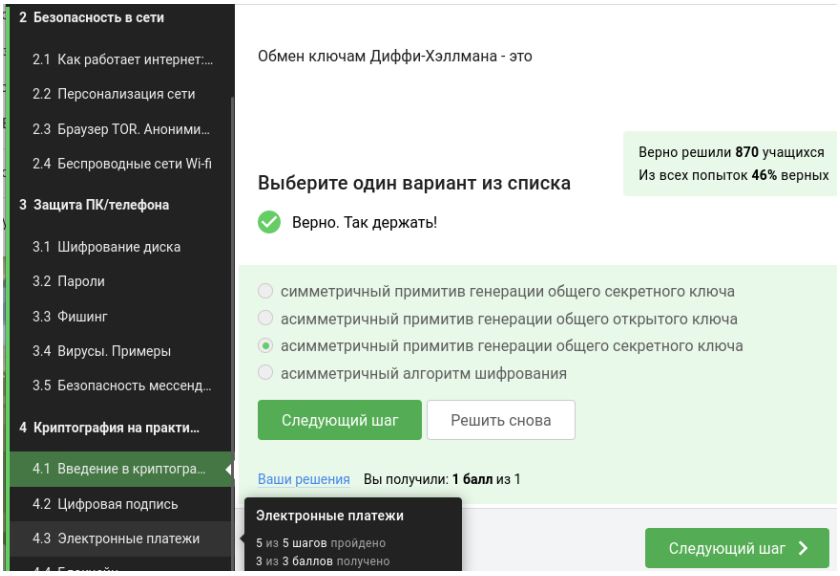

Рис. 3.5: Тест 5

Цифровая подпись имеет прямую связь с асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный ключ сторона хранит у себя. (рис. 3.6).

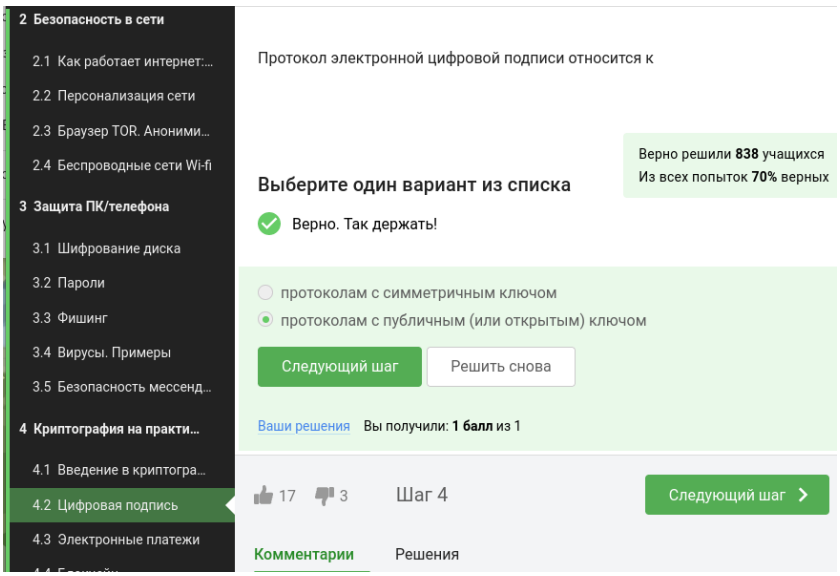

Рис. 3.6: Тест 6

Первый алгоритм занимается генерацией ключей, он генерирует публичный ключ и секретный ключ. Публичный ключ мы держим в открытом доступе, секретный ключ – у себя, никому не показываем. Секретный ключ еще называется подписывающим ключом, а открытый – проверяющим или ключом верификации. Второй алгоритм – это генерация подписи, которая берет на вход сообщение и секретный ключ и выдает нам подпись. И третий – это верификация подписи, которая берёт на вход подпись, сообщение и открытый ключ и выдает нам либо тот факт, что подпись верна, либо тот факт, что подпись неверна. (рис. 3.7).

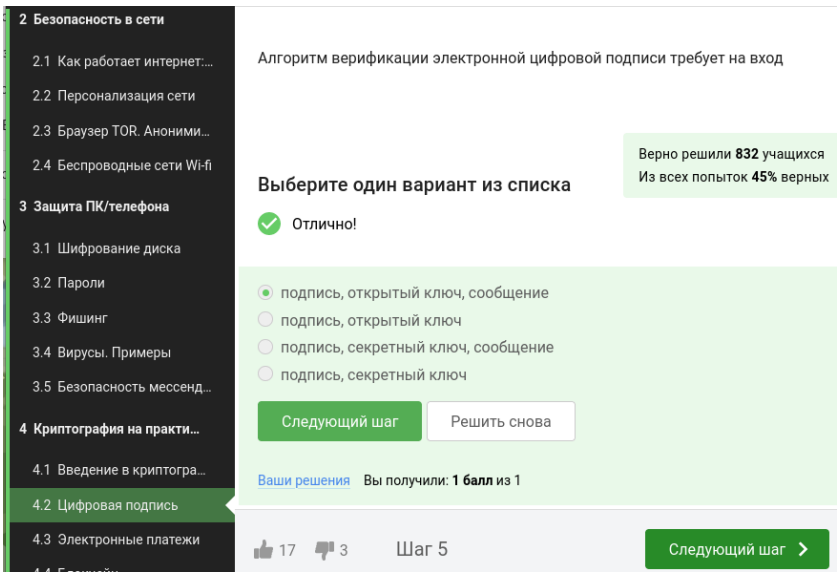

Рис. 3.7: Тест 7

Цифровая подпись предназначена, во-первых, для обеспечения целостности сообщения, иными словами, если сообщение в процессе передачи было изменено, то подпись этого измененного сообщения будет проверена некорректно, то есть при проверке корректности подписи мы узнаем о том, что сообщение было изменено. Во-вторых, цифровая подпись обеспечивает аутентификацию сообщения, то есть мы можем установить принадлежность подписи владельцу, иными словами, никто другой не смог бы поставить такую подпись под этим сообщением. Ну и последнее, третье – это неотказ от авторства, то есть как только подпись подписана, подписавший её человек не может отказаться от того факта, что он ее подписал. (рис. 3.8).

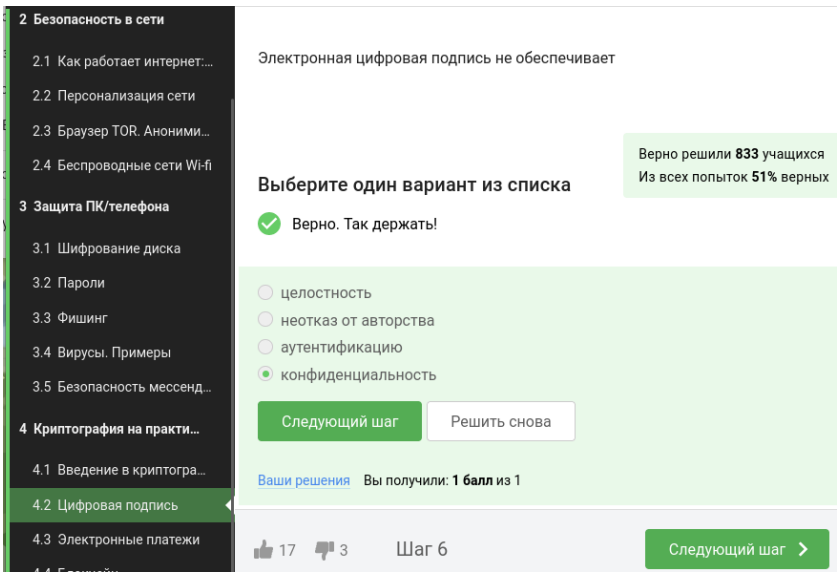

Рис. 3.8: Тест 8

Существует три различных точки зрения на подписи: простая, усиленная неквалифицированая и усиленная квалифицированная. Первые два типа не имеет юридической силы или она довольно ограничена (рис. 3.9).

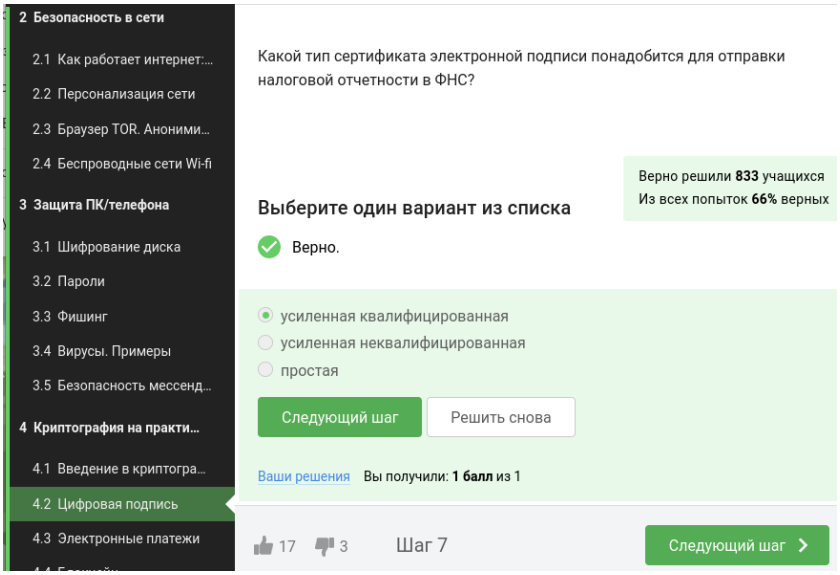

Рис. 3.9: Тест 9

А вот что касается усиленной квалифицированной подписи, эта подпись уже

имеет юридическую силу, она, как правило, равнозначна рукописной. Для того, чтобы получить такую подпись, вам нужно пойти со своим паспортом и с другими данными в сертификационный центр, который должен быть аккредитован конкретным министерством. Такие подписи используются на Госуслугах, в государственном документообороте. (рис. 3.10).

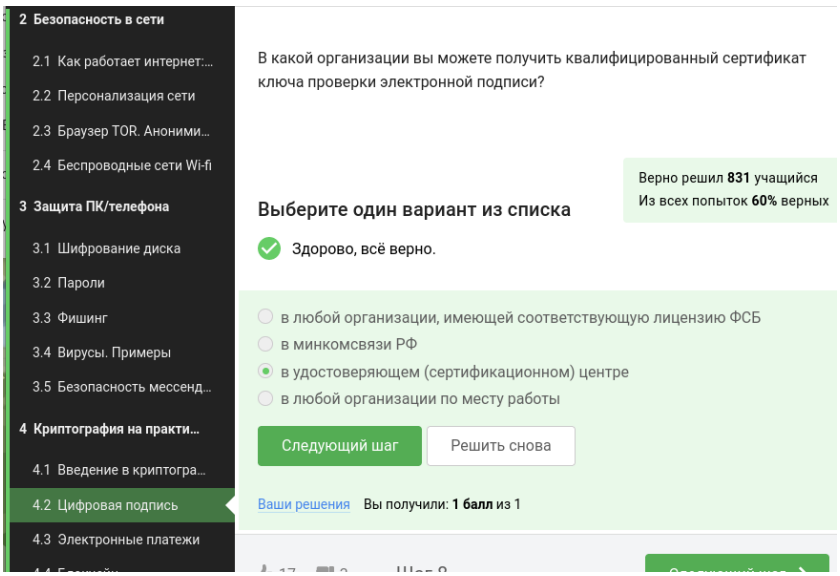

Рис. 3.10: Тест 10

Данные платежные системы самые популярные (рис. 3.11).

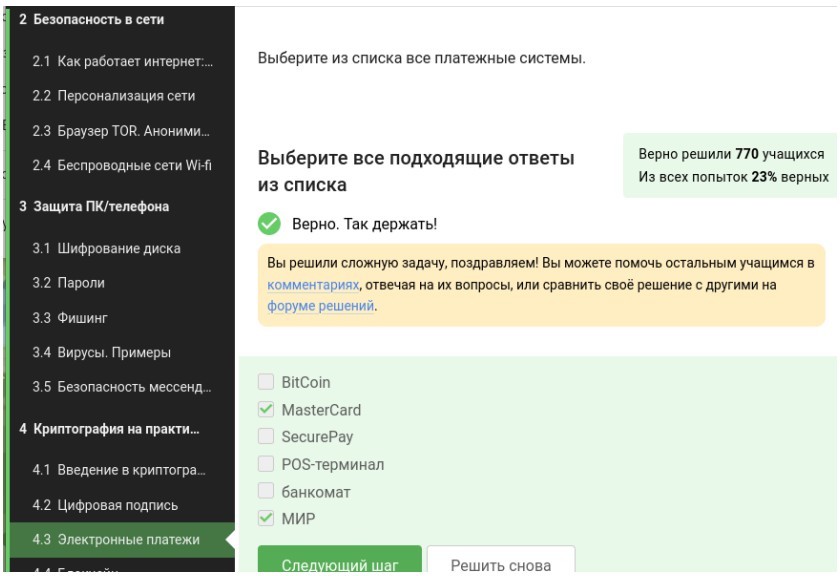

Рис. 3.11: Тест 11

Многофакторная аутентификация заключается в том, что мы доказываем в ходе этого протокола несколько вещей есть. Основные категории вещей, которые мы можем доказать: 1) то, что я знаю – это либо пароль, либо PIN-код, либо в случае онлайн-платежей это секретный код, 2) конкретно в онлайн-платежах мы еще используем второй фактор – это то, чем я владею, например, телефон, именно поэтому нам часто приходит код, который вы должны подтвердить или вбить в ваш браузер, 3) другой фактор аутентификации – это свойства, например, биометрия, опечаток пальца, сетчатки глаза, 4) четвертый фактор аутентификации – локация. Способ аутентификации, как правило, выбирается банком. (рис. 3.12).

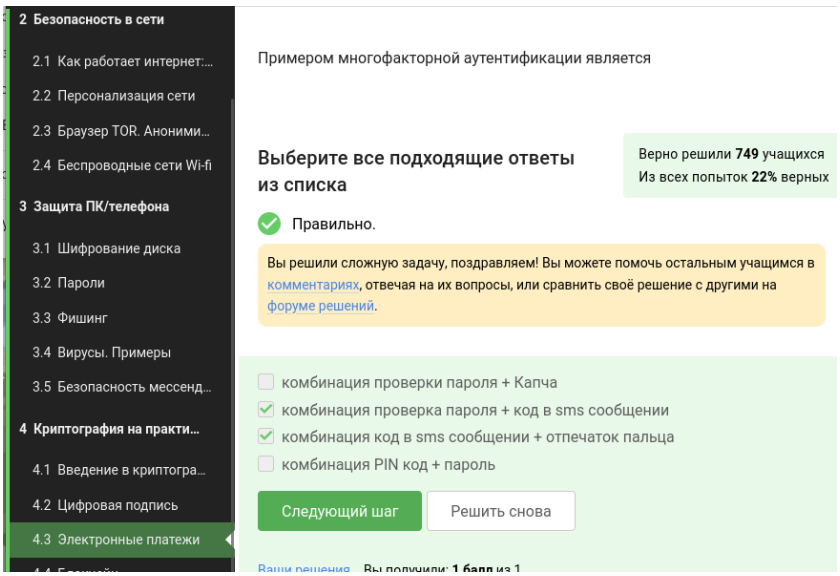

Рис. 3.12: Тест 12

Происходит многофакторная аутентификация. Аутентификация вообще – это криптографический протокол, в котором есть две стороны: первая – это доказующая (в этом случае покупатель) и проверяющая (в этом случае это банк), которые доказывают, что некое утверждение верно. В аутентификации при покупке утверждение, которое я как покупатель хочу доказать, это то, что это моя карта и она мне принадлежит. Вообще, аутентификация может осуществляться не только при покупке, онлайн-платежах, она может осуществляется, когда мы открываем свою машину бесконтактным ключом, мы тоже пытаемся себя аутентифицировать. (рис. 3.13).

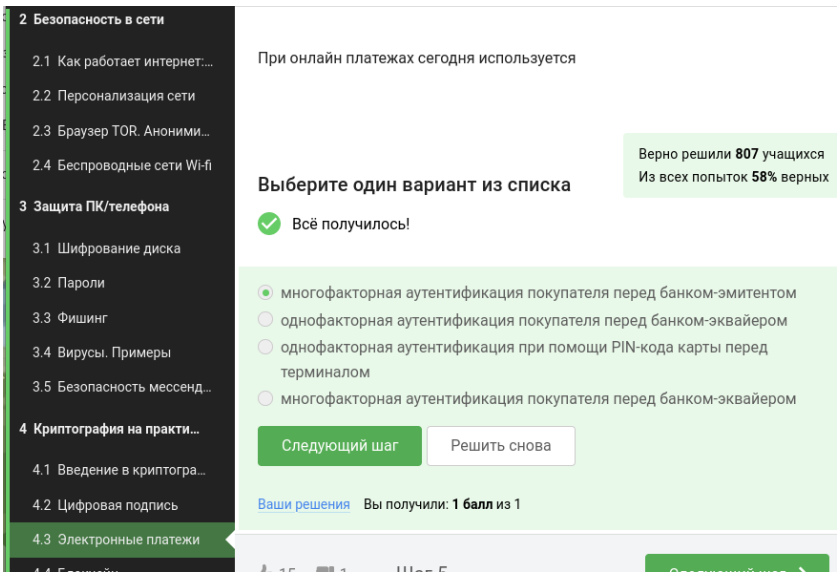

Рис. 3.13: Тест 13

Рассмотрим, наконец, одно из этих доказательств, например, доказательство работы, потому что оно сегодня самое популярное, поскольку оно используется в биткоине, самой распространённой криптовалюте. Как работает доказательство работы? Тут мы с вами вспоминаем старую добрую криптографическую хэш-функцию, это функция, которая берет на вход любые данные и выдает за какое-то быстрое время фиксированное число бит. И задача майнера в доказательстве работы - это отыскать такой вход в хэш-функцию, что ее значение имеет определенный паттерн, иными словами, отыскать такой x, что h(x) имеет, например, 17 первых нулей или 17 первых единиц, это неважно. В биткоине используют 18 или 19 первых нулей. Это число на самом деле может быть модифицировано относительно производительности сети в тот или иной момент времени. (рис. 3.14).

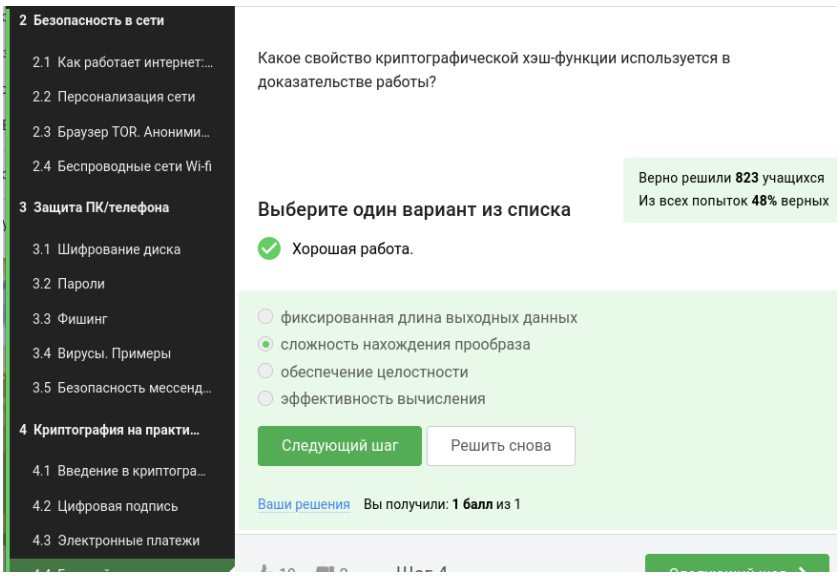

Рис. 3.14: Тест 14

В основе блокчейна лежит консенсус — — публичная структура данных или леджер (бухгалтерская книга), которая обеспечивает • постоянство добавленные когда-либо данные не могут быть удалены • консенсус все участники видят одни и те же данные (за исключением последних пары блоков) • живучесть участники могут добавлять новые транзакции • открытость (не для всех блокчейнов) любой может стать участником блокчейна (рис. 3.15).

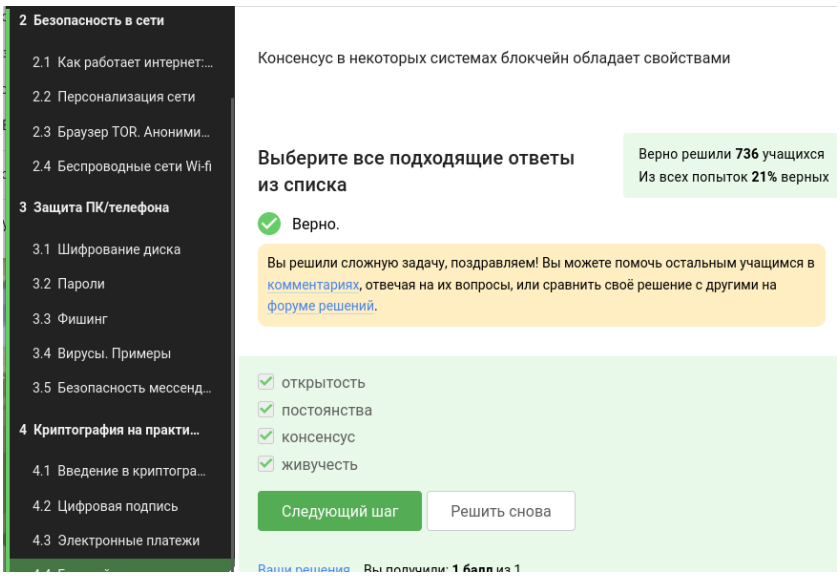

Рис. 3.15: Тест 15

Важно то, что у каждого участника есть свой секретный ключ, и своим секретным ключом мы всегда будем подтверждать какую-то транзакцию. Важно то, что этот ключ у нас секретный, мы его используем для подписи. Подпись – это и есть подтверждение моей транзакции. Мы с вами разбирали в одной из лекций, как работает электронная цифровая подпись, у этого примитива есть секретный и открытый ключи, и наш секретный ключ - это то, что позволяет нам совершать транзакции от нашего лица. (рис. 3.16).

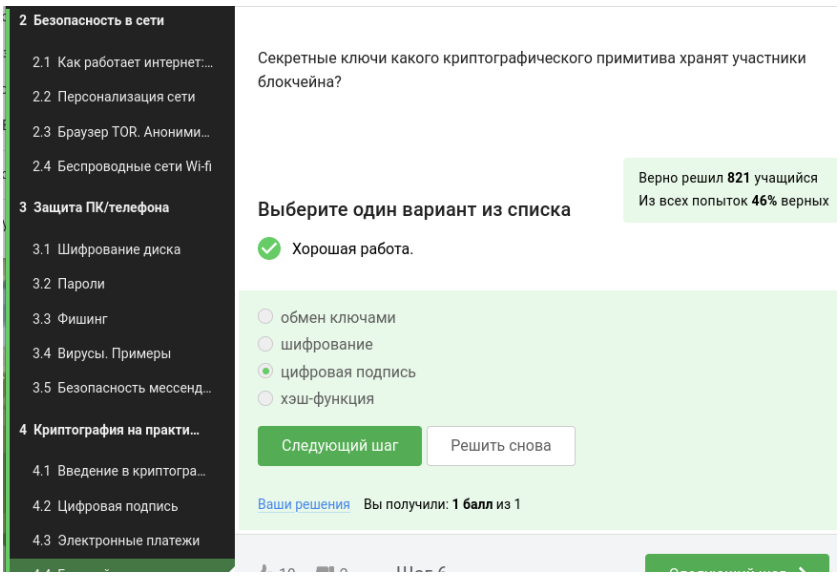

Рис. 3.16: Тест 16

4 Выводы

Мы рассмотрели что такое криптография на практике. Узнали для чего нужна цифровая подпись и как работают электронный платежи. Разобрались откуда появился блокчейн и как он работает.