

Блокчейн-игра. Построй свою цепочку

Цель игры:

Смоделировать работу блокчейна Биткойна, наглядно показать школьникам:

1. Как транзакции объединяются в блоки и проверяются сетью.
2. Почему блокчейн защищён от подделок благодаря хешированию и децентрализации.
3. Роль майнинга и консенсуса в поддержании безопасности сети.
- 4*. Как можно атаковать блокчейн? На примере «атака 51%».

Легенда игры

В этот раз Вим Вивальди предлагает игрокам попробовать один из способов защиты записей о суммах, которые он одалживает и получает назад.

Этот способ использует его приятель Джакомо Чианфанелли, владелец одноимённого банка. У Джакомо схожая проблема, но связана она с тем, что Чианфанелли это очень большой банк с отделениями сразу в нескольких городах. Клиент банка может, например, взять кредит в Элландере, а вернуть его долг может совсем другой человек где-нибудь в Ковире. Все эти переводы и пополнения как-то надо сохранять; при этом о них должны знать в каждом банке.

У Джакомо получилось придумать хитрый способ записи, и Вим хочет проверить, можно ли подобное проверить в его банке.

Суть игры

Участники разбиваются на команды.

Каждая команда участников — это команда майнеров. Майнеры в рамках игры собирает несколько **транзакций** в один **блок** и добавляет блок единую **цепь блоков**, буквально **блокчейн**.

Для создания **блока** необходимо провести определённые математические операции с **транзакциями**, и оформить (записать) **блок** определённым образом. После этого **блок** можно отправить на проверку: этим также занимаются майнеры. Только проверенные **блоки** отправляются в цепочку. За каждый успешно добавленный к цепочке блок команда **майнеров** получает вознаграждение.

Для справки:

Майнер (англ. *mining* — добыча полезных ископаемых) — человек или группа людей, которые создают новые структуры (обычно речь идёт о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ (таких, как биткойн).

Подготовка к игре

Деление на команды майнеров по 4-5 человек (в рамках 1 этапа урока «Связанные одной цепью» уже проведено).

Знакомство с презентацией к игре **с объяснением правил** (Приложение 3).

Ведущий игры (организатор) управляет игрой (вводит транзакции и контролирует атаки).

Материалы игры:

Карточки транзакций (Приложение №4)	На карточках размещены единичные транзакции в формате: « Комиссия. Отправитель → Получатель: Сумма». Карточки транзакций распечатываются, разрезаются и размещаются на доске (флипчарте). Карточки видны всем командам в равной степени.
Карточки блоков (Приложение №5)	Пустые шаблоны с полями: - Номер блока. - Хеш предыдущего блока. - Хеш текущего блока. - Nonce. - Список транзакций в этом блоке. - Подпись. Каждая команда получает по 4 карточки блока для заполнения.
Карточка ключей (Приложение №6)	Выдаётся каждой команде.

Также используются:

- Таймер (на майнинг можно выделить от 10 до 5 минут). Рекомендуем начать с большего времени. В процессе игры его можно уменьшить, введя как новое условие для всех.

- Калькуляторы (или приложения на мобильных телефонах участников).

- Доска, где фиксируется общая цепочка **блоков**, собранных командой майнеров.

- Таблица подстановки A1Я3З (Приложение №7)

- Карточка «нулевого блока» (Приложение №8)

- Карточки с именами получателей/отправителей транзакций (Приложение №9)

Ведущий размещает на доске (флипчарте):

- Таблицу с балансами (количеством монет) отправителей и получателей **транзакций**, которые обрабатывают **команды майнеров** (см. ниже)

- Таблицу команд **майнеров**.

Этапы игры

1 этап. Создание публичного и секретного ключа каждой команды. Старт игры.

Каждая команда придумывает название на русском языке, кириллическими буквами (**это важно!**)

Шаг 1 из 4. На доске размещаются:

- таблица с отправителями и получателями транзакций, которые обрабатывают майнеры (Приложение №9).

Имя	Баланс монет

Имена отправителей и получателей можно разрезать и закрепить на доске, или написать на доске от руки.

В Приложении 9 указаны имена получателей и отправителей всех транзакций: возможно, часть из них не будут выложены на доске

Важно: у каждого отправителя/получателя **изначально по 10 монет**. В течение игры, после проведения перевода, их баланс меняется.

В начале игры таблица выглядит следующим образом:

Имя	Баланс монет
Боромир	10
Фродо	10
Леголас	10

- таблица команд **майнеров**.

Название команды	Публичный ключ	Количество монет	Добавлено блоков

Важно: каждая команда майнеров изначально стартует с 5 монетами.

Шаг 2 из 4: Формирование секретного ключа

Каждая команда придумывает **секретный ключ** — любое целое число от 1 до 20 — вписывают его в свою карточку (Приложение №6). Остальным командам он не известен! Карточка остаётся у команды.

Шаг 3 из 4: Формирование публичного ключа

Каждая команда создаёт **публичный ключ**. Для этого она умножает свой секретный ключ на любое целое число от 1 до 7. Результат умножения становится публичным ключом.

Публичный ключ размещается на доске, в таблице команд **майнеров**. Также на доске размещается название команды.

Шаг 4 из 4. Старт игры

На доске размещаются:

- 10-15 первых транзакций, количество транзакций зависит от количества команд.

- Нулевой блок (Приложение №8)

- Запускается таймер (10 минут)

2 этап. Создание блока (Майнинг)

Шаг 1 из 5: Выбор транзакций.

Команды выбирают **3 транзакции** из размещённых на доске и забирают их себе для обработки.

Пример транзакций:

1. Илья → Диане: 5
1. Ева → Фёдору: 8
2. Мансур → Глебу: 7

Эти транзакции будут команды будут собирать в один блок.

Шаг 2 из 5: Расчёт хеша блока.

Для справки:

Хеш (англ. hash — «превращать в фарш», «мешанина»), или функция свёртки — функция, преобразующая массив входных данных произвольного размера в строку установленного размера в соответствии с определённым алгоритмом.

Хеш блока состоит из суммы хешей всех транзакций блока, транзакции вознаграждения и хеша прошлого блока

В рамках игры мы будем использовать упрощённый алгоритм хеширования.

Мы возьмём все буквы имён во всех транзакциях одного блока и переведём их в цифры с помощью подстановки А1Я3З (замена буквы на её номер в алфавите, см. Приложение №7).

Пробелы и знак «→» и другие знаки не учитываются.

Сложим все получившиеся цифры и прибавим количество монет, которые пользователи переводят друг-другу.

При этом комиссии не учитываются! Сумма комиссий за проведение транзакций в рамках блока фиксируется отдельно в формате:

Вимме → [Название команды]: общая сумма монет вознаграждения

Также прибавим Хеш предыдущего блока.

Пример:

Предположим, что название команды— Майнеры. Хеш предыдущего блока равен 0. Тогда транзакции из примера выше:

1. Илья → Диане: 5
1. Ева → Фёдору: 8
2. Мансур → Глебу: 7

рассчитываются следующим образом:

Транзакции	Суммы
Вимме → Майнеры: 1+1+2 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
Итого:	521

Комментарий для ведущего игры:

Для упрощения вы можете взять для Хеширования только первые 3 буквы в имени.

Прибавляем к сумме хешей блока хеш прошлого блока. Как мы и говорили выше, для примера он равен 0. Тогда:

$$521+0 = 521$$

Шаг 3 из 5: Расчёт nonce.

Для справки:

Название Nonce происходит от англ. аббревиатуры Number That Can Only Be Used Once, то есть «Число, которое можно использовать только раз». Это число, отвечающее определенным требованиям, и используемое майнерами в процессе создания блоков в сетях, которые работают на алгоритме консенсуса PoW (Proof of Work).

В рамках игры необходимо найти число nonce, чтобы полученное на предыдущем шаге число+nonce делилось на 10 без остатка.

Пример:

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

$$\text{nonce} = 9$$

Шаг 4 из 5: Подпись блока через шифрование.

Команда шифрует хеш, умножая его на произведение секретного ключа и заранее придуманного числа от 1 до 7.

Например, команда «Майнеры» придумала секретный ключ 2, а заранее придуманное числа от 1 до 7 в их случае равно 5. В этом случае:

$$521 * 2 * 5 = 5210$$

Шаг 5 из 5: Заполнение карточки блока

Теперь у команды есть всё необходимое для оформления блока.

Команда заполняет карточку блока:

- Хеш предыдущего блока.
- Рассчитанный командой хеш текущего блока.
- Nonce (число для подбора хеша).
- Список транзакций.
- Свою подпись (через шифрование).

Важно: команда не вписывает номер блока на этом этапе!

Пример заполненной карточки блока:

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

После этого блок готов к проверке остальными командами.

3 этап. Проверка (валидация) блока

Этот этап происходит одновременно с обработкой следующих блоков. Таймер не останавливается

Все команды проверяют предложенный блок по следующим параметрам:

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

Голосование:

Если >50% команд одобряют блок, то достигнут **консенсус**, и блок добавляется в цепочку, ему присваивается номер.

В этом случае команда получает вознаграждение: указанную комиссию за транзакции + 5 монет

Если < 50% команд одобряют блок, то он отклоняется. Все транзакции неподтверждённого блока возвращаются на доску и доступны для выбора, а команда теряет 5 монет.

Обновление цепочки:

Ведущий закрепляет новый блок на доске, после предыдущего. Его хеш проверяется в следующем блоке и используется для его расчёта.

Ведущий также обновляет таблицу команд майнеров: добавляет заработанные монеты команде, обновляет количество блоков.

Также команда участников, которые получили вознаграждение, обновляют таблицу с отправителями и получателями транзакций: вносят новое имя (при необходимости), стирают старый и вносят новый баланс.

Далее этапы 2 и 3 повторяются

Спустя 10 минут игры происходит уменьшение вознаграждения командам (вместо 5 монет они получают 4 или 3).

Таймер перезапускается.

Для справки:

Халвингом в сети Биткойна называют процедуру снижения вознаграждения за добычу блока в данной сети в два раза. Она происходит каждые 210 тысяч блоков в сети Биткойна или приблизительно четыре года.

4 этап. Атака 51%

На этом этапе одна из команд (или внешняя группа) пытается атаковать сеть.

Ведущему не обязательно объявлять об этом публично о начале этого этапа, но он может это сделать. Также он может «вступить в сговор» с одной из команд: это нужно сделать до начала игры.

Возможная механика атаки:

- Ведущий создаёт поддельный блок с фальшивой транзакцией, например, «3. Ева → Илье: 50 монет». Также возможно создать транзакцию типа «10. Ева → Илье: 15». При этом у пользователя Ева нет такого количества монет.

Злоумышленники должны убедить >50% команд принять этот блок. Участники проверяют его (см. этап 3)

Если атака успешна, злоумышленники крадут монеты и нарушают цепочку. Если нет, то злоумышленники терпят поражение.

Завершение игры.

Игра завершается после успешной обработки всех транзакций.

Её можно завершить и раньше, если каждая команда создала хотя-бы один свой блок.