Внешний курс. Блок 3: Криптография на практике

#### Основы информационной безопасности

Талебу Тенке Франк Устон

Содержание

1. [Цель работы 5](#_TOC_250006)
2. [Выполнение блока 3: Криптография на практике 6](#_TOC_250005)
   1. [Введение в криптографию . . . . . . . . . . . . . . . . . . . . . . . . 6](#_TOC_250004)
   2. [Цифровая подпись . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8](#_TOC_250003)
   3. [Электронные платежи 11](#_TOC_250002)
   4. [Блокчейн 12](#_TOC_250001)
3. [Выводы 15](#_TOC_250000)

Список иллюстраций

|  |  |  |
| --- | --- | --- |
| 2.1 Вопрос 4.1.1 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
| 2.2 Вопрос 4.1.2 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 7 |
| 2.3 Вопрос 4.1.3 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 7 |
| 2.4 Вопрос 4.1.4 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 8 |
| 2.5 Вопрос 4.1.5 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 8 |
| 2.6 Вопрос 4.2.1 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 9 |
| 2.7 Вопрос 4.2.2 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 9 |
| 2.8 Вопрос 4.2.3 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 10 |
| 2.9 Вопрос 4.2.4 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 10 |
| 2.10 Вопрос 4.2.5 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 11 |
| 2.11 Вопрос 4.3.1 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 11 |
| 2.12 Вопрос 4.3.2 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 12 |
| 2.13 Вопрос 4.3.3 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 12 |
| 2.14 Вопрос 4.4.1 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 13 |
| 2.15 Вопрос 4.4.2 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 13 |
| 2.16 Вопрос 4.4.3 | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 14 |

Список таблиц

# Цель работы

Пройти третий блок курса “Основы кибербезопасности”

## Выполнение блока 3: Криптография на практике

### Введение в криптографию

Для ответа на вопрос используется определение ассмиетричного шифрования с двумя ключами (рис. 2.1).

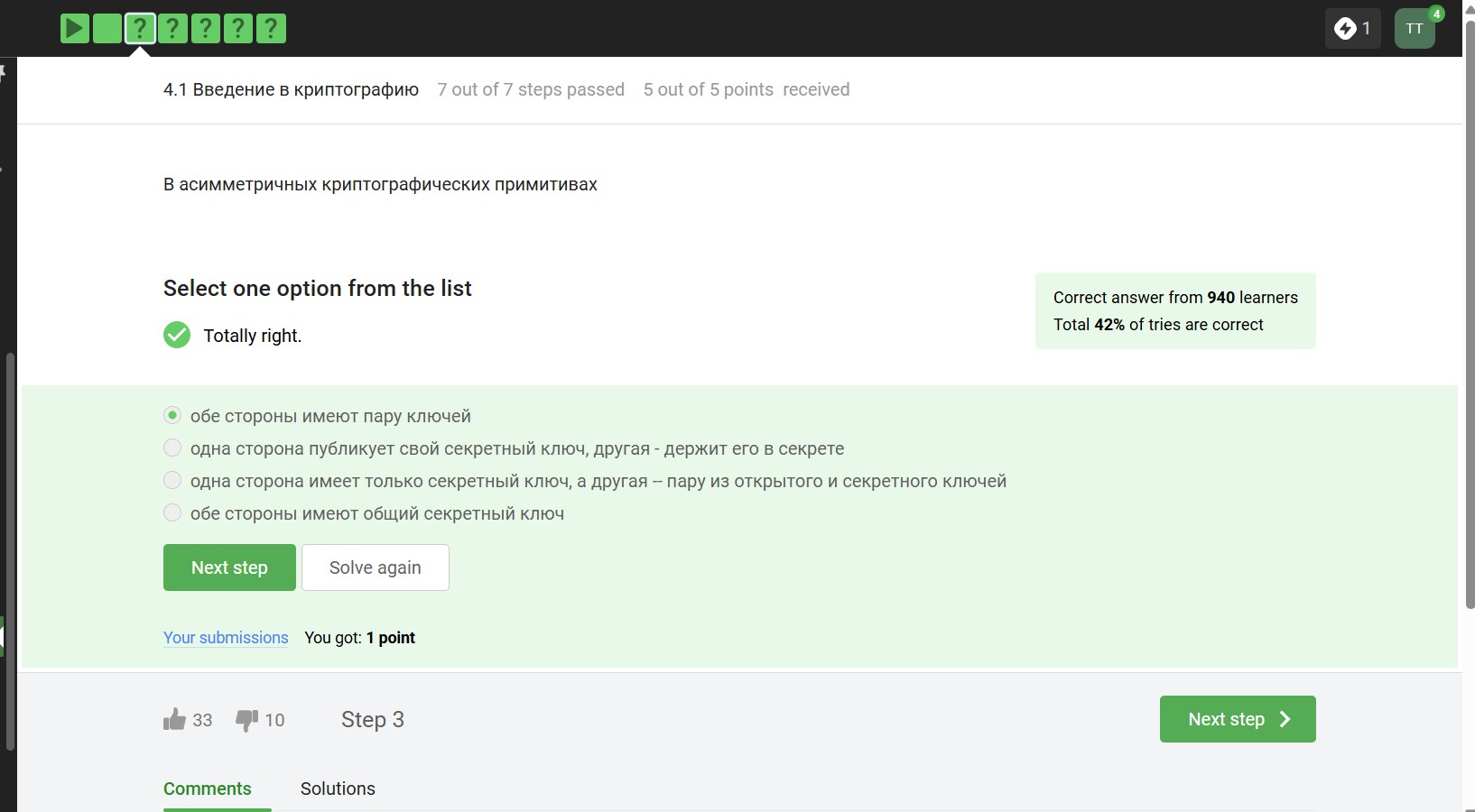


Рис. 2.1: Вопрос 4.1.1

Отмечены основные условия для криптографической хэш-функции (рис. 2.2).

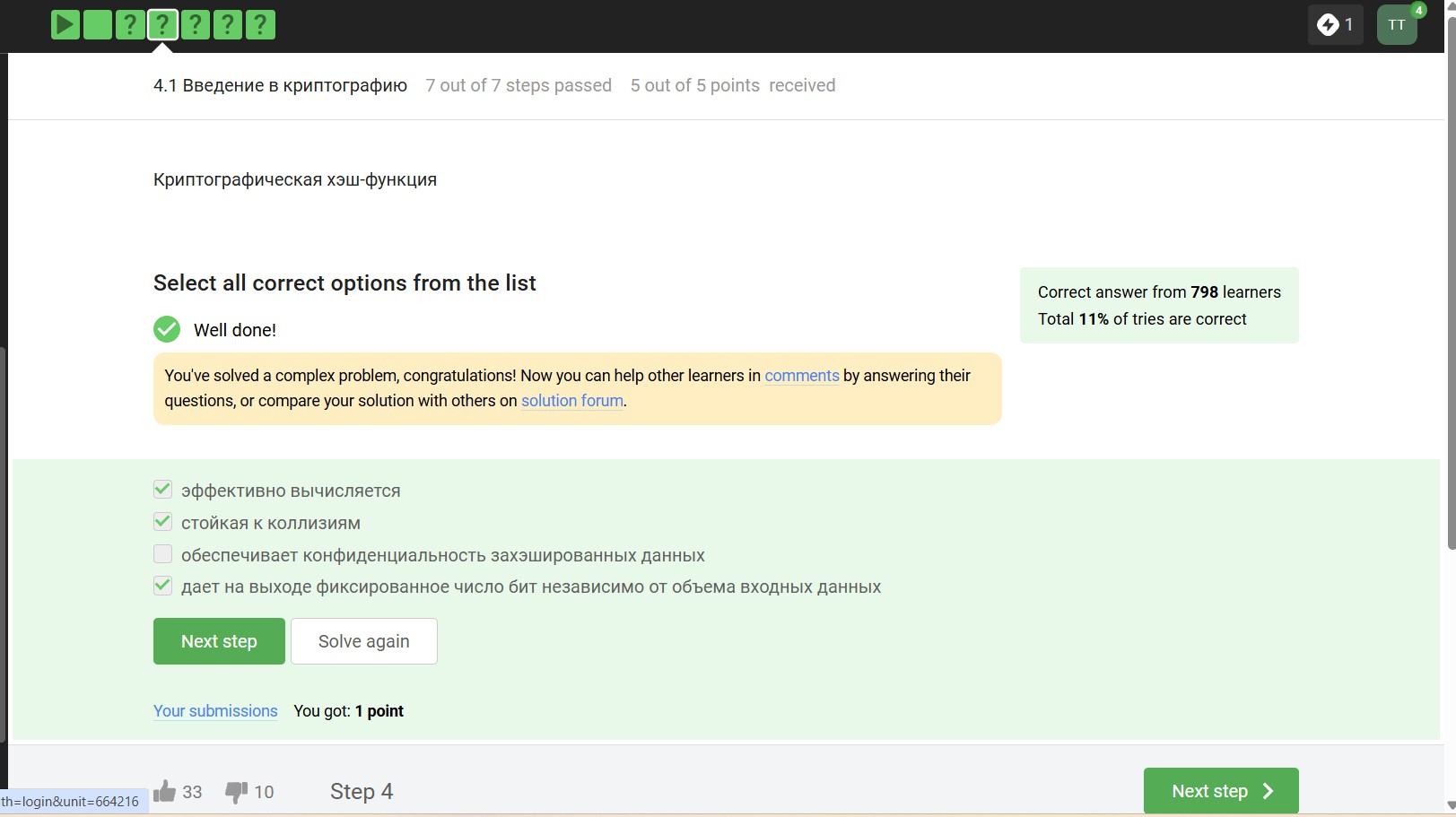


Рис. 2.2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 2.3).

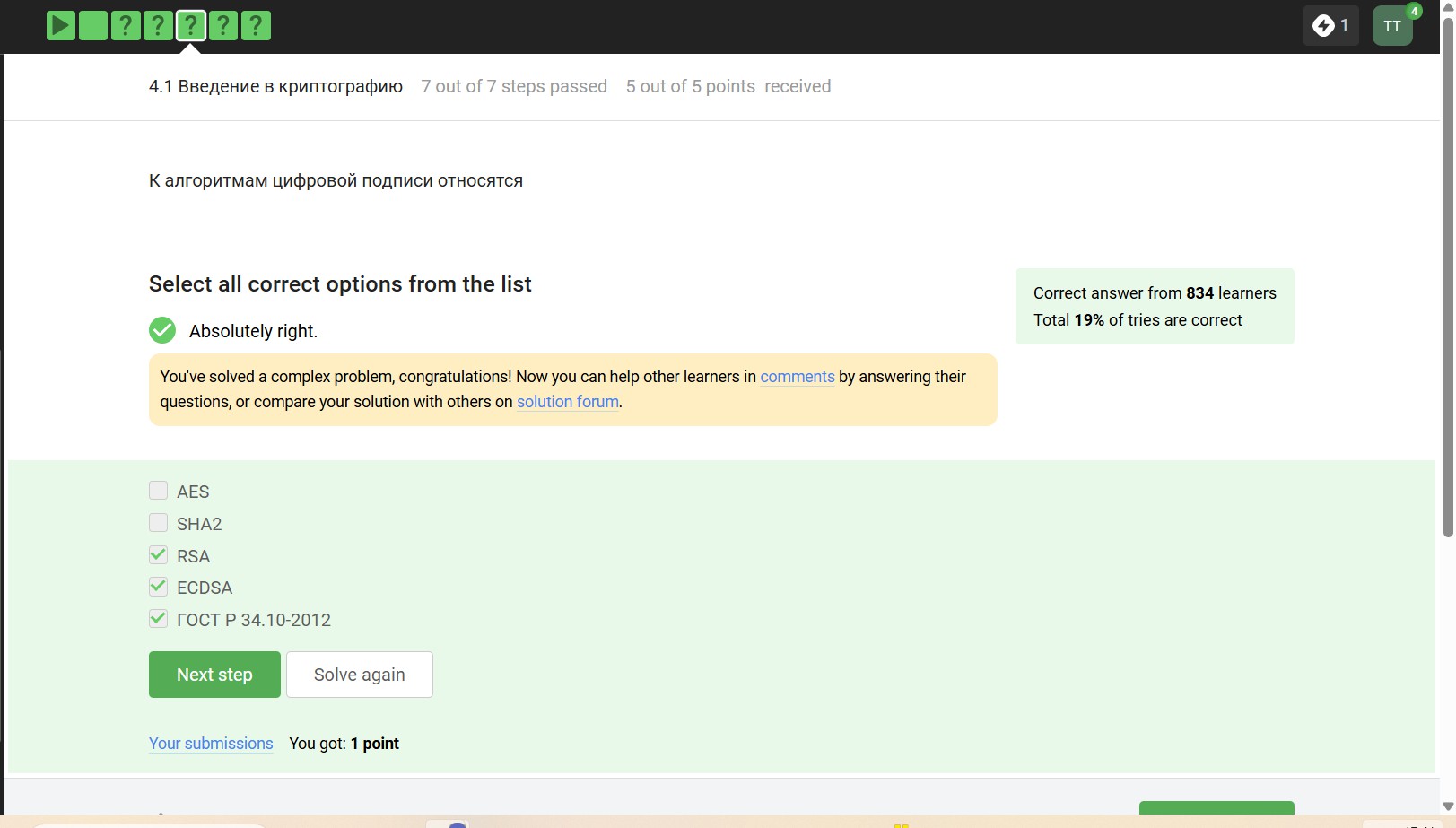


Рис. 2.3: Вопрос 4.1.3

В информационной безопасности аутентификация сообщения или аутентифи- кация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения (рис. 2.4)

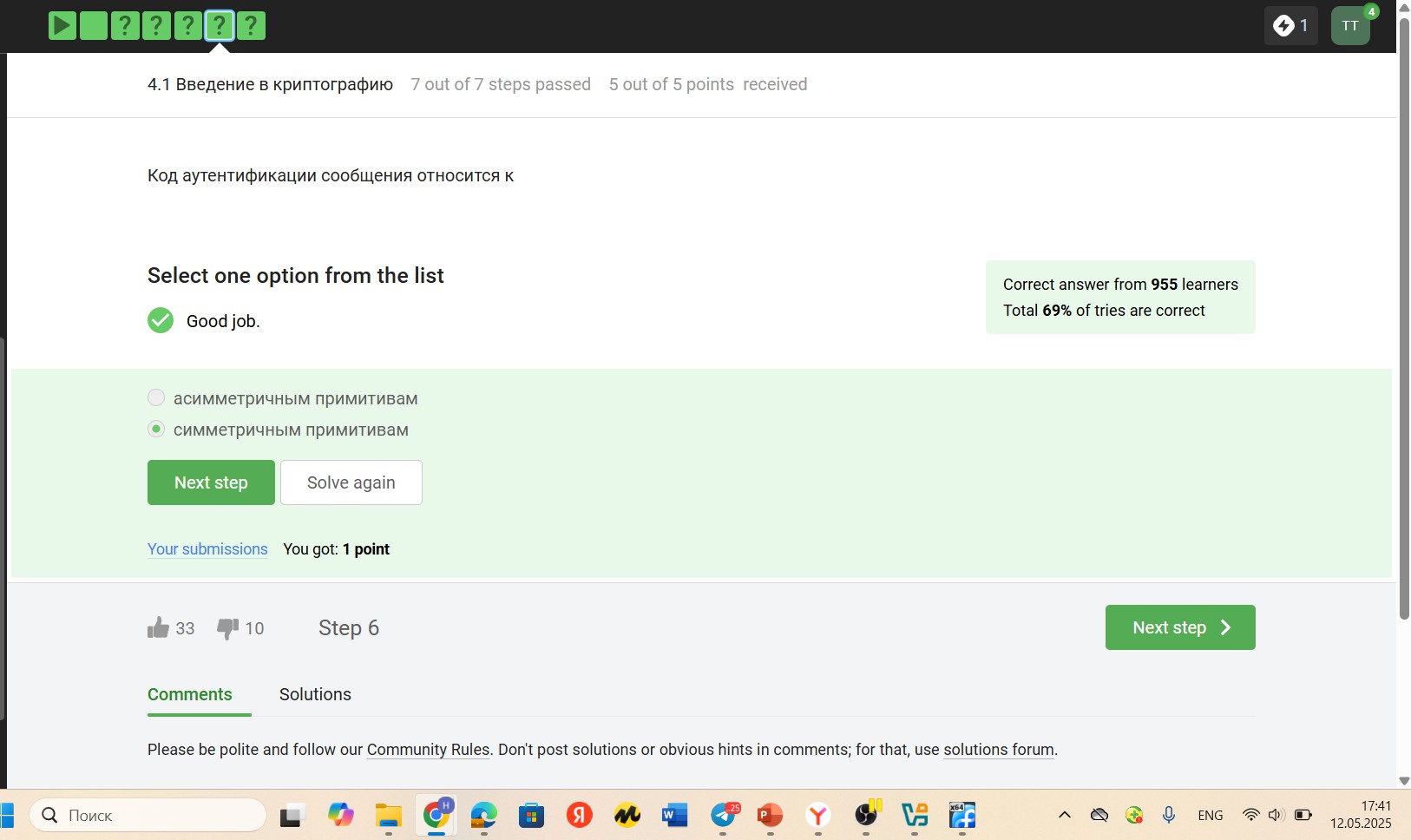


Рис. 2.4: Вопрос 4.1.4

Определение обмена ключами Диффи-Хэллмана. (рис. 2.5).

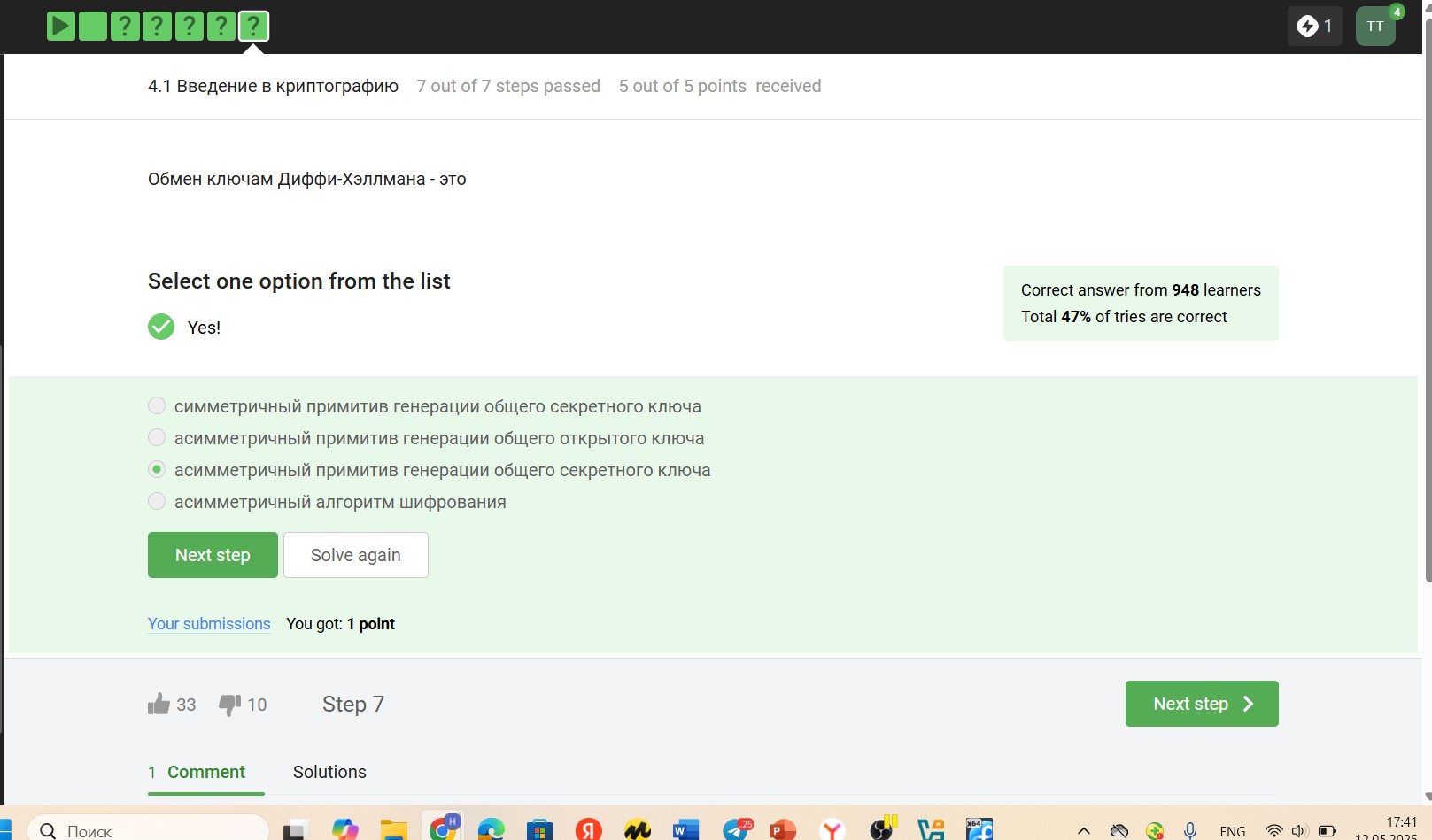


Рис. 2.5: Вопрос 4.1.5

### Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом (рис. 2.6).

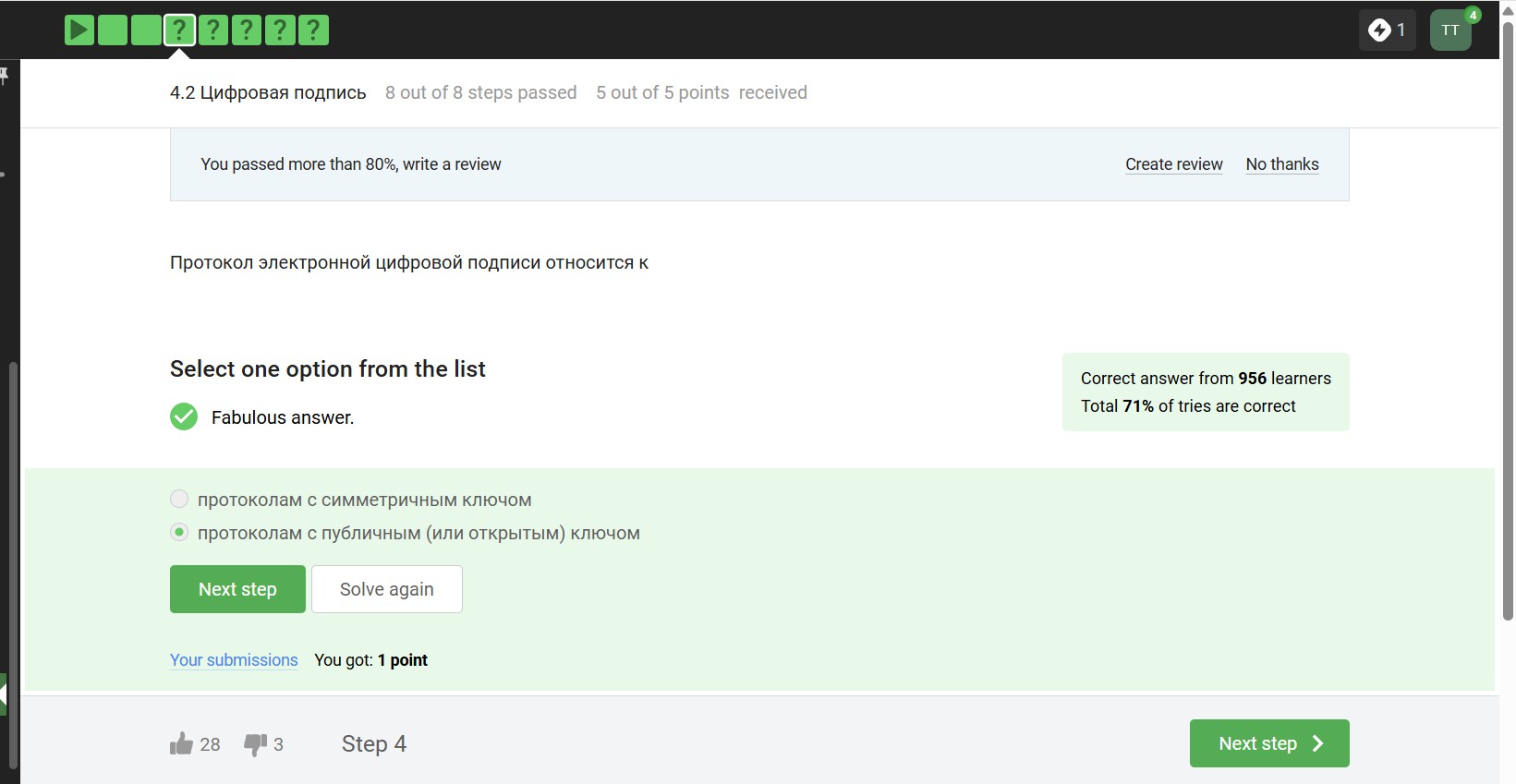


Рис. 2.6: Вопрос 4.2.1

лгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный вариант хэш-функции подпи- санного документа. На втором этапе происходит расшифровка хэш-функции, со- держащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш- функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства (рис. 2.7).

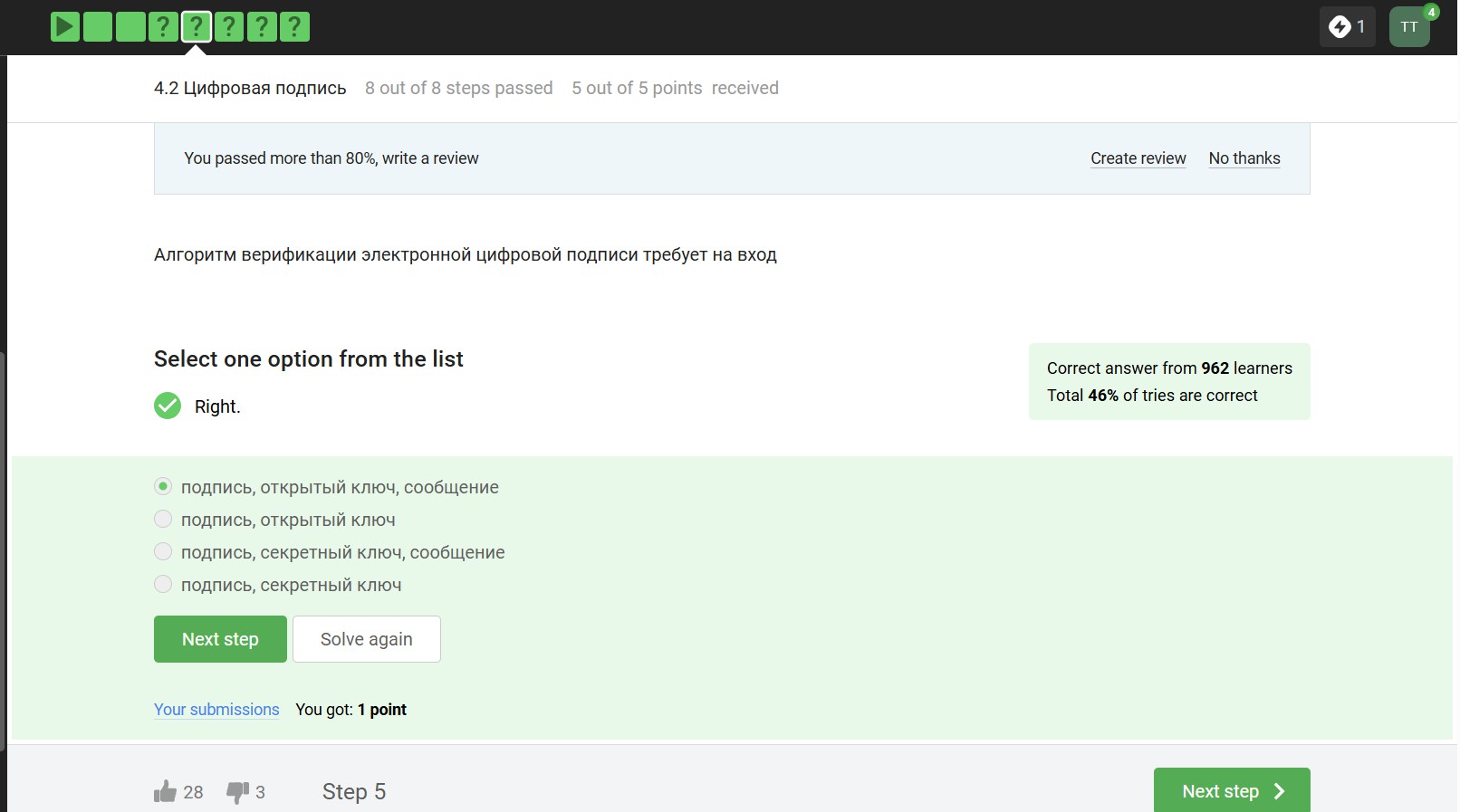


Рис. 2.7: Вопрос 4.2.2

Электронная подпись обеспечивает все указанное, кроме конфиденциальности (рис. 2.8).

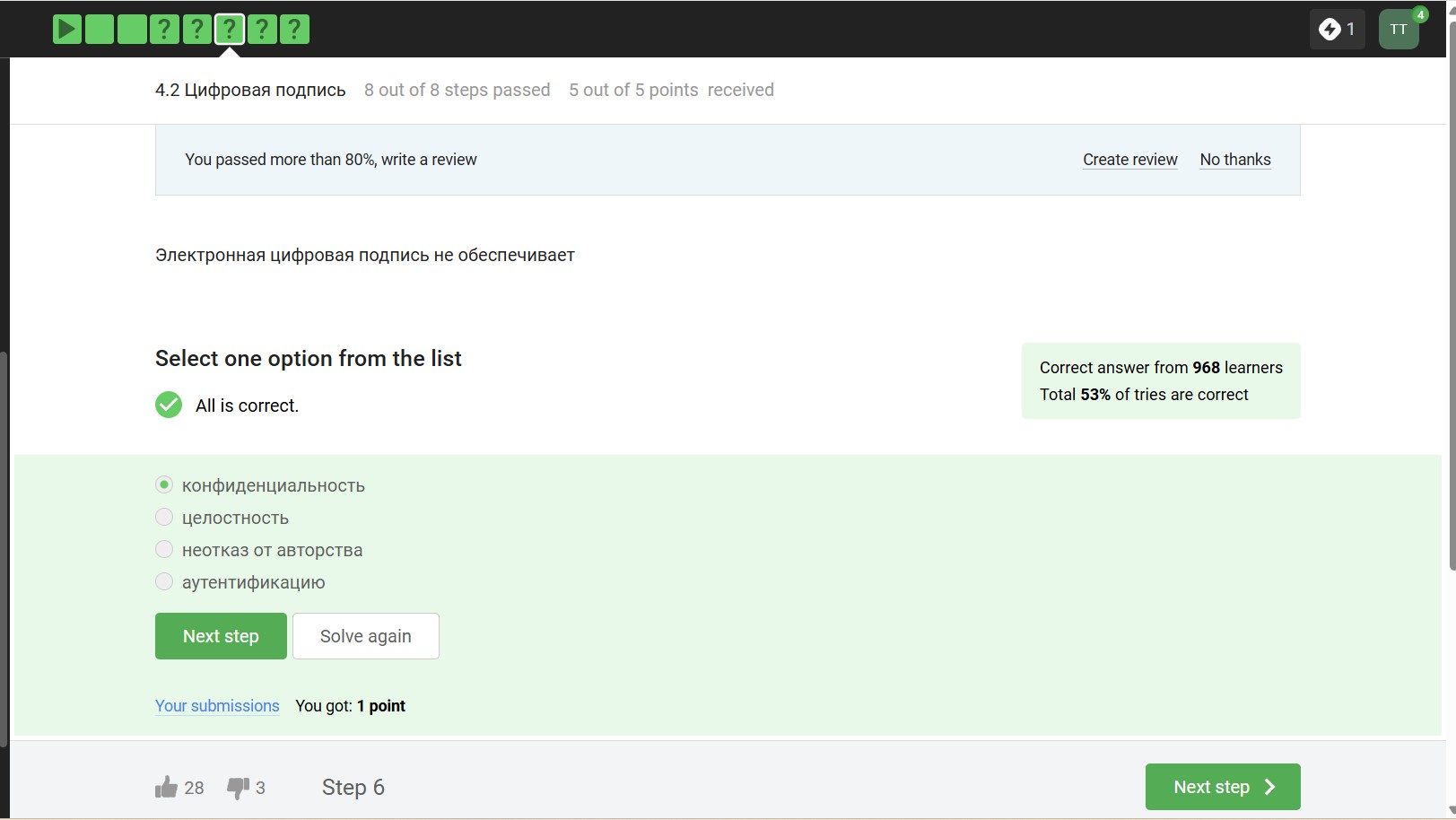


Рис. 2.8: Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифи- цированная электронная подпись (рис. 2.9).

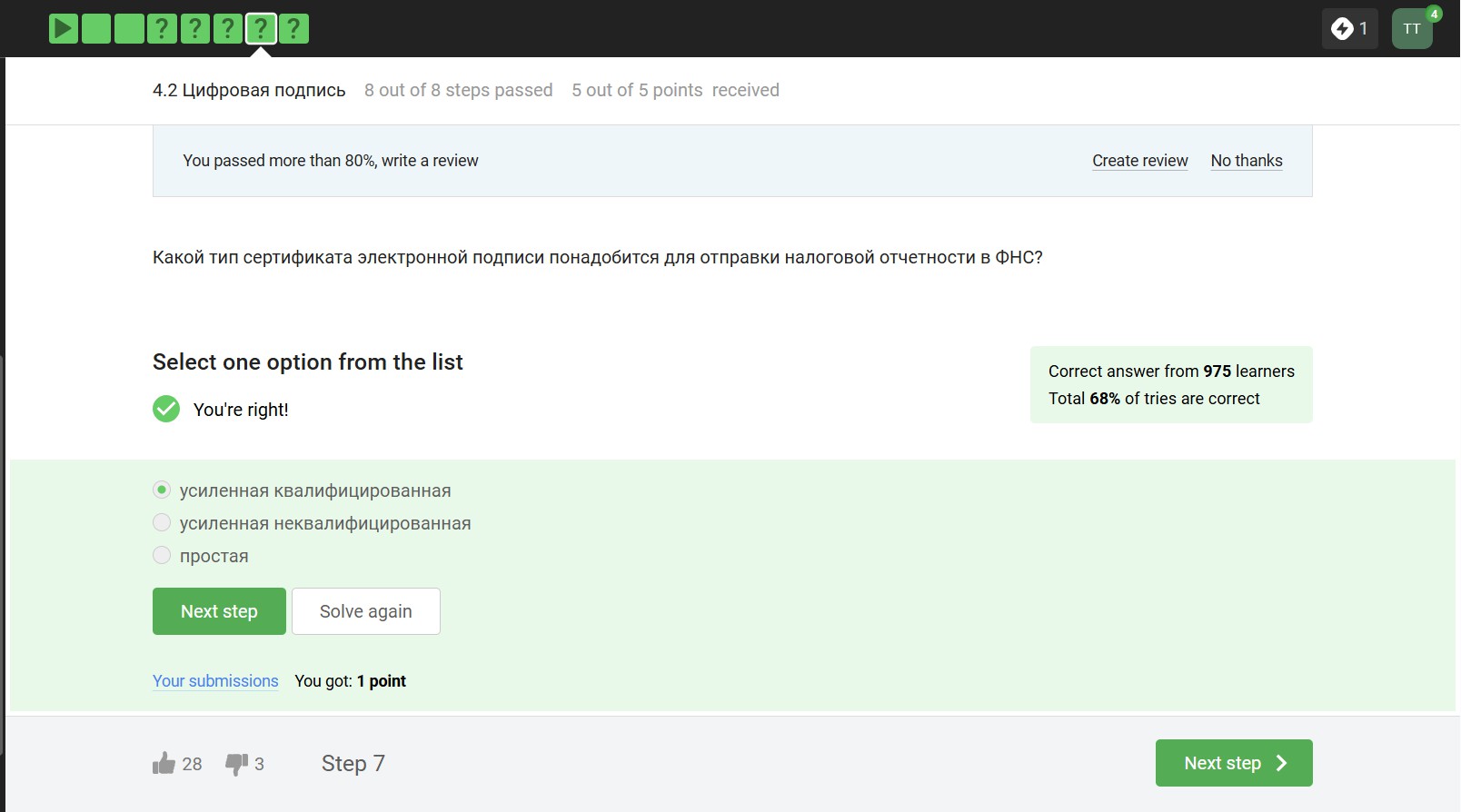


Рис. 2.9: Вопрос 4.2.4

Верный ответ укзаан на изображении (рис. 2.10).

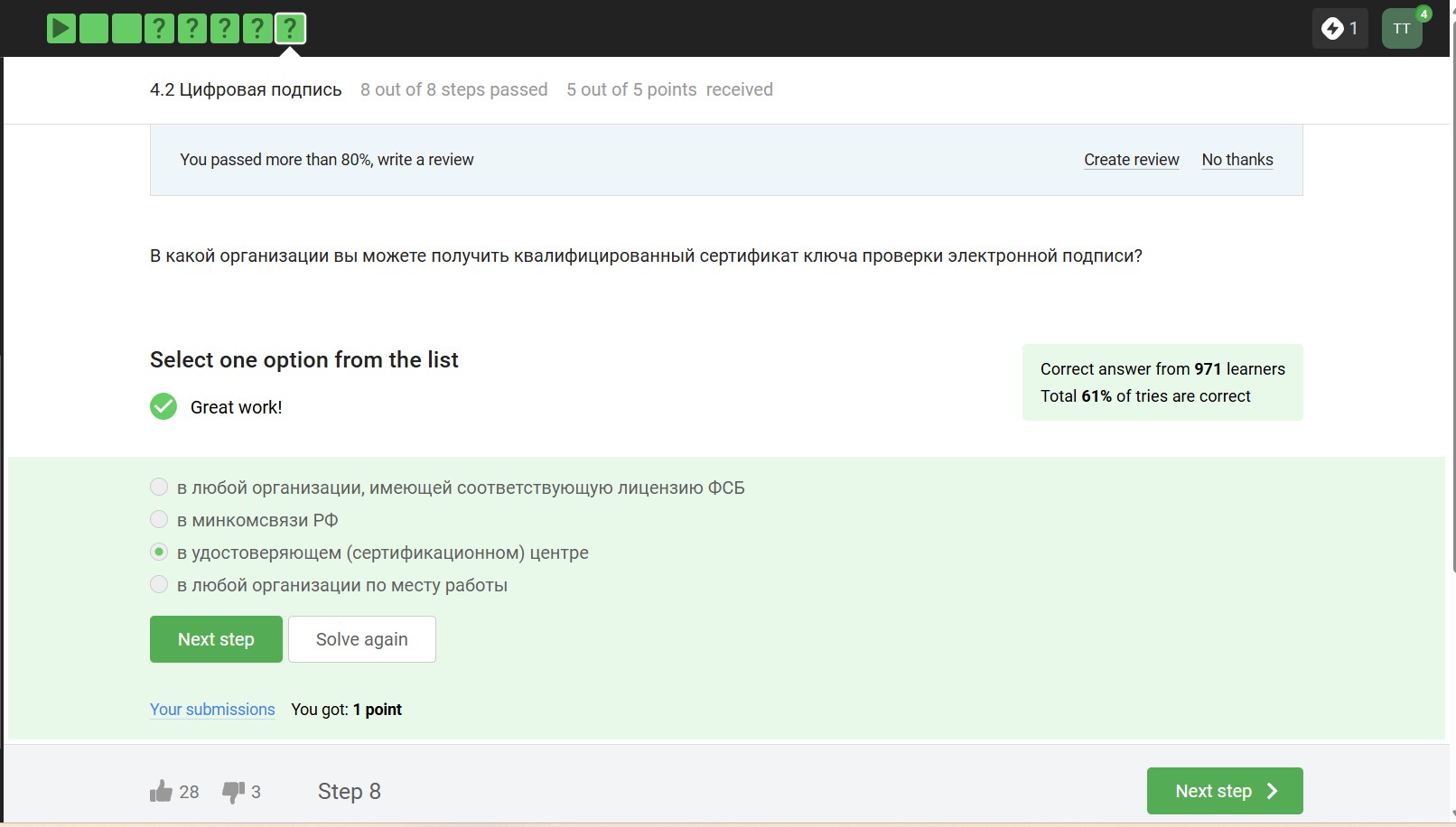


Рис. 2.10: Вопрос 4.2.5

### Электронные платежи

Известные платежные системы - Visa, MasterCard, МИР (рис. 2.11).

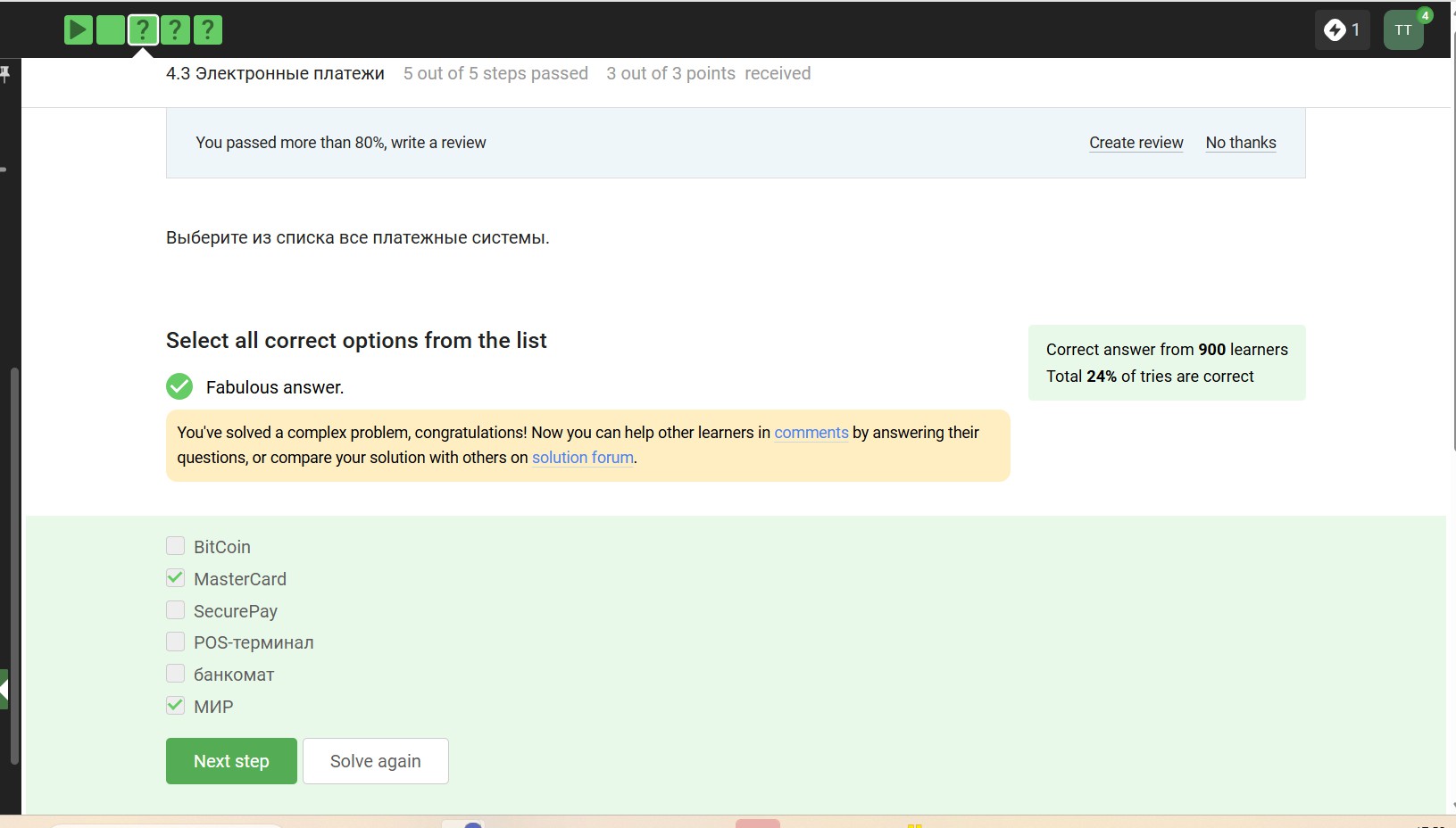


Рис. 2.11: Вопрос 4.3.1

Верный ответ на изображении (рис. 2.12).

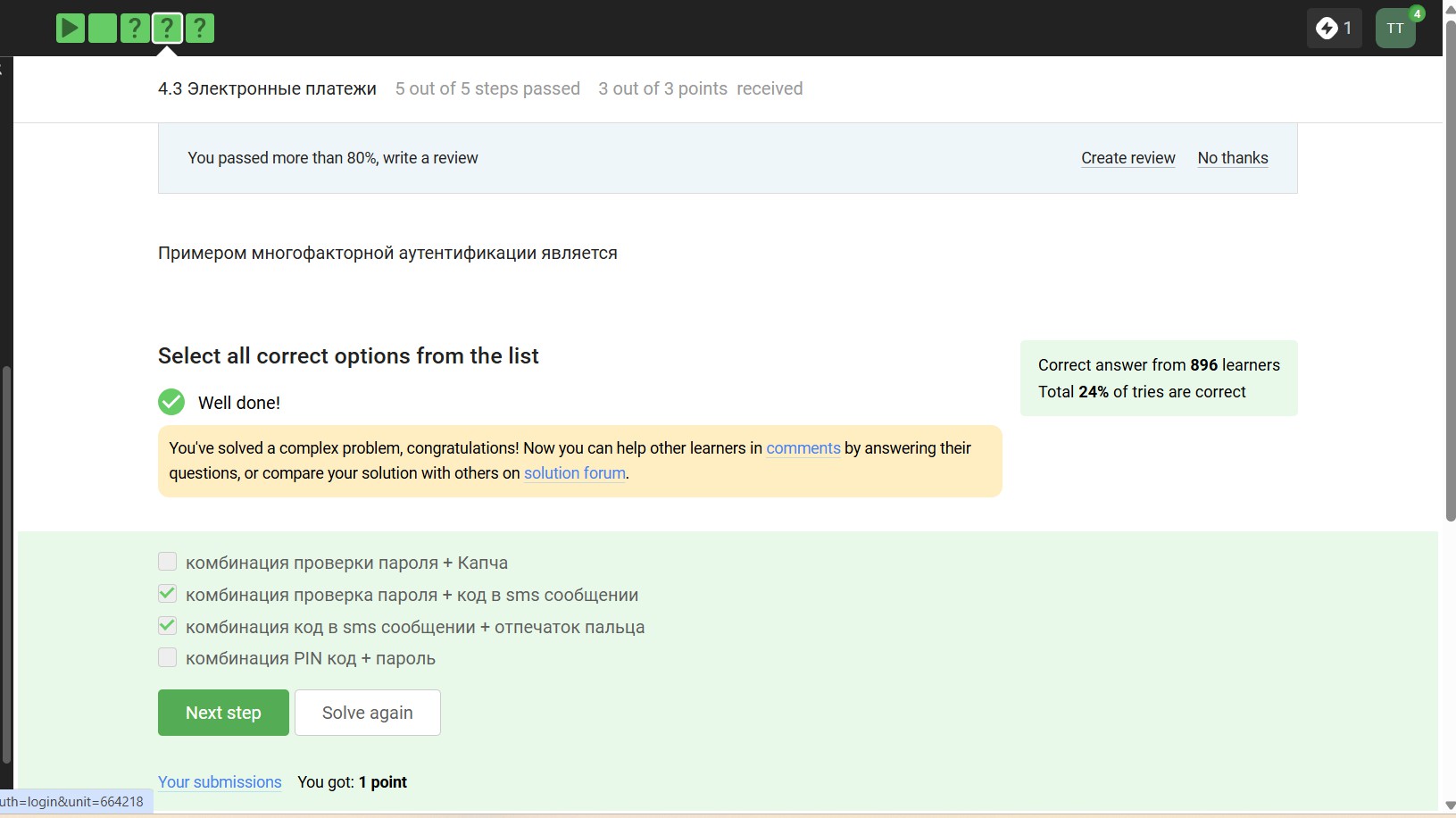


Рис. 2.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация (рис.

2.13).

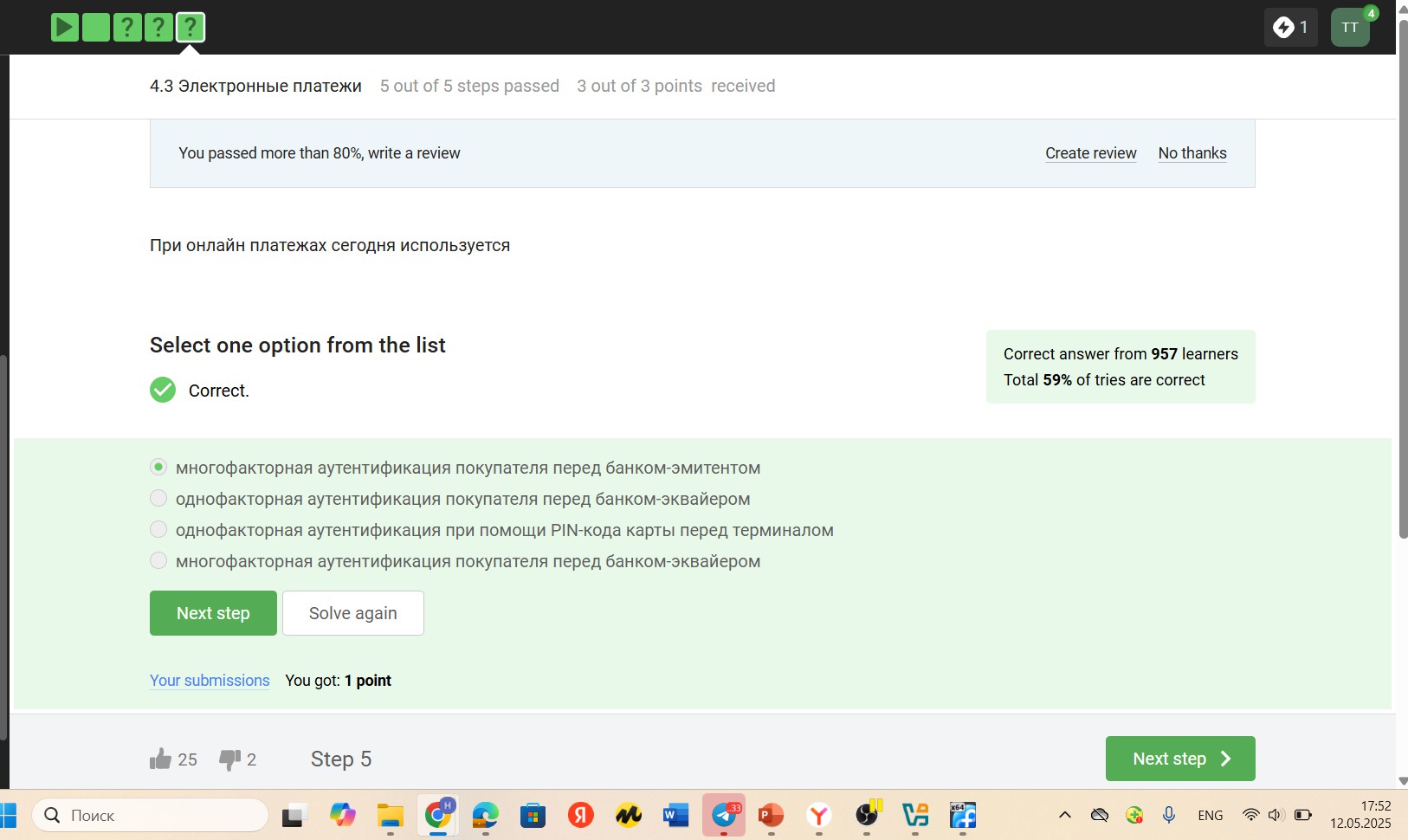


Рис. 2.13: Вопрос 4.3.3

### Блокчейн

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне; он используется для подтверждения тран- закций и создания новых блоков. С помощью PoW майнеры конкурируют друг с другом за завершение транзакций в сети и за вознаграждение. Пользователи

сети отправляют друг другу цифровые токены, после чего все транзакции соби- раются в блоки и записываются в распределенный реестр, то есть в блокчейн. (рис. 2.14).

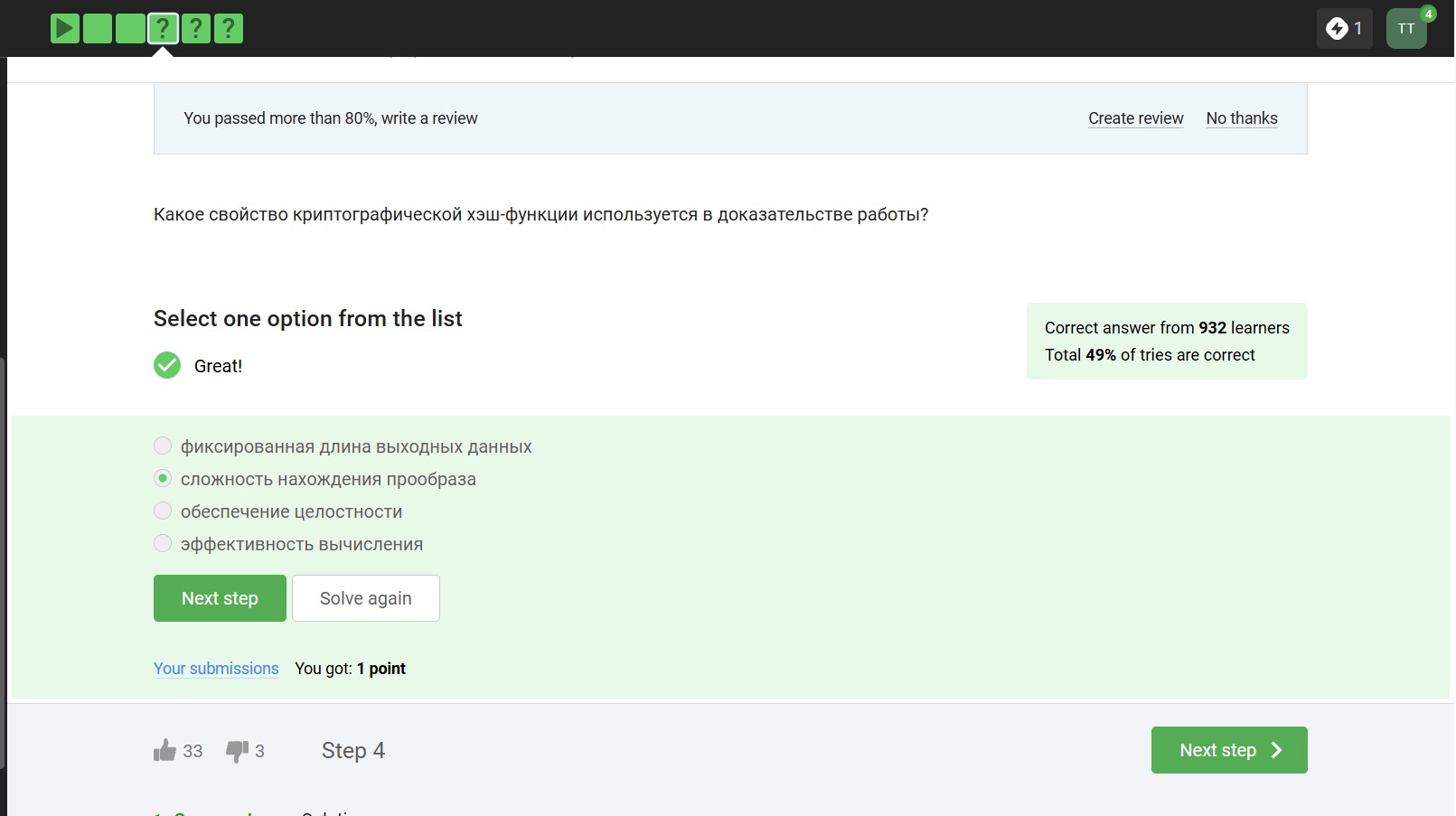


Рис. 2.14: Вопрос 4.4.1

Консенсус блокчейна — это процедура, в ходе которой участники сети дости- гают согласия о текущем состоянии данных в сети. Благодаря этому алгоритмы консенсуса устанавливают надежность и доверие к самоу сети. (рис. 2.15).

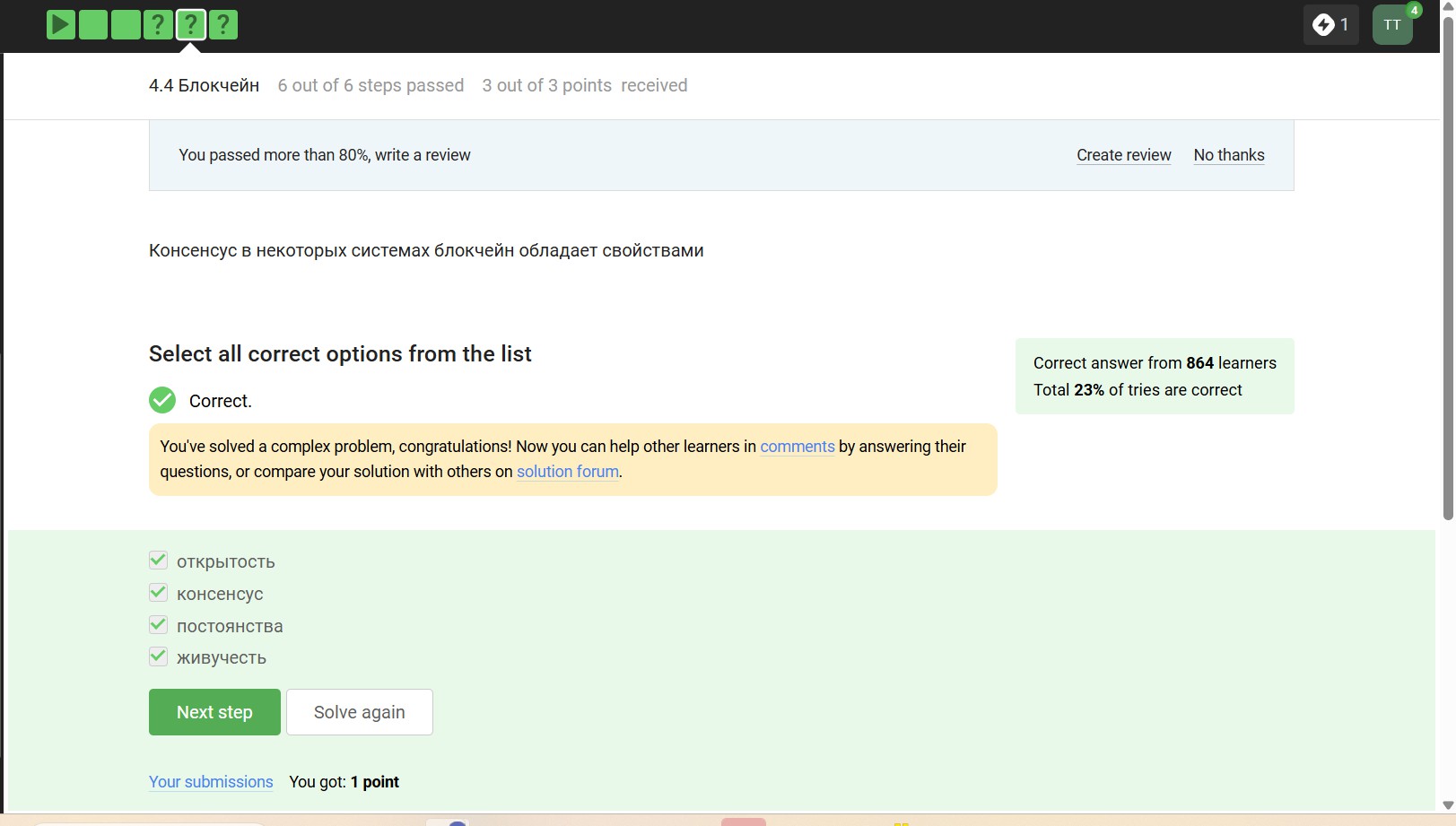


Рис. 2.15: Вопрос 4.4.2

Ответ - цифровая подпись (рис. 2.16).

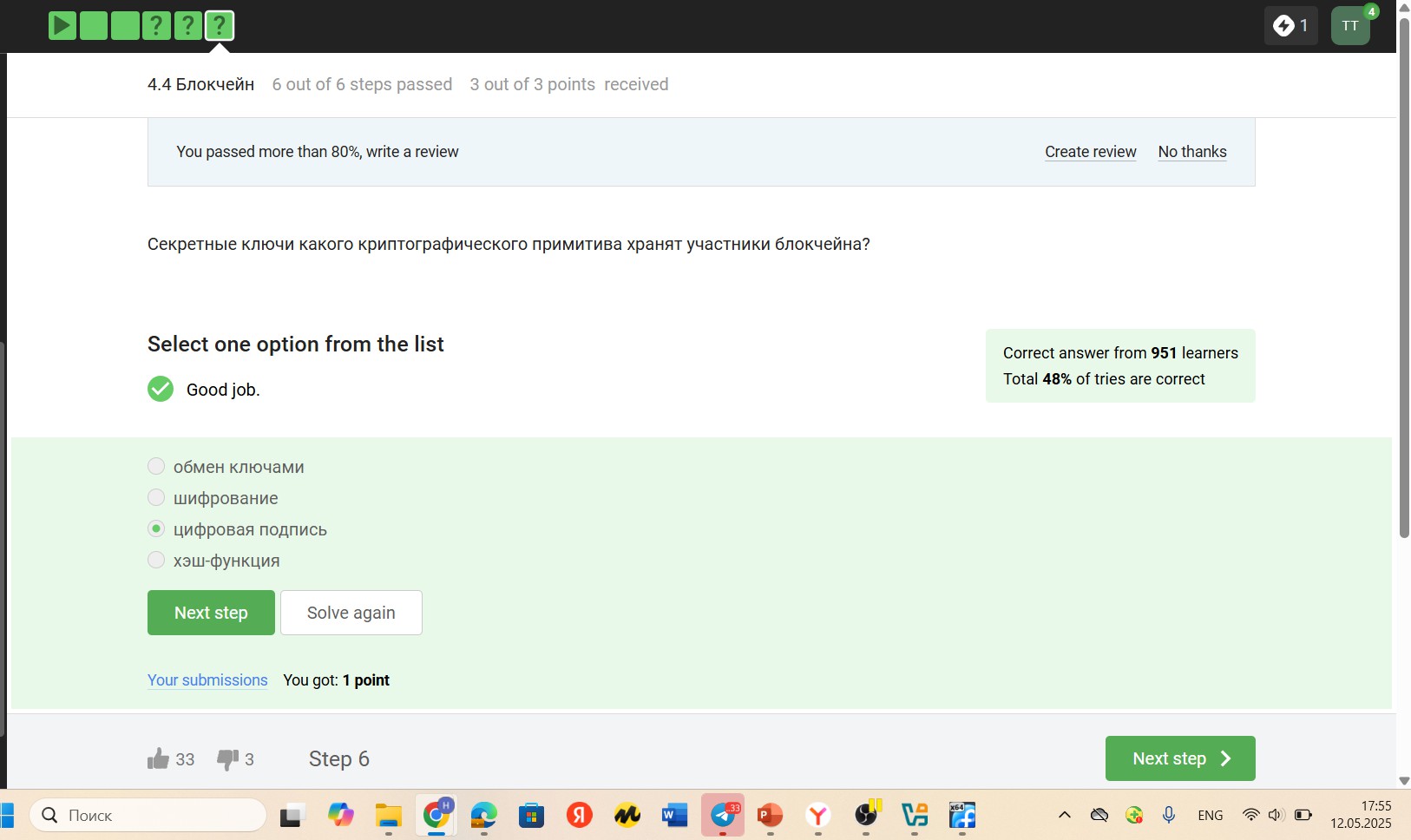


Рис. 2.16: Вопрос 4.4.3

# Выводы

Я прошла третий блок