



Блокчейн-игра

Построй свою цепочку





Каждая команда — это команда майнеров.

Майнеры собирают несколько транзакций в один блок и добавляют его в единую цепочку блоков.



Для создания блока требуется:

- провести математические операции с транзакциями;
- записать их в блок определённым образом.

После этого блок можно отправить на проверку.



Проверкой блока занимаются сами майнеры.

Только проверенные блоки отправляются в цепочку.

За каждый успешно добавленный к цепочке блок майнеры получают вознаграждение



Сыграем?!

Но сначала изучим
правила



1. СОЗДАДИМ КЛЮЧИ

Ключи помогут нам подписать блок, чтобы остальные майнеры (и Вим Вивальди) знали, кто именно добавил блок в цепочку и кто получит за него вознаграждение



Как создать ключи?

Секретный ключ: любое целое число от 1 до 20

Публичный ключ: секретный ключ * целое число от 1 до 7

Например:

Секретный ключ: 2

Публичный ключ: 10 ($2 * 5$)



2. ВЫБИРАЕМ ТРАНЗАКЦИИ

1. Илья → Диане: 5

1. Ева → Фёдору: 8

2. Мансур → Глебу: 7



БЛОК



Как выглядит транзакция?





2. СЧИТАЕМ ХЕШ БЛОКА

Хеш переводится как нарезка, фарш.

Ведь если мы положим мясо в мясорубку или порежем его ножом, то собрать кусок мяса назад мы уже не сможем.

То же самое происходит с транзакциями после хеширования...



Хеш блока состоит из...

Хеш вознаграждения майнерам за
обработку всех транзакций

$$X_{\text{Блок}N} = X_{\text{Tr}1} + X_{\text{Tr}2} + X_{\text{Tr}3} + X_{\text{возн}} + X_{\text{Блок}N-1}$$

Хеш текущего
блока

Сумма хешей всех
транзакций

Хеш
предыдущего
блока



Считаем хэш транзакции

1. Илья → Диане. 5

Вознаграждения
майнера

Отправитель
транзакции

Получатель
транзакции

Сумма транзакции



Считаем хэш транзакции

1. Илья → Диане. 5

Вознаграждения майнера
переносим в отдельную
транзакцию



Переводим буквы в цифры
(А→1, б→2 и т.д.)



Складываем все цифры,
включая сумму транзакцию



Считаем хеш транзакции

1. **Илья → Диане: 5**

$$10+13+30+33 \quad + \quad 5+10+1+15+6 \quad +5 \quad = \mathbf{128}$$

Сумму вознаграждения переносим в отдельную транзакцию. Её мы посчитаем отдельно

Переводим буквы в цифры
(А→1, б→2 и т.д.)

Не забываем про сумму транзакции

Складываем все цифры и получаем хеш транзакции. В нашем примере хеш = **128**



А как же наше вознаграждение?

Вимме → [Мы]: сумма вознаграждения

Сумма вознаграждения отправителей
за все транзакций

Отправитель
никогда
НЕ МЕНЯЕТСЯ

Указываем название нашей команды,
например, «Майнеры»



Хеш транзакции вознаграждения

Вимме → Майнеры: 5+8+7

$$3+10+14+14+6 \quad + \quad 14+1+11+15+6+18+29 \quad +1+1+2 \quad = \mathbf{145}$$

Переводим буквы в цифры
(А→1, б→2 и т.д.)

Сумма всех
вознаграждений за
транзакции в блоке

Складываем все цифры и получаем хеш транзакции вознаграждения. В нашем примере хеш = **145**



Например

1. Илья → Диане: 5

1. Ева → Фёдору: 8

2. Мансур → Глебу: 7



Например

Сеть → Майнеры: 5+1+4 монет	$3+10+14+14+6+14+1+11+15+6+18+29+1+1+2=145$
Илья → Диане: 5 монет	$10+13+30+33+5+10+1+15+6+5=128$
Ева → Фёдору: 8 монет	$6+3+1+22+7+5+16+18+21+8=107$
Мансур → Глебу: 7 монет	$14+1+15+19+21+18+4+13+6+2+21+7=141$
Хэш предыдущего блока	0
Итого:	521



3. СЧИТАЕМ NONCE

Nonce — это аббревиатура от **Number that can only be used once**

Расчёт *Nonce* доказывает остальным майнерам (и Виму Вивальди) что команда провела нужное количество работы над блоком.



Рассчитываем nonce

Мы будем искать такое число nonce, чтобы сумма хеш блока+nonce делилась на 10 без остатка.

Например:

$$\frac{521+9}{10} = \mathbf{53}$$

$$\mathbf{nonce = 9}$$



4. ПОДПИСЫВАЕМ БЛОК

Чтобы подписать блок, нам будет нужен секретный ключ (который мы придумали ранее) и хеш блока (который мы посчитали). Подпись блока поможет Виму Вивальди понять, кто добавил блок в цепочку.



Подписываем блок

**Подпись блока = Хеш блока * секретный
ключ * ранее задуманное число от 1 до 7**

В нашем пример это

$$521 * 2 * 5 = 5210$$



5. ЗАПОЛНЯЕМ КАРТОЧКУ БЛОК

У нас есть всё необходимое для заполнения карточки, и есть бланк карточки.
Теперь главное не ошибиться



Заполняем карточку блоков

Номер блока	
Хеш предыдущего блока	0
Хеш текущего блока	521
Nonce	9
Список транзакций	Сеть → Майнеры: 1+1+2 монет Илья → Диане: 5 монет Ева → Фёдору: 8 монет Мансур → Глебу: 7 монет
Подпись	5210



6. ПРОВЕРЯЕМ КАРТОЧКУ БЛОК

У нас есть всё необходимое для заполнения карточки, и есть бланк карточки.

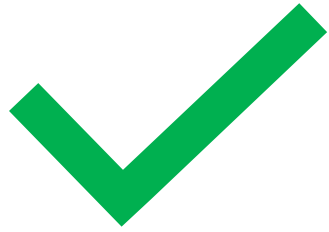
Теперь главное не ошибиться

Карточки проверяют все команды!



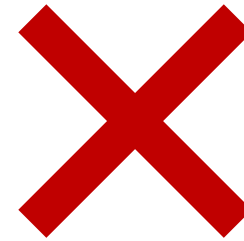
Параметры проверки

- Правильность хеша **предыдущего блока** (они должны совпадать).
- Правильность **расчёта хеша** текущего блока.
- Правильность **Nonce**: Nonce + Хеш делится на 10 без остатка.
- Наличие средств у отправителей транзакций на момент её проведения.
- Соответствие подписи (подпись=хеш \times публичный ключ команды майнеров)



Команда получает:

- вознаграждение в 5 монет
- комиссию
- её блок добавляется в цепочку



Команда теряет 5 монет

Транзакции блока
возвращаются на доску и
доступны для обработки