Что такое блокчейн?

Евгений Ломов

Междисциплинарная неделя «Кроссворда Тьюринга» и школы «Лес»

Обо мне

- Закончил Физфак МГУ по специальности «Квантовые вычисления»
- Поработал в криптостартапе
- Разрабатываю компиляторы для DSP
- Организую школу «Лес»

Канал физического отделения «Лес»

Часть 1: Немного истории и постановка задачи

Обмен в доцифровую эпоху

Обмен в доцифровую эпоху

Компьютерные системы и Интернет

Компьютерные системы и Интернет

???

Наличные и банковская система

Наличные **Банк**

Наличные и банковская система

Наличные

- Нет посредника

Банк

- Банк является доверенной третьей стороной

Наличные и банковская система

Наличные

- Нет посредника
- Необратимость без согласия сторон

Банк

- Банк является доверенной третьей стороной
- Банковкая операция может быть отменена

Наличные и банковская система

Наличные

- Нет посредника
- Необратимость без согласия сторон
- Нет накладных расходов

Банк

- Банк является доверенной третьей стороной
- Банковкая операция может быть отменена
- Банковский перевод - платная услуга

Электронные деньги

Электронные деньги

- Нет посредника, которому необходимо доверять

Электронные деньги

- Нет посредника, которому необходимо доверять
- Необратимые операции

Электронные деньги

- Нет посредника, которому необходимо доверять
- Необратимые операции
- Низкая стоимость транзакций

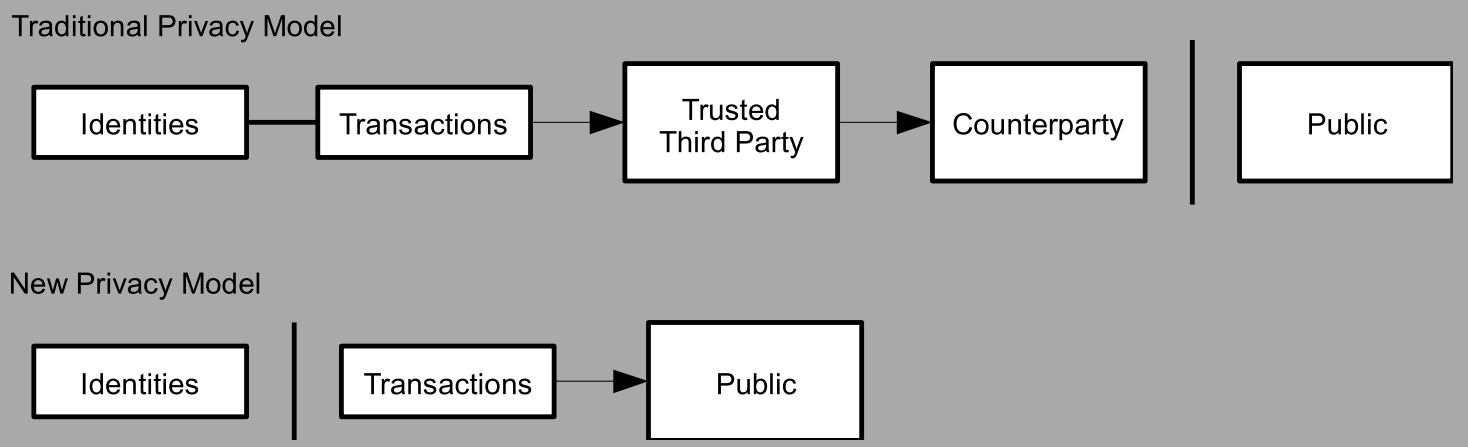
Электронные деньги

- Нет посредника, которому необходимо доверять
- Необратимые операции
- Низкая стоимость транзакций
- Обязательная авторизация

Электронные деньги

- Нет посредника, которому необходимо доверять
- Необратимые операции
- Низкая стоимость транзакций
- Обязательная авторизация
- Приватность

Новая модель приватности



Проблемы, которые надо решить

КОРЕШОК ЧЕКА

АЭ № 066576

16 01 19 93

Остаток лимита 189 р. 19 к.

Списано по настоящему чеку 5 р. 00 к.

Остаток лимита к следующему чеку 184 р. 19 к.

ЧЕК ДЕЙСТВИТЕЛЕН В ТЕЧЕНИЕ 10 ДНЕЙ, НЕ СЧИТАЯ ДНЯ ВЫДАЧИ

БАНК СССР

г. Свердловск П-111

РАСЧЕТНЫЙ ЧЕК АЭ № 066579

из лимитированной книжки

на 45 руб. 00 коп.

Перечислите магазин №63

за товар

Сорок пять долларов 80 центов

Место выдачи магазин №63 6 февраля 1993

ВЫДАЧА СДАЧИ С ЭТОГО ЧЕКА НАЛИЧНЫМИ ВОСПРЕЩАЕТСЯ

Проблемы, которые надо решить

- Подтверждение личности отправителя

Проблемы, которые надо решить

- Подтверждение личности отправителя
- Проверка наличия средств у отправителя

Проблемы, которые надо решить

- Подтверждение личности отправителя
- Проверка наличия средств у отправителя
- Невозможность тратить одни и те же деньги несколько раз

Часть 2: Криптографический ликбез

Односторонние функции

$$y = f(x) \leftarrow \text{Вычисляется } \textit{легко}$$

$$x = f^{-1}(y) \leftarrow \text{Не существует или вычисляется } \textit{сложно}$$

Односторонние функции: примеры

- **Умножение:** $c = ab$ – легко, но $(a, b) = f(c)$ – трудно

Односторонние функции: примеры

- **Умножение:** $c = ab$ – легко, но $(a, b) = f(c)$ – трудно
- **Возведение в степень:** $c = a^b$ – легко, но $b = \log_a(c)$ – трудно

Хеш-функции

Хеш-функция – функция, преобразующая массив входных данных произвольного размера в выходную битовую строку фиксированного размера.

— Википедия

Хеш-функции

Хеш-функция – функция, преобразующая массив входных данных произвольного размера в выходную битовую строку фиксированного размера.

— Википедия

$$h(x) = x \bmod N, \text{где } N - \text{простое число}$$

Хеш-функции: свойства

- **Коллизия** – пара входных значений m и m', такие что $h(m) = h(m')$

Хеш-функции: свойства

- **Коллизия** – пара входных значений m и m', такие что $h(m) = h(m')$
- **Лавинный эффект** – малое изменение входных данных полностью изменяет значение хеш-функции

Требования к криптографическим хеш-функциям

- **Сопротивление поиску прообраза:** для значения хэша x должно быть трудно найти m такое, что $x = h(m)$

Требования к криптографическим хеш-функциям

- **Сопротивление поиску прообраза:** для значения хэша x должно быть трудно найти m такое, что $x = h(m)$
- **Сопротивление поиску второго прообраза:** для m_1 должно быть сложно найти m_2 такое, что: $h(m_1) = h(m_2)$

Требования к криптографическим хеш-функциям

- **Сопротивление поиску прообраза:** для значения хэша x должно быть трудно найти m такое, что $x = h(m)$
- **Сопротивление поиску второго прообраза:** для m_1 должно быть сложно найти m_2 такое, что: $h(m_1) = h(m_2)$
- **Стойкость к поиску коллизий:** должно быть сложно найти m, m' такие, что $h(m) = h(m')$

Цифровая подпись

Цифровая подпись – метод подтверждения подлинности цифрового сообщения. Подтвержденная цифровая подпись доказывает, что сообщение пришло от отправителя, а не кого-то другого.

— Wikipedia(en)

Односторонняя функция с *секретом*

- $f_S(m) = c$ *легко* вычислить без знания *секрета*
- $f_S^{-1}(c) = m$ – *сложно*
- $f_S^{-1}(c) = m$ – *легко*

Цифровая подпись: общая схема

- **Генерация ключей:** С помощью генератора случаных чисел создаются открытый (P) и закрытый (S) ключи

Цифровая подпись: общая схема

- **Генерация ключей:** С помощью генератора случаных чисел создаются открытый (P) и закрытый (S) ключи
- **Публикация открытого ключа**

Цифровая подпись: общая схема

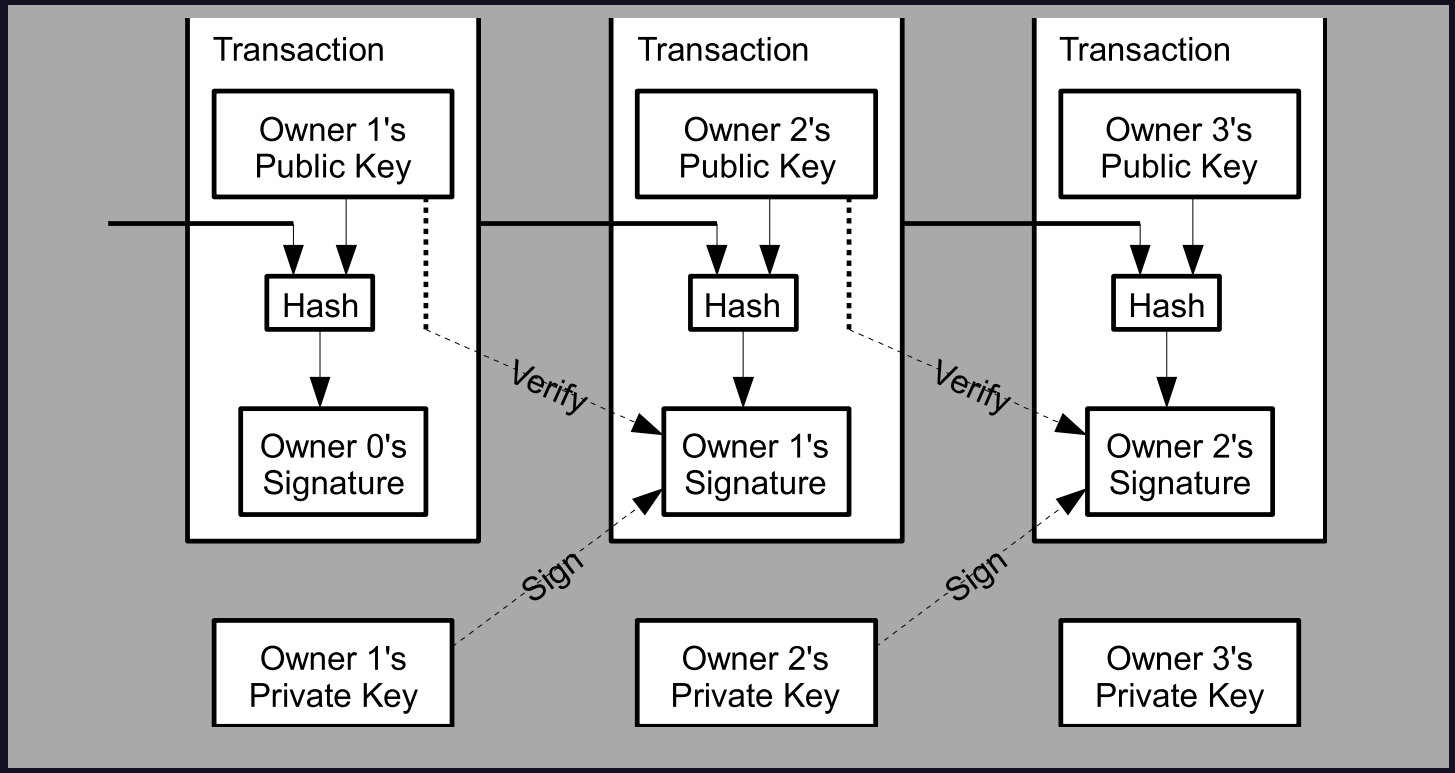
- **Генерация ключей:** С помощью генератора случаных чисел создаются открытый (P) и закрытый (S) ключи
- **Публикация открытого ключа**
- **Подписывание сообщений с использованием закрытого ключа**

Часть 3: Блокчейн (наконец-то)

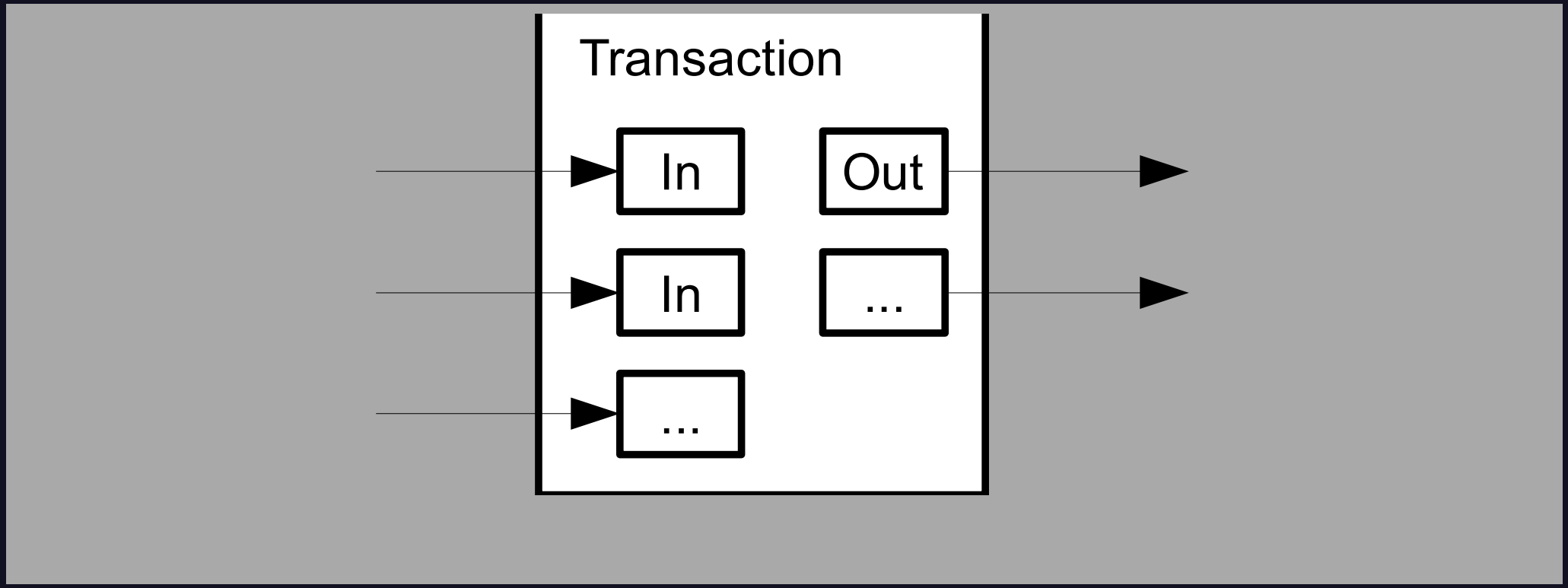
Проблемы, которые надо решить

- Подтверждение личности отправителя
- Проверка наличия средств у отправителя
- Невозможность тратить одни и те же деньги несколько раз

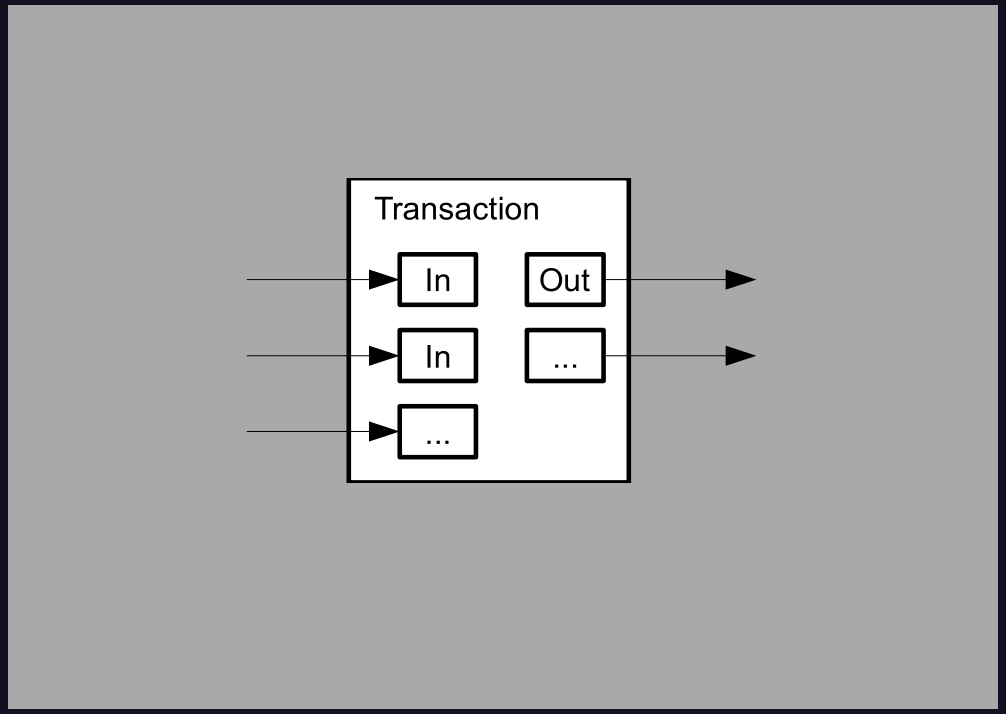
Цепочка транзакций



Устройство транзакции

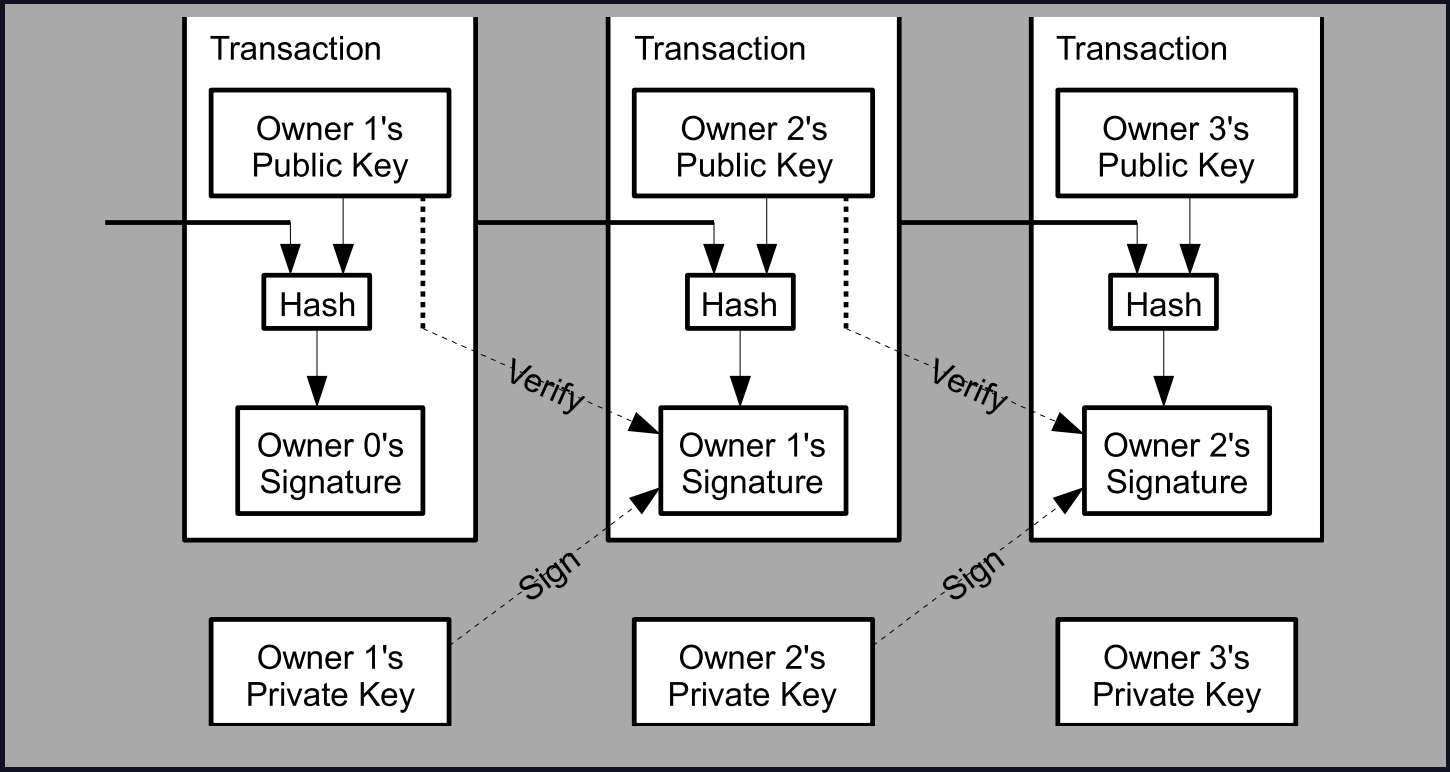


Устройство транзакции

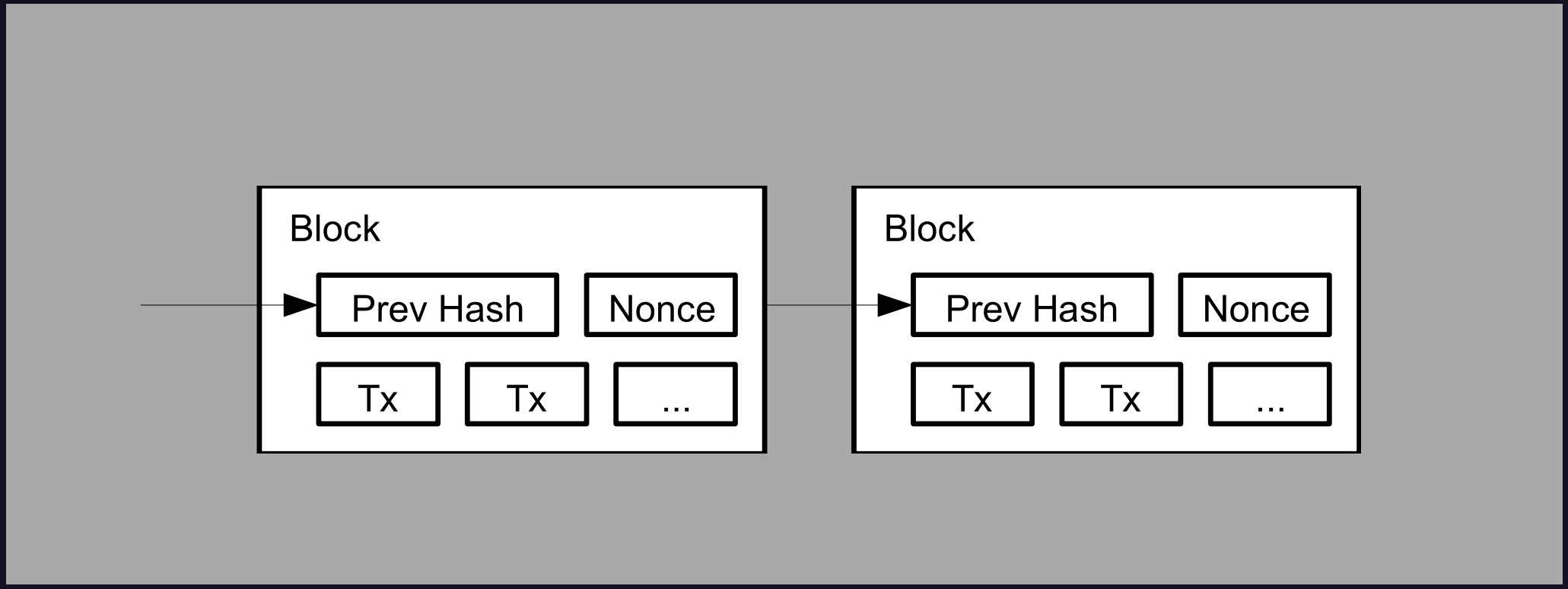


- $\sum \mathrm{In} = \sum \mathrm{Out}$
- Биткоины из входных транзакций полностью переводятся в выходные
- Для «сдачи» адрес отправителя включается в *выходы* транзакции

Цепочка транзакций



Цепочка блоков



Proof of work

Идея: сделаем так, чтобы создавать блоки было вычислительно трудно.

Proof of work

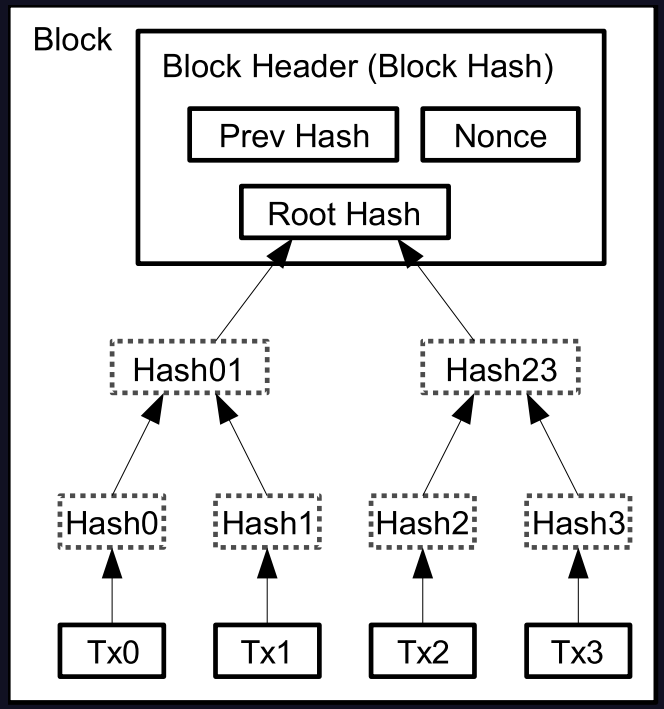
Идея: сделаем так, чтобы создавать блоки было вычислительно трудно.

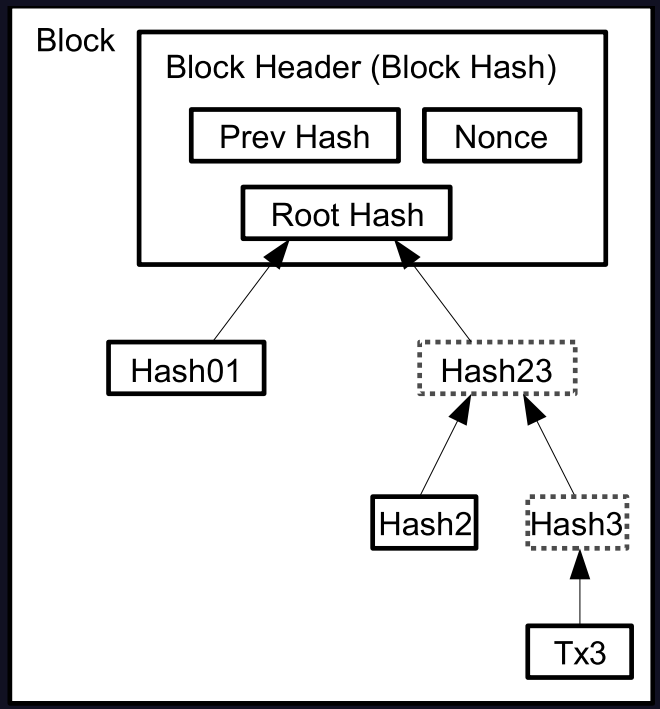
- Добавим в блок поле **Nounce**(*англ.* соль), значение которого может быть любым
- Потребуем, чтобы значение хеша блока удовлетворяло некоторому условию

Устройство блока

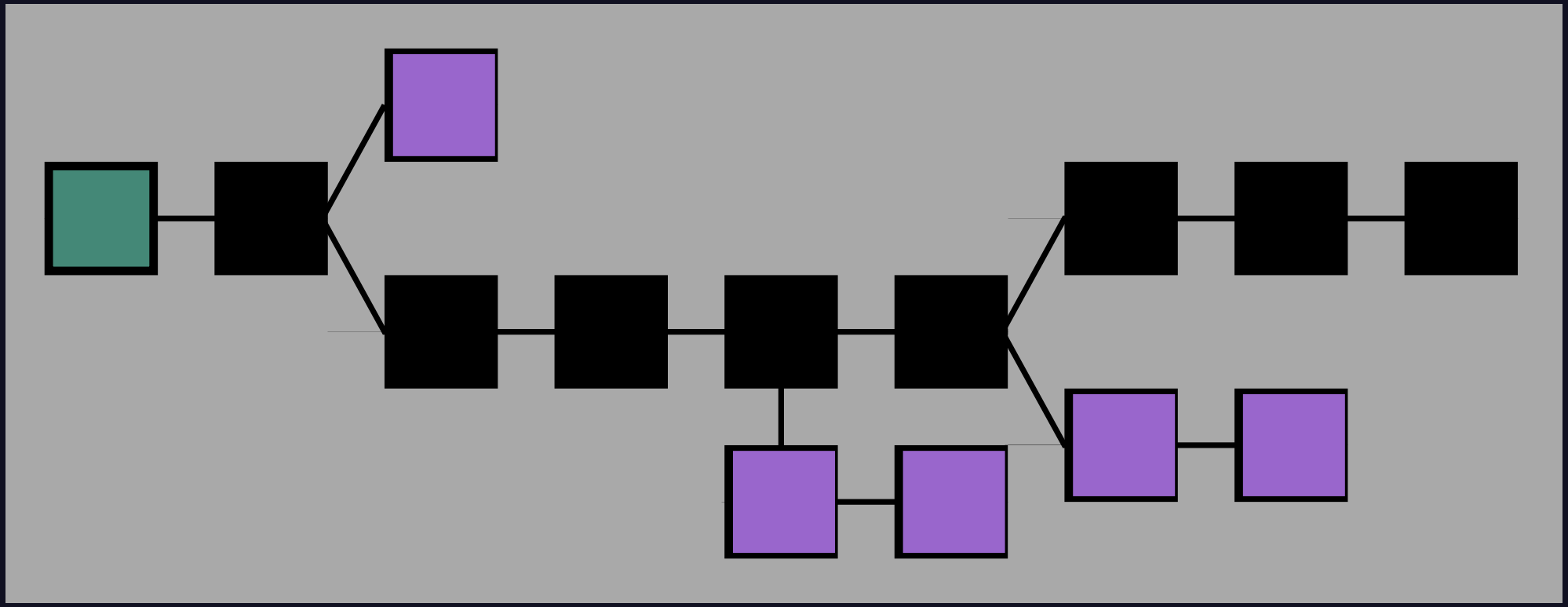
Поле	Значение
Timestamp (не показано)	Время генерации этого блока
Prev Hash	Хеш предыдущего блока
Nonce	Значение, которое нужно подобрать
Difficulty (не показано)	количество нулей, которое должно быть у хеша этого блока
Tx1, Tx2…	Транзакции, которые включены в этот блок

Хранение списка транзакций





А если цепочка раздвоится?



Ссылки

На меня

На канал «Леса»

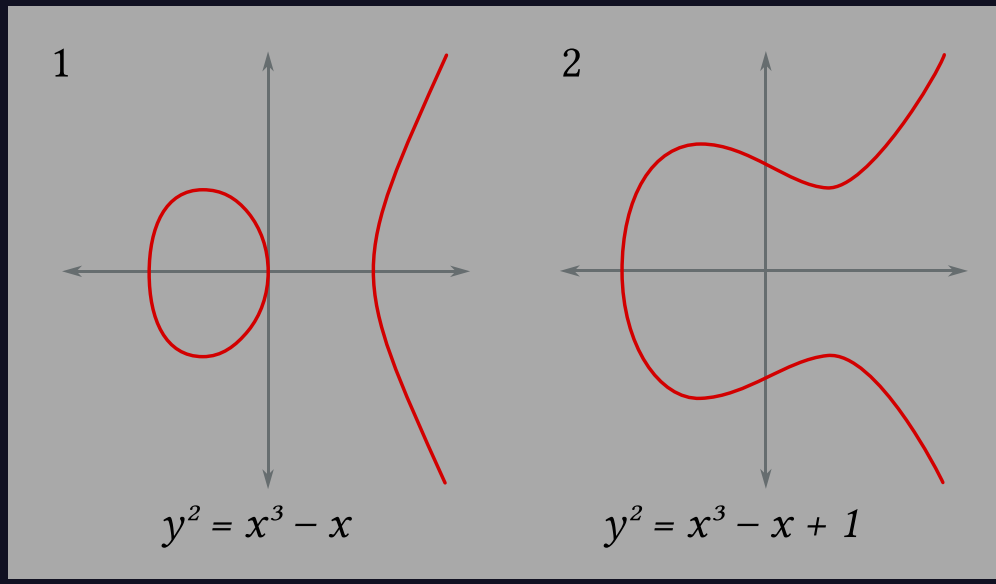
На «ФизЛес»

(QR кликабельны в PDF)

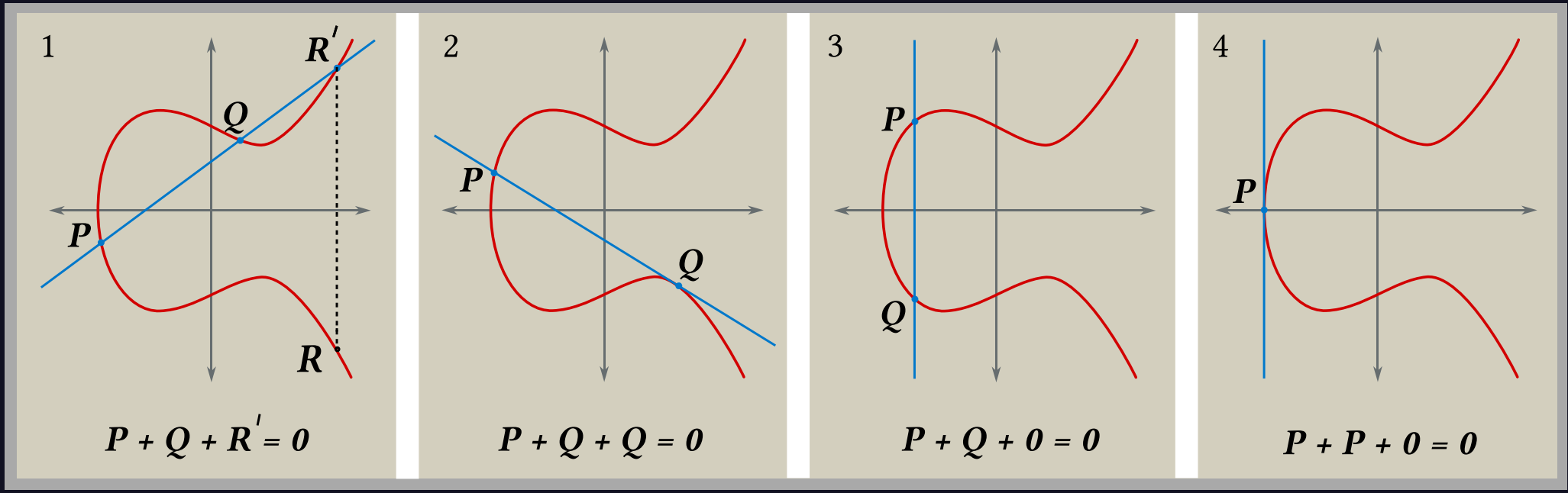
Bonus: Как всё-таки работает цифровая подпись?

Эллиптические кривые

- $y^2 = x^3 + ax + b$
- $\Delta = -16(4a^3 + 27b^2) \neq 0$



Эллиптические кривые: закон сложения точек



Эллиптические кривые: закон сложения точек

Пусть $P = (x_P, y_P)$ и $Q = (x_Q, y_Q)$ – точки на кривой.

Допустим, что $x_P \neq x_Q$ и пусть $s = \frac{y_P - y_Q}{x_P - x_Q}$

Тогда $R = P + Q = (x_R, y_R)$:

$$x_R = s^2 - x_P - x_Q$$

$$y_R = -y_P + s(x_P - x_R)$$

Эллиптические кривые: закон сложения точек

Если $x_P = x_Q$:

- $y_P = -y_Q \Rightarrow P + Q = O$ – по определению.
- $y_P = y_Q \neq 0$, тогда $P + Q = 2P = (x_R, y_R)$:

$$s = \frac{3x_P^2 + a}{2y_P}$$

$$x_R = s^2 - 2x_P$$

$$y_R = -y_P + s(x_P - x_R)$$

Если $y_P = y_Q = 0$ то $P + P = O$

Алгоритм ECDSA

Параметры алгоритма:

- Эллиптическая кривая $y^2 = x^3 + 486662x^2 + x$ над $GF(2^{255} - 19)$
- Точка G с координатой $x = 9$
- Порядок группы, образуемой точкой: $n = 2^{252} + 27742317777372353535851937790883648493$

(Curve25519)

Алгоритм ECDSA: создание секретного ключа

1. Выбрать случайное число d в интервале $[0, n-1]$
2. Вычислить $Q = d \times G$

Закрытый ключ: (d, Q)

Открытый ключ: Q

Алгоритм ECDSA: подпись сообщения

1. Хешировать сообщение $e = h(m)$

Алгоритм ECDSA: подпись сообщения

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.

Алгоритм ECDSA: подпись сообщения

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Выбрать криптографически случайное число $k \in [0, n-1]$

Алгоритм ECDSA: подпись сообщения

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Выбрать криптографически случайное число $k \in [0, n-1]$
4. Вычислить $(x_1, y_1) = k \times G$

Алгоритм ECDSA: подпись сообщения

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Выбрать криптографически случайное число $k \in [0, n-1]$
4. Вычислить $(x_1, y_1) = k \times G$
5. Вычислить $r = x_1 \bmod n$, если $r = 0$, вернуться к шагу 3.

Алгоритм ECDSA: подпись сообщения

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Выбрать криптографически случайное число $k \in [0, n-1]$
4. Вычислить $(x_1, y_1) = k \times G$
5. Вычислить $r = x_1 \bmod n$, если $r = 0$, вернуться к шагу 3.
6. Вычислить $s = k^{-1}(z + rd) \bmod n$, если $s = 0$, вернуться к шагу 3.

Алгоритм ECDSA: подпись сообщения

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Выбрать криптографически случайное число $k \in [0, n-1]$
4. Вычислить $(x_1, y_1) = k \times G$
5. Вычислить $r = x_1 \bmod n$, если $r = 0$, вернуться к шагу 3.
6. Вычислить $s = k^{-1}(z + rd) \bmod n$, если $s = 0$, вернуться к шагу 3.

Подписью сообщения будет пара (r, s)

Алгоритм ECDSA: проверка подписи

1. Хешировать сообщение $e = h(m)$

Алгоритм ECDSA: проверка подписи

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.

Алгоритм ECDSA: проверка подписи

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Вычислить $u_1 = zs^{-1} \bmod n$ и $u_2 = rs^{-1} \bmod n$

Алгоритм ECDSA: проверка подписи

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Вычислить $u_1 = zs^{-1} \bmod n$ и $u_2 = rs^{-1} \bmod n$
4. Вычислить $C = (x_2, y_2) = u_1 \times G + u_2 \times Q$, если $(x_2, y_2) = O$, то подпись недействительна.

Алгоритм ECDSA: проверка подписи

1. Хешировать сообщение $e = h(m)$
2. Взять $z = e_{L..0}$, где L - битовая длина n.
3. Вычислить $u_1 = zs^{-1} \bmod n$ и $u_2 = rs^{-1} \bmod n$
4. Вычислить $C = (x_2, y_2) = u_1 \times G + u_2 \times Q$, если $(x_2, y_2) = O$, то подпись недействительна.

Подпись верна, если $r = x_2 \bmod n$

Почему это работает?

Алгоритм ECDSA: доказательство корректности

1. $\mathrm{C} = u_1 \times G + u_2 \times Q$

Алгоритм ECDSA: доказательство корректности

1. $\mathrm{C} = u_1 \times G + u_2 \times Q$
2. $\mathrm{C} = u_1 \times G + u_2 d \times G$

Алгоритм ECDSA: доказательство корректности

1. $\mathrm{C} = u_1 \times G + u_2 \times Q$
2. $\mathrm{C} = u_1 \times G + u_2 d \times G$
3. $\mathrm{C} = (u_1 + u_2 d) \times G$

Алгоритм ECDSA: доказательство корректности

1. $\mathrm{C} = u_1 \times G + u_2 \times Q$
2. $\mathrm{C} = u_1 \times G + u_2 d \times G$
3. $\mathrm{C} = (u_1 + u_2 d) \times G$
4. $\mathrm{C} = (z s^{-1} + r s^{-1} d) \times G$

Алгоритм ECDSA: доказательство корректности

1. $\mathrm{C} = u_1 \times G + u_2 \times Q$
2. $\mathrm{C} = u_1 \times G + u_2 d \times G$
3. $\mathrm{C} = (u_1 + u_2 d) \times G$
4. $\mathrm{C} = (z s^{-1} + r s^{-1} d) \times G$
5. $\mathrm{C} = (z + rd) s^{-1} \times G$

Алгоритм ECDSA: доказательство корректности

1. $\mathrm{C} = u_1 \times G + u_2 \times Q$
2. $\mathrm{C} = u_1 \times G + u_2 d \times G$
3. $\mathrm{C} = (u_1 + u_2 d) \times G$
4. $\mathrm{C} = (z s^{-1} + r s^{-1} d) \times G$
5. $\mathrm{C} = (z + rd) s^{-1} \times G$
6. $\mathrm{C} = (z + rd) \frac{k}{z + rd} \times G$

Алгоритм ECDSA: доказательство корректности

1. $\mathrm{C} = u_1 \times G + u_2 \times Q$
2. $\mathrm{C} = u_1 \times G + u_2 d \times G$
3. $\mathrm{C} = (u_1 + u_2 d) \times G$
4. $\mathrm{C} = (z s^{-1} + r s^{-1} d) \times G$
5. $\mathrm{C} = (z + rd) s^{-1} \times G$
6. $\mathrm{C} = (z + rd) \frac{k}{z+rd} \times G$
7. $\mathrm{C} = k \times G = (x_2, y_2)$

При этом $r = x_1$, $(x_1, y_1) = k \times G$, а проверка подписи заключалась в $r = x_2 \bmod n$

Почему k должно быть случайным?

Допустим, одно и то же k использовалось для двух подписей (r, s) и (r, s') известных сообщений m и m'.

Почему k должно быть случайным?

Допустим, одно и то же k использовалось для двух подписей (r, s) и (r, s') известных сообщений m и m'.

1. z и z' известны $\Rightarrow k = \frac{z - z'}{s - s'}$

Почему k должно быть случайным?

Допустим, одно и то же k использовалось для двух подписей (r, s) и (r, s') известных сообщений m и m'.

1. z и z' известны $\Rightarrow k = \frac{z - z'}{s - s'}$
2. $s = k^{-1}(z + rd) \Rightarrow d = \frac{sk - z}{r}$

Ссылки

На меня

На канал «Леса»

На «ФизЛес»

(QR кликабельны в PDF)