Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Технология блокчейн. Криптовалюты.

Простой список

Хранение информации у третьей стороны:

1. Петя продал квартиру Васе
2. Оля купила машину у Игоря
3. Наташа подарила дачу Марине
4. ....

Простой список

Хранение информации у третьей стороны:

1. Петя продал квартиру Васе
2. Оля купила велосипед у Игоря
3. Наташа подарила дачу Марине
4. ....

Связанный список

Хранение информации у третьей стороны:

1. Петя продал квартиру Васе
2. Оля купила машину у Игоря || MD5(п.1)
3. Наташа подарила дачу Марине || MD5(п.2)
4. ....

Связанный список

Хранение информации у третьей стороны:

1. Петя продал картину Васе
2. Оля купила машину у Игоря || MD5(п.1)
3. Наташа подарила дачу Марине || MD5(п.2)
4. ....

Список с предвычислениями

Хранение информации у третьей стороны (связанный список + суперкомпьютер):

1. Петя продал квартиру Васе
2. Оля купила машину у Игоря || MD5(п.1 || число), такой что результат начинается с 8-и нулевых байт (сложность 2^{64})
3. Наташа подарила дачу Марине || MD5(п.2 || число), такой что результат начинается с 8-и нулевых байт (сложность 2^{64})
4. ....

Подбор MD5

Петя продал квартиру Bace0

MD5 =4c e2 c3 5b dd 5d bd 98 19 94 d2 88 9a bb 2e 6d

Петя продал квартиру Bace100

MD5 = 31 8b bd 09 cf f1 87 f3 15 56 4e d5 1f 47 73 9a

Петя продал квартиру Bace39676

MD5 = 00 00 05 94 f9 f8 6b b1 d6 84 12 1b 5f d2 a6 7a

Петя продал квартиру Bace4542933

MD5 = 00 00 00 0a 5c aa 5a bb af 08 1a 91 84 24 19 b5

Список с предвычислениями

Хранение информации у третьей стороны (связанный список + суперкомпьютер):

1. Петя продал картину Васе
2. Оля купила машину у Игоря || MD5(п.1 || число), такой что результат начинается с 8-и нулевых байт (сложность 2^{64})
3. Наташа подарила дачу Марине || MD5(п.2 || число), такой что результат начинается с 8-и нулевых байт (сложность 2^{64})
4. ....

Биткойн

Биткойн – децентрализованная пиринговая платежная система.

Биткойн – единица учета операций (монета) с обозначением BTC (минимально возможная сумма:
1 сатоси = 10^{-8} BTC).

История биткойн

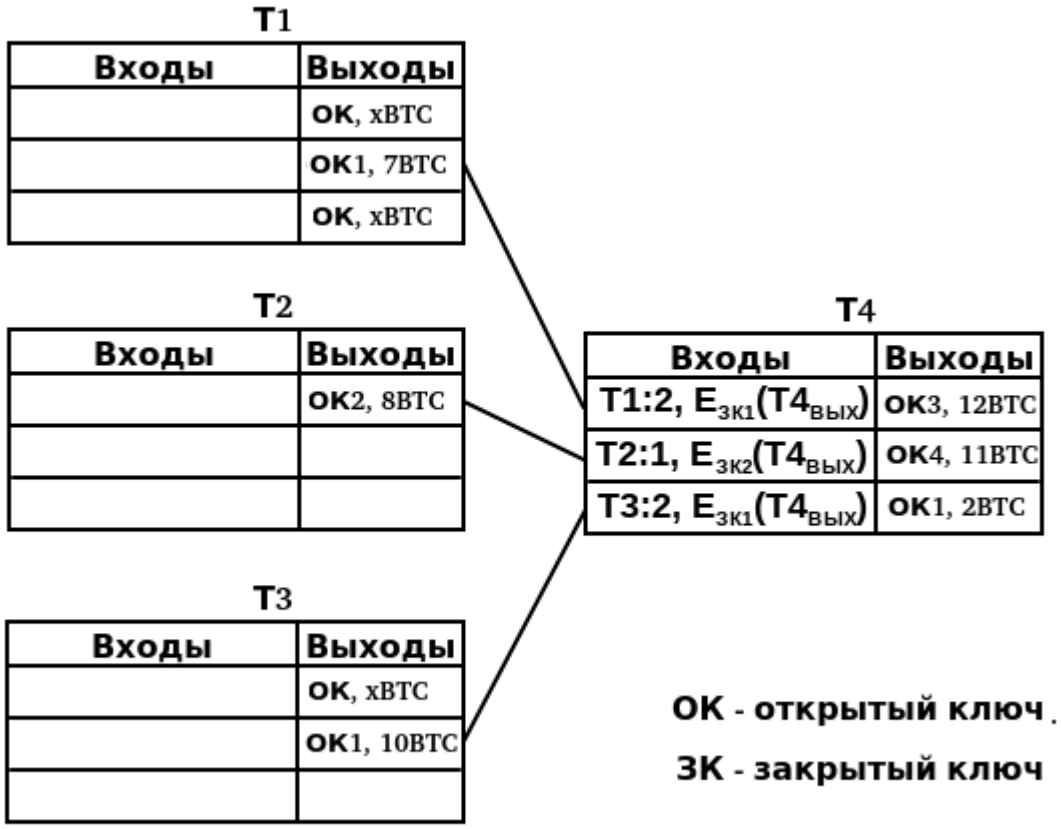
История:

- 2008 г. - человеком или группой людей под псевдонимом Сатоси Накамото был опубликован файл с описанием протокола и принципа работы платёжной системы в виде одноранговой сети.
- 3 января 2009 г. - сгенерирован первый блок и получены первые 50 BTC.
- 12 января 2009 г. - осуществлена первая транзакция в 10 BTC.
- сентябрь 2009 г. - первый обмен биткойнов на деньги (за 5050 BTC один пользователь получил от другого 5.02 доллара на PayPal).
- май 2010 г. - за 10000 BTC пользователь заказал 2 пиццы с доставкой.

Данные биткойн

- Блокчейн – файл с транзакциями-платежами за всю историю биткойн.
- Все узлы сети проводят и проверяют операции по одним и тем же алгоритмам. Исходный код системы находится на https://github.com/bitcoin/bitcoin/releases.
- Узел: **полный** - хранит весь блокчейн (около 300 Гб); **облегченный** - хранит только заголовки блоков (около 50 Мб).

Транзакция



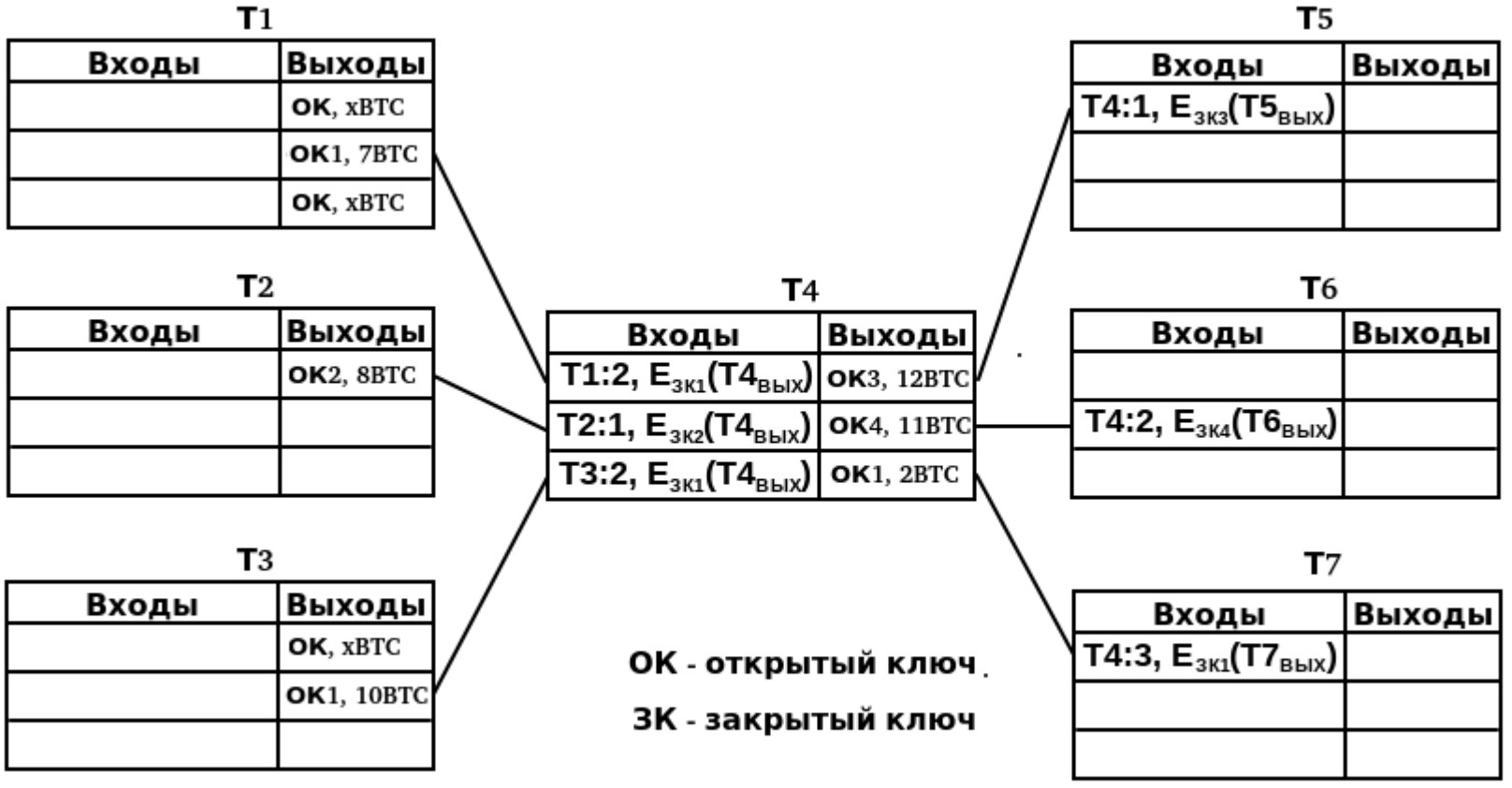
В системе у пользователей нет кошельков с биткойнами. Воспользоваться можно только выходными биткойнами из предыдущих транзакций, подтвердив свое право владения.

Открытый ключ – 512 бит.

Закрытый ключ – 256 бит.

Алгоритм подписи – ECDSA.

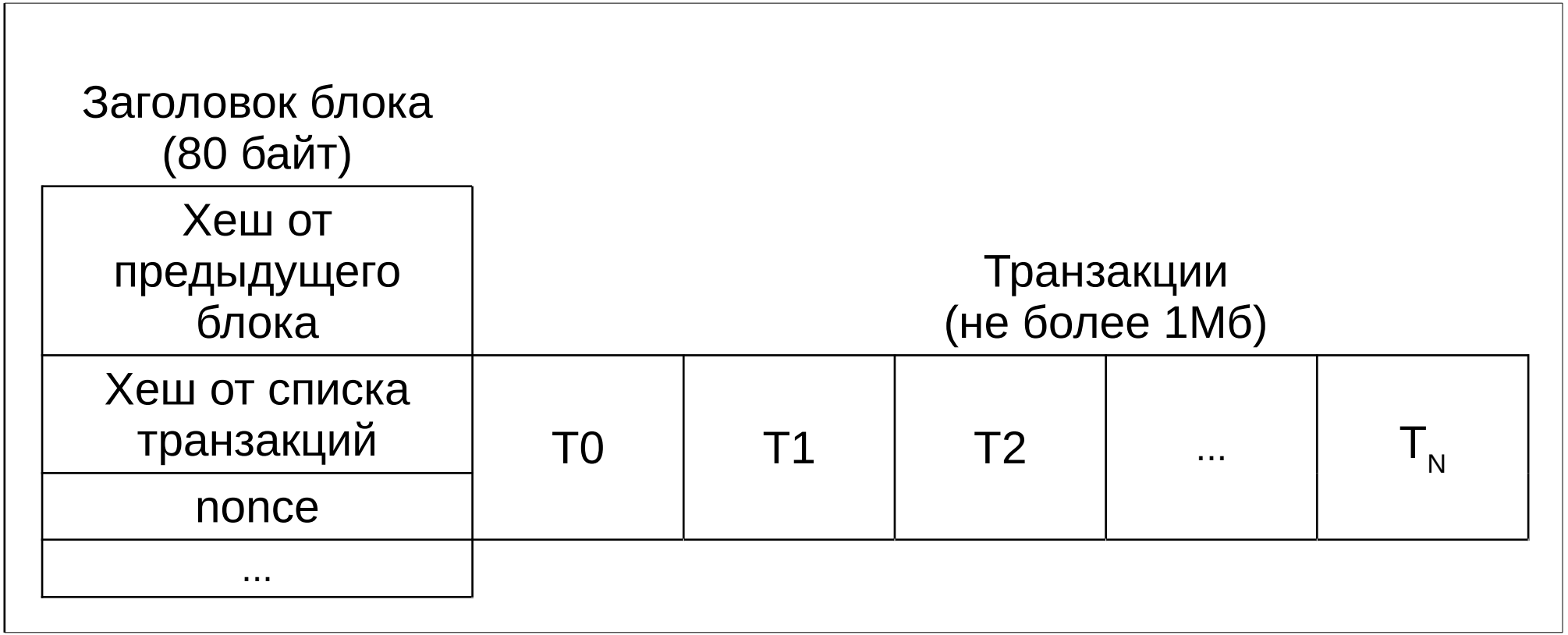
Транзакция


T1
Входы
Выходы
ОК, xBTC
ОК1, 7BTC
ОК, xBTC
T2
Входы
Выходы
ОК2, 8BTC
T3
Входы
Выходы
ОК, xBTC
ОК1, 10BTC
T4
Входы
Выходы
T1:2, $E_{ЗК1}(T4_{ВЫХ})$
ОК3, 12BTC
T2:1, $E_{ЗК2}(T4_{ВЫХ})$
ОК4, 11BTC
T3:2, $E_{ЗК1}(T4_{ВЫХ})$
ОК1, 2BTC
T5
Входы
Выходы
T4:1, $E_{ЗК3}(T5_{ВЫХ})$
T6
Входы
Выходы
T4:2, $E_{ЗК4}(T6_{ВЫХ})$
T7
Входы
Выходы
T4:3, $E_{ЗК1}(T7_{ВЫХ})$
ОК - открытый ключ
ЗК - закрытый ключ

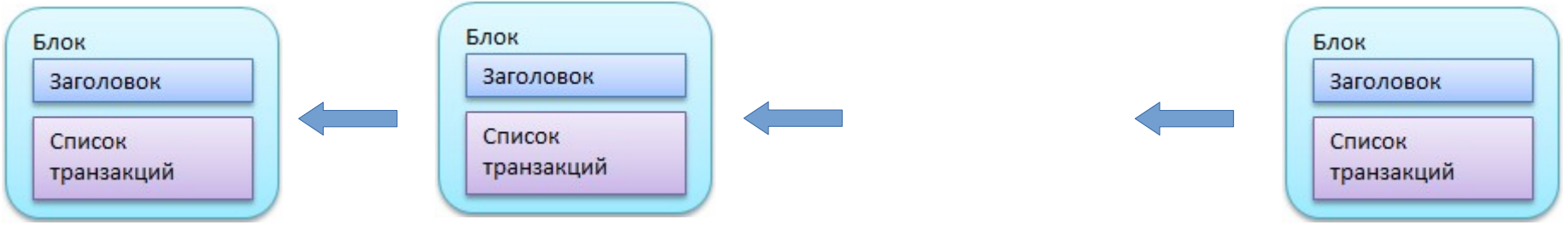
Транзакция

- Для осуществления транзакции необходим открытый и закрытый ключ.
- **Биткойн-адрес** – символьное представление хеша открытого ключа, удобное для передачи между абонентами (например, 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2).
- Каждый абонент может иметь неограниченное число биткойн-адресов.
- Транзакции являются **необратимыми**: если биткойны отправлены на неверный адрес, или злоумышленник узнал закрытый пароль и провел транзакцию от имени абонента, то опротестование транзакции невозможно.

Блок


Заголовок блока
(80 байт)
Хеш от предыдущего блока
Хеш от списка транзакций
nonce
...
Транзакции
(не более 1Мб)
T0
T1
T2
...
T_N

Блокчейн



Блок 0 Блок 1 Блок N

Самый первый блок в блокчейн называется блоком генезиса или генезис-блоком.

Добавление блока

- **Майнинг** (mining - добыча) – процесс решения математической задачи при поиске добавляемого блока.
- Блок может добавить любой абонент сети, если SHA256(SHA256(заголовок блока)) < $2^{256}/k$, где k – текущая сложность майнинга (сейчас примерно $13*10^{12} \approx 13*2^{40}$).
- За добавление блока абонент получает награду (первая транзакция в блоке не имеет входов, а только один выход – адрес абонента).
- Сложность майнинга автоматически изменяется так, чтобы новый блок добавлялся примерно раз в 10 минут.

Биткойн монеты

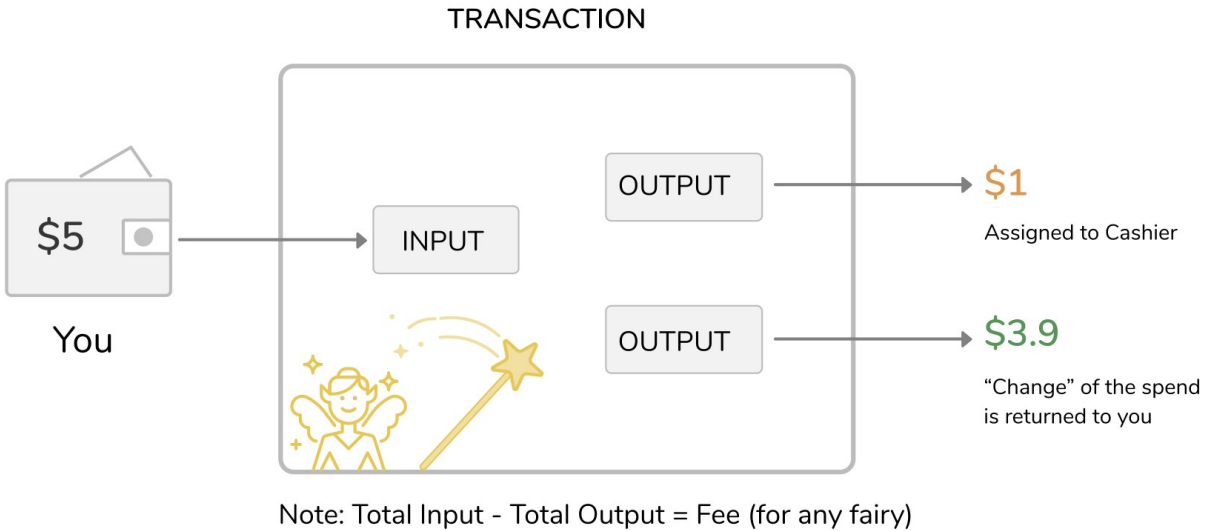
- Награда первым майнерам была 50BTC за блок.
- Через каждые 210000 блоков награда за новый блок уменьшается в 2 раза.
- 9.01.2009 – 50BTC; 29.11.2012 – 25BTC;
  9.07.2016 – 12.5BTC; 21.05.2020 – 6.25BTC.
- Максимальное количество биткойн (в 2140 году) составит 21 миллион BTC (сейчас 18 миллионов BTC).
- По оценкам утеряно от 3 до 4 миллионов BTC.

Коллизии

- Из нескольких вариантов блокчейн абонент выбирает наиболее сложную версию (более длинную).
- Если два майнера добыли блок одновременно, то одна часть сети работает с одним блоком, другая – с другим.
- “Побеждает” та часть, которая первой добавит к своему блоку следующий. Более короткая ветка отбрасывается участниками и пропадает.
- Самые нижние блоки считаются ненадежными. Надежными считаются блоки, за которыми следует 5-6 блоков.

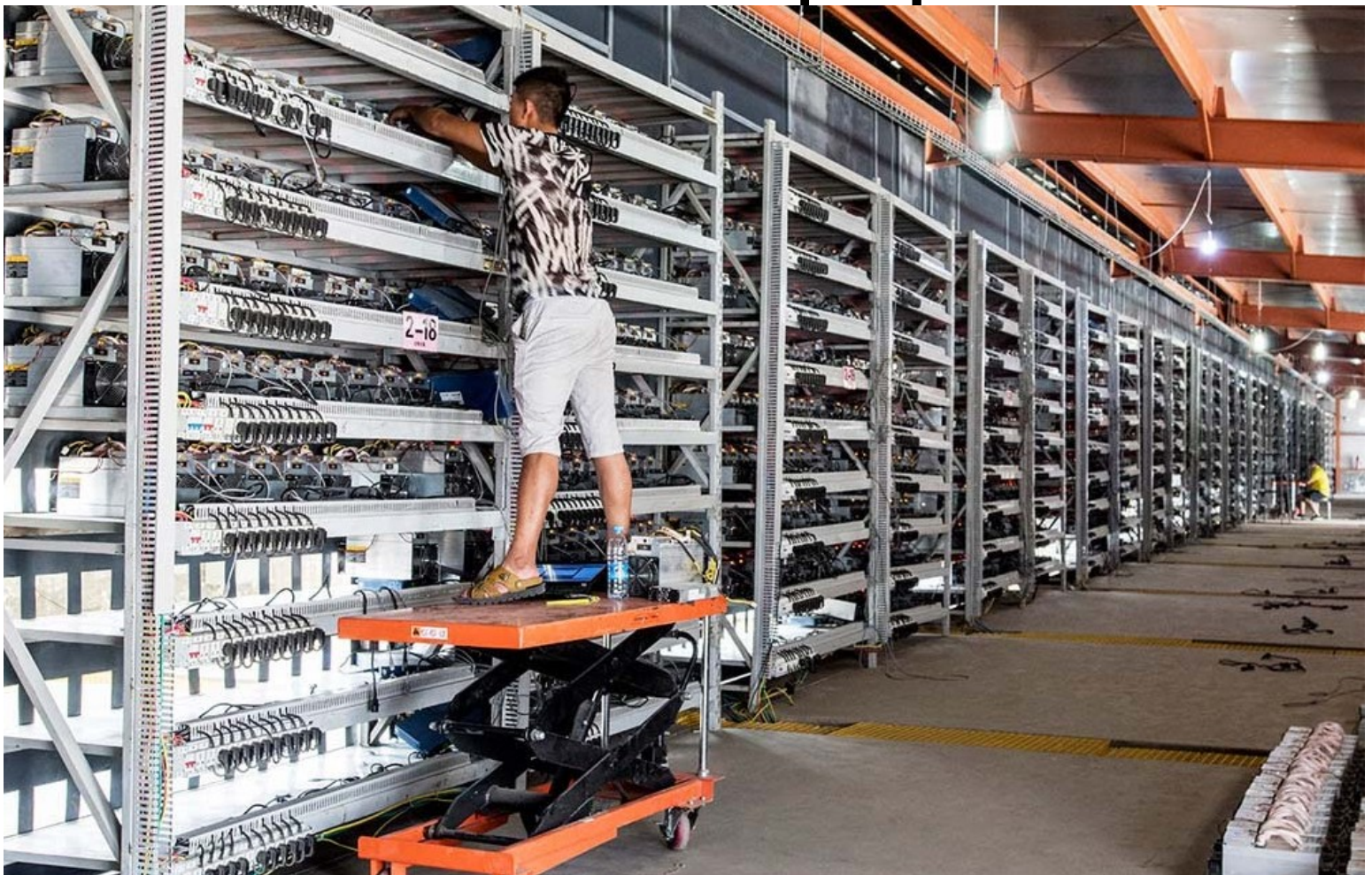
Прибыль майнера

- Награда за нахождение блока.
- Комиссии за транзакции.

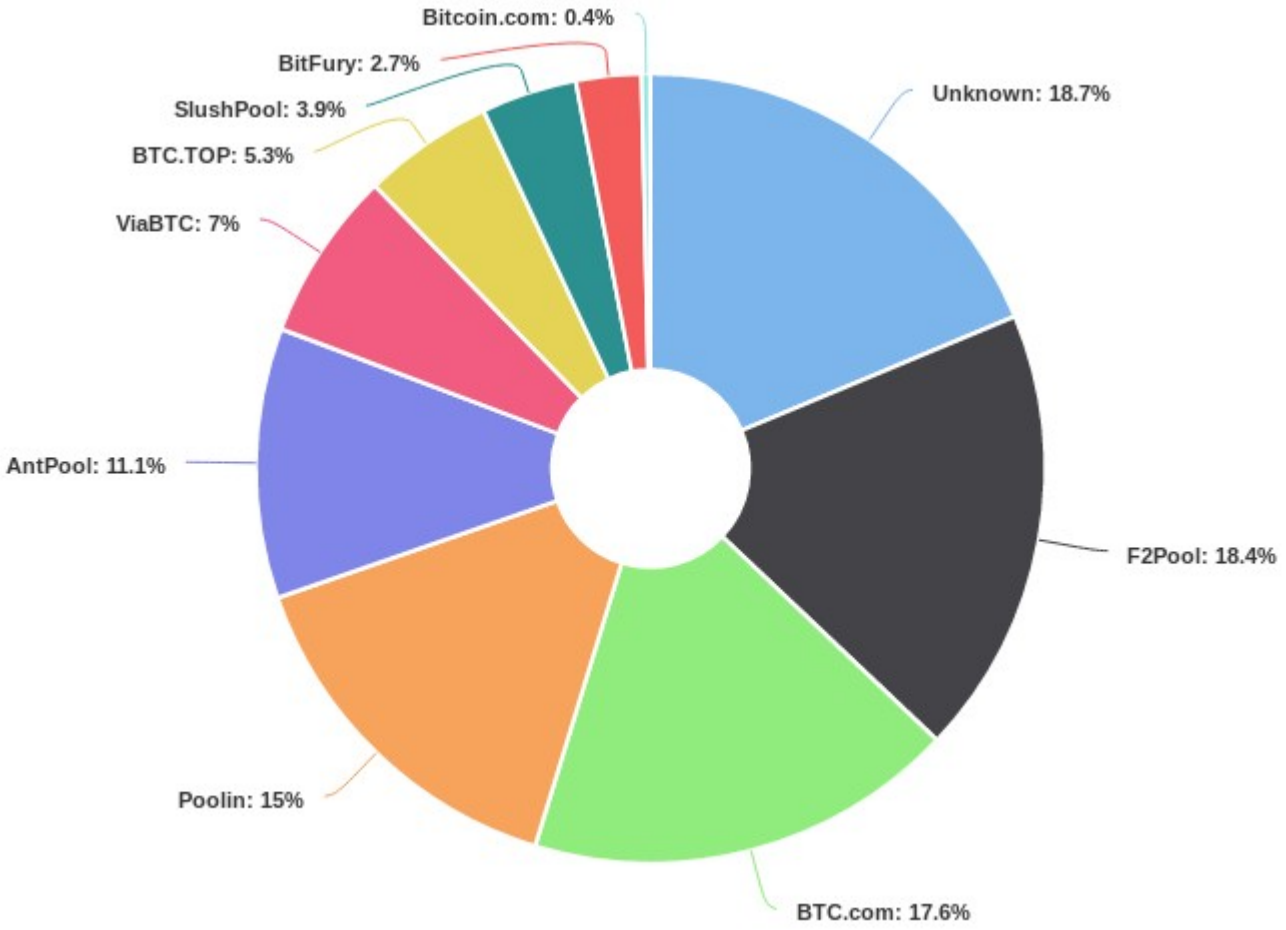


ASIC

Майнинг-ферма



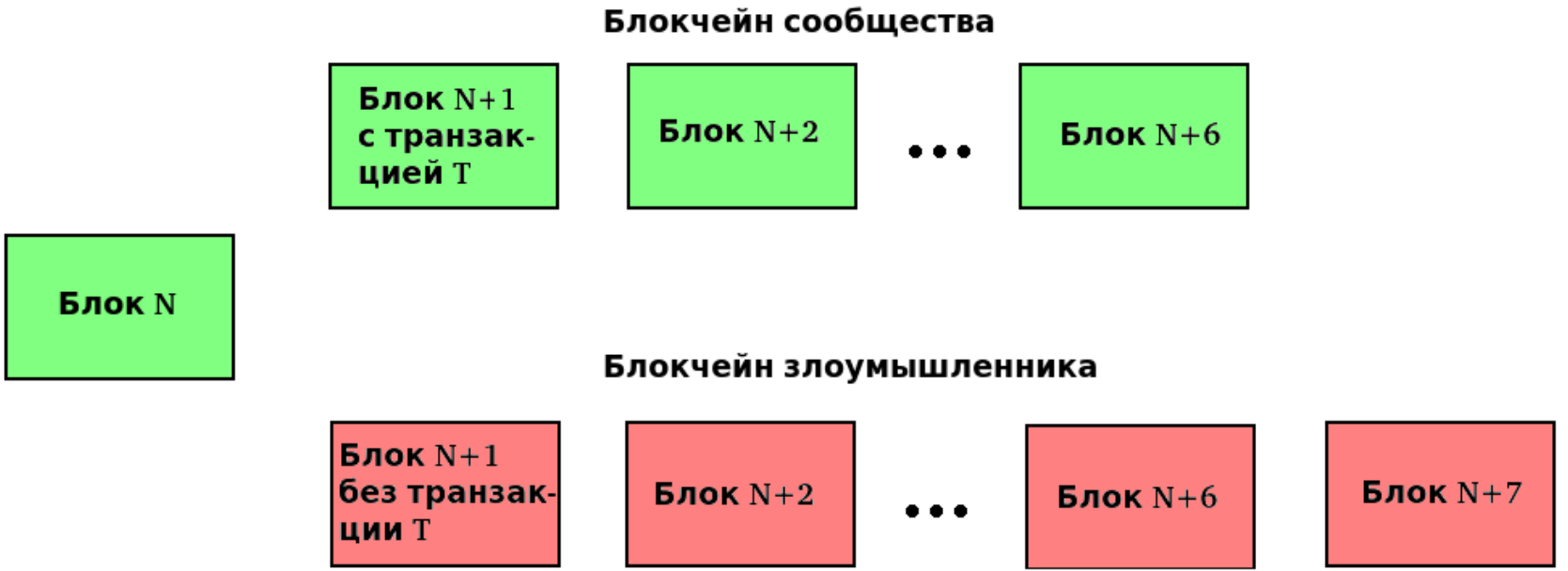
Майнинг-пулы



Майнинг

- **ASIC** (application-specific integrated circuit - интегральная схема специального назначения) – специализированное оборудование для вычислений SHA256. Скорость порядка 10^{12} хеш в секунду (компьютер порядка 10^{6}).
- **Майнинг-ферма** - локально расположенный программно-аппаратный комплекс, объединяющий большое количество вычислительных устройств (процессоры, видеокарты и/или ASIC-майнеры) и предназначенный для эффективного майнинга криптовалюты за счет распараллеливания вычислений.
- **Майнинг-пул** - территориально распределенный программно-аппаратным комплекс. Он объединяет сотни или тысячи различных участников, в т.ч. и майнинг-фермы, для более эффективного майнинга. Доходы в этом случае распределяются между участниками пула, как правило, согласно их вклада в процесс добычи BTC.

Атака 51%



После передачи товара или оказания фактической услуги за оплату по транзакции T, злоумышленник представляет сети свою более сложную ветвь блокчейн без транзакции T. В результате он и получает блага, и оставляет деньги на своем счету (двойная трата).

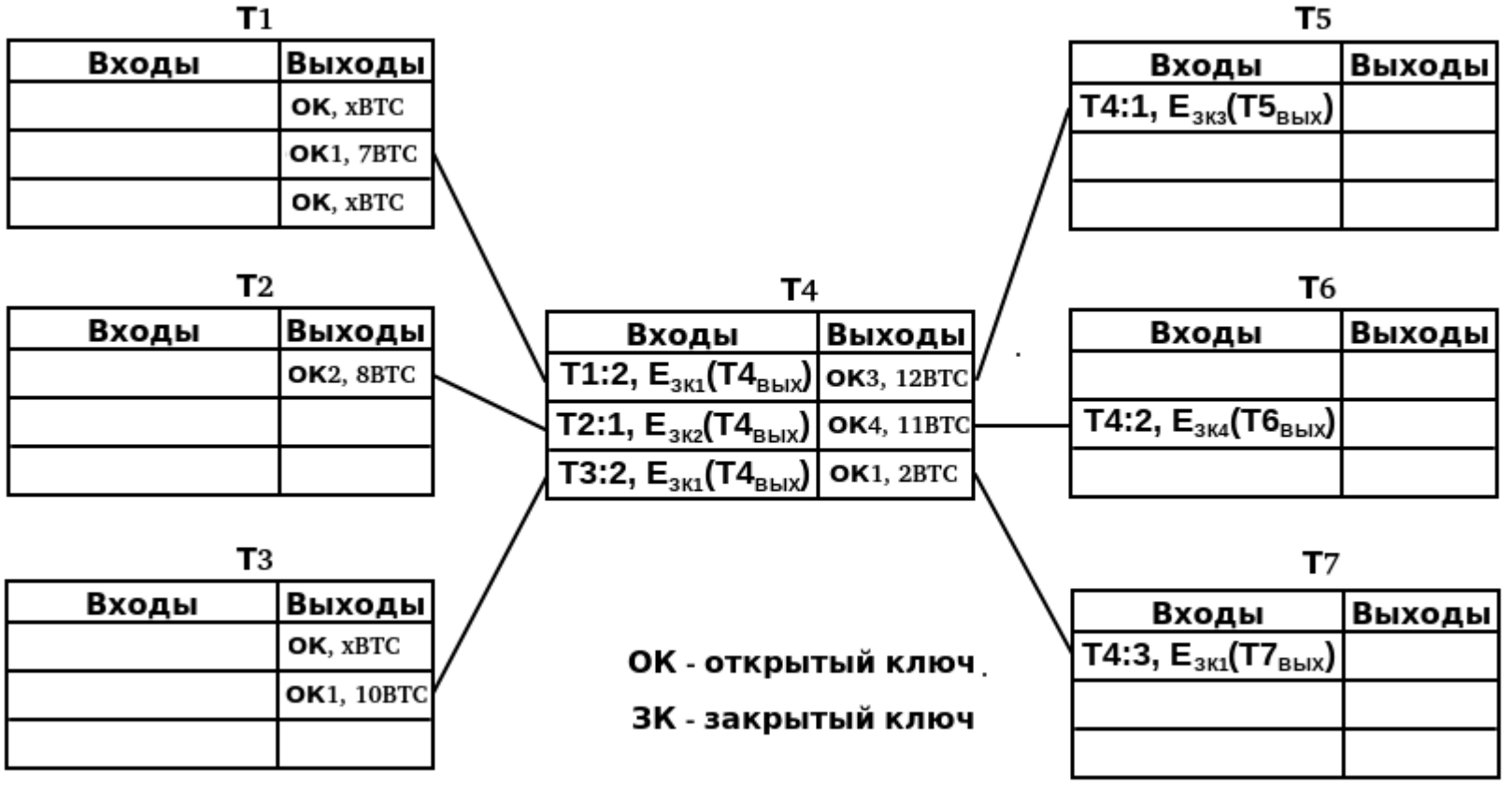
Биткойн-Script

Входные и выходные поля транзакций биткойн содержат в себе необольшие программы на специальном скриптовом языке.

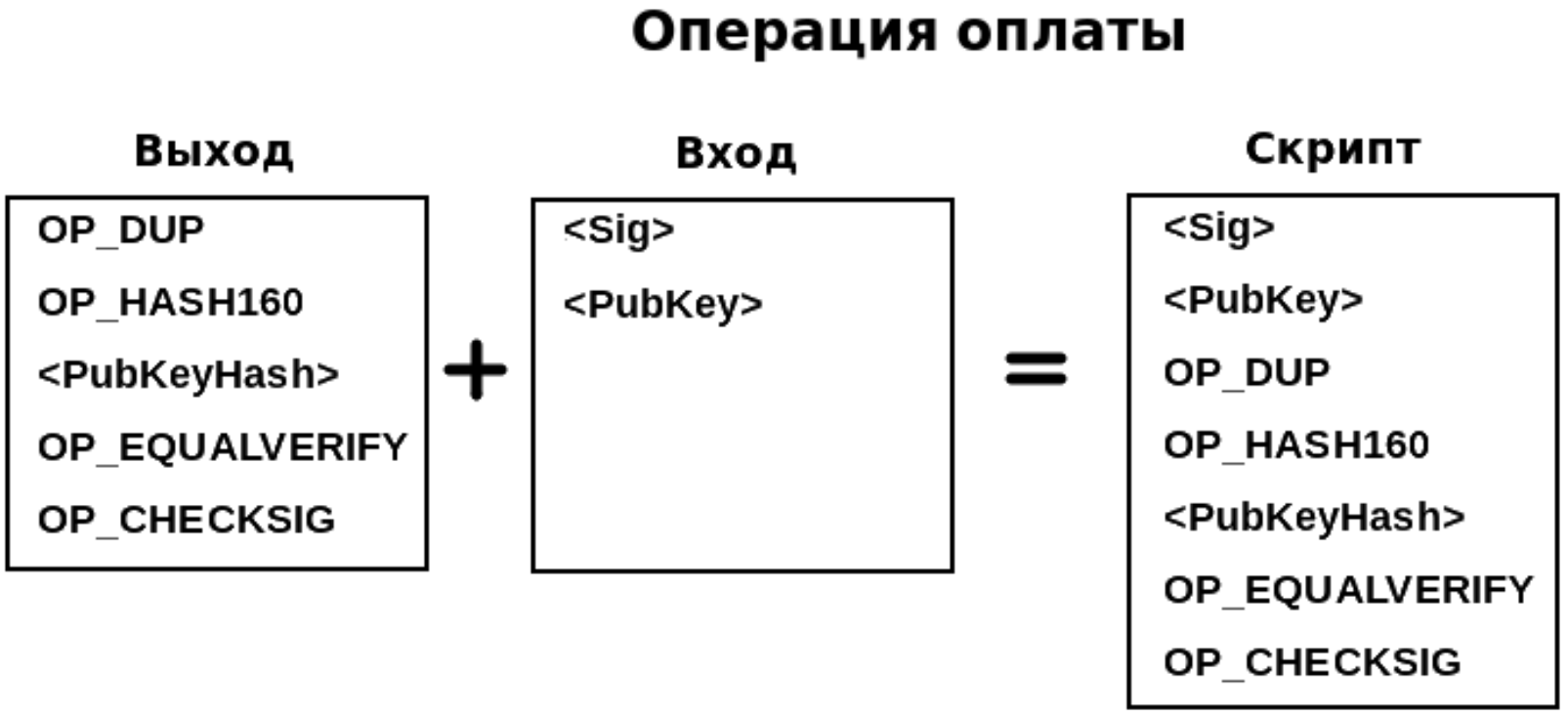
Скриптовой язык Биткойн:

- 166 команд
- есть операторы ветвления, арифметические команды, криптографические команды
- нет циклов
- для хранения переменных используется стек

Биткойн-Script



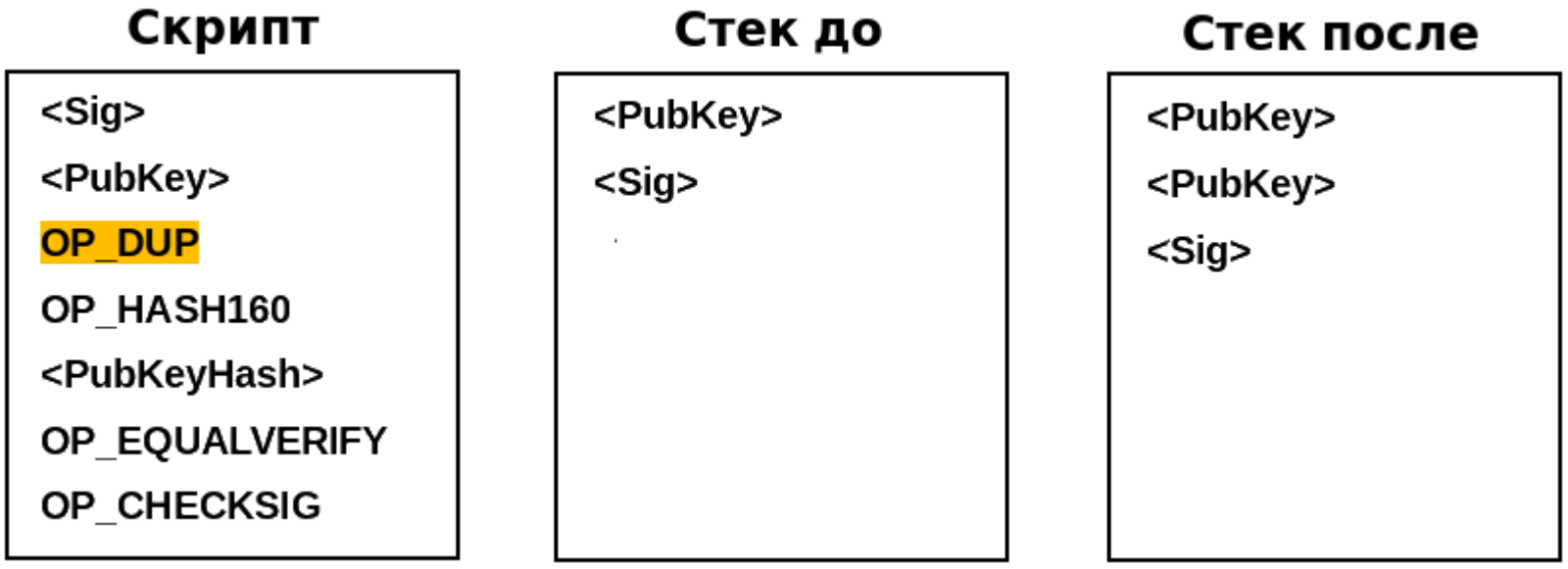
Биткойн-Script



Операция оплаты

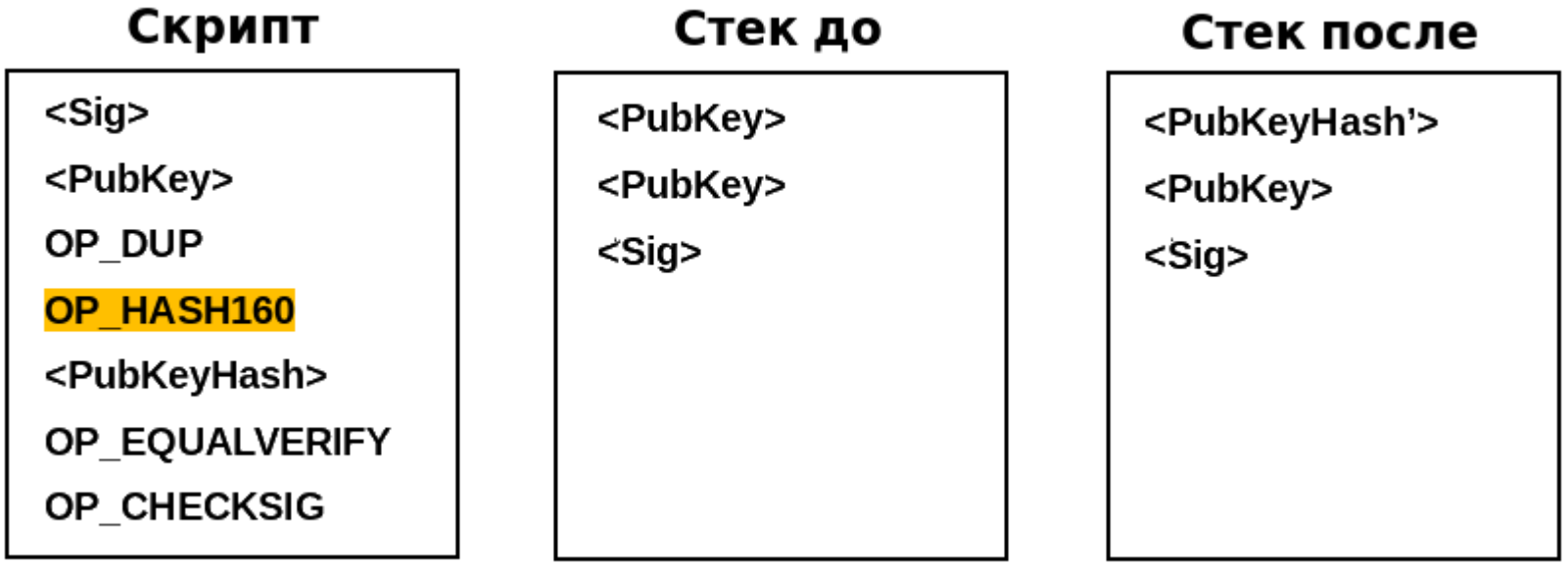
Операция оплаты

Операция оплаты



OP_DUP (код 0x76) – создание копии верхнего значения в стеке

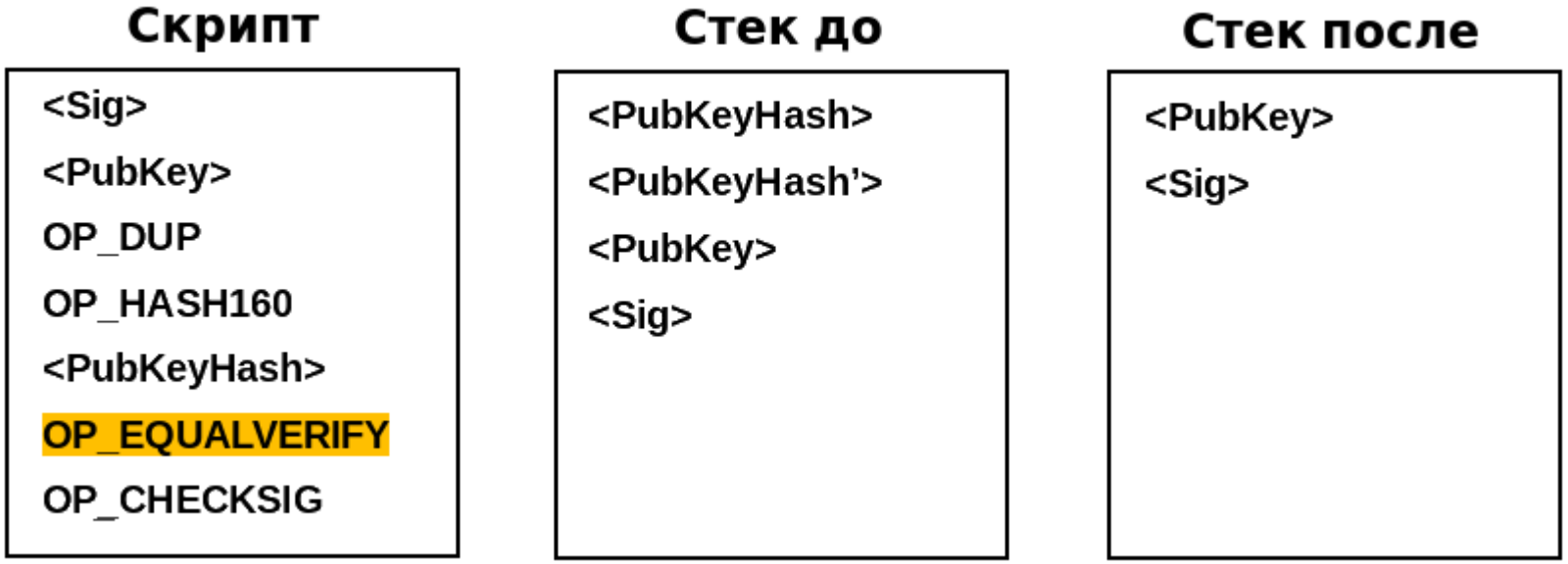
Операция оплаты



OP_HASH160 (код 0xa9) – вычисление хеша от верхнего аргумента стека

Операция оплаты

Операция оплаты

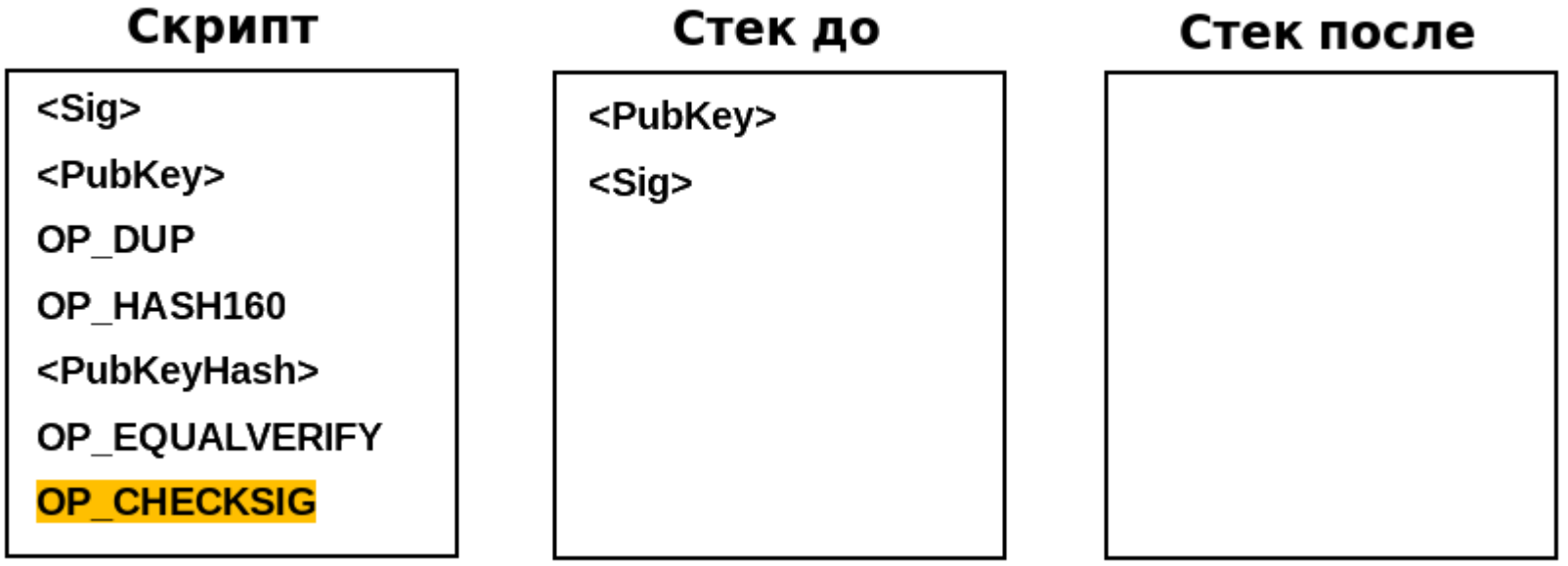


OP_EQUALVERIFY (код 0x88) – сравнение двух верхних значений в стеке

PubKeyHash – хеш открытого ключа в выходном поле

PubKeyHash’ - хеш от открытого ключа во входном поле

Операция оплаты



OP_CHECKSIG (код 0xAC) – проверка правильности подписи транзакции
PubKey – открытый ключ подписи
Sig – подпись транзакции на закрытом ключе

Биткойн-Script

Транзакция принимается только в том случае, если во время исполнения скрипта не возникло ошибок.

В биткойн-script нет циклов, поскольку проверяющий запускает скрипт на собственных вычислительных мощностях.

Ethereum

- Криптовалюта и платформа для создания онлайн-сервисов на базе блокчейн.
- Обменная единица – эфир (ETH).
- Основной приоритет отдается смарт-контрактам.
- Запущена 30 июля 2015 г.

Смарт-контракты

- Язык команд в Ethereum более функциональный по сравнению с Биткойн и поддерживает циклы.
- Смарт-контракты разрабатываются на различных языках программирования (Solidity, Vyper, Mutan, LLL).
- Перед загрузкой в блокчейн смарт-контракты переводятся в байт-код, который выполняется в Ethereum Virtual Machine (EVM).
- За исполнение контракта составитель платит вознаграждение (газ).
- Контракты могут запускать другие контракты, находящиеся в блокчейн, изменять внутренние данные.

Смарт-контракты

- Плата за исполнение контактов защищает майнеров от атаки на их вычислительные мощности.
- Перед выполнением каждой операции виртуальная машина проверяет, достаточно ли еще газа осталось. Если газ закончился, то выполнение контракта прерывается, изменения не сохраняются, потраченный газ отправителю контракта не возвращается.
- Абонент должен быть уверен в вызываемых контрактах.

DAO

- Decentralized Autonomous Organization – крупнейший краудфандинговый проект на основе Ethereum (разработан Stock.it и командой Ethereum).
- Участник может выбрать или предложить проект для инвестиций. Участники проекта могут заключить договор с исполнителем, контролировать выполнение проекта, получать прибыль.
- В июне 2016 года неизвестный обнаружил уязвимость в протоколах DAO и перевел на свои счета 50 млн. долларов.

PoW

- **Proof of work** (доказательство выполненной работы) – принцип, основанный на выполнении на стороне клиента сложных вычислений, которые легко проверяются на стороне сервера.
- Биткойн и Ethereum основываются на принципе PoW.
- PoW позволяет обеспечить достоверность данных блокчейн без доверительных центров.
- Технология PoW очень ресурсозатратна (затраты электроэнергии и материалы для вычислителей).

PoS

Proof of Stake (подтверждение доли) – альтернативный механизм организации блокчейн, не требующих высоких вычислительных мощностей.

Минтинг (minting - чеканка) - процесс решения вычислительной задачи по добавлению нового блока в системе PoS.

Классический PoS

- hash(B,nonce) <= M/D – для PoW
- hash(B, hash(B_{prev}), A, t) <= bal(A)*M/D – для PoS
  - [0..M] – область значений хеш-функции
  - D – целевая сложность
  - hash(B_{prev}) – хеш предыдущего блока
  - A – адрес пользователя
  - bal(A) – баланс пользователя
  - t – текущее время (UTC) – единственный параметр, значение которого изменяется

Модификации PoS

$hash(B, hash(B_{prev}), A, t) <= bal(A)*age(A)*M/D$

age(A) – время, прошедшее с тех пор, как A сгенерировал предыдущий блок

$hash(B, hash(B_{prev}), A) <= t*bal(A)*M/D$

Проблема “Ничего на кону”

Рациональное поведение пользователя в PoS - минтить блоки во всех известных ветках.

Это проблема облегчает атаку двойного расходования.

Проблема начального распределения

Начальные держатели монет не заинтересованы в трате денег.

Валюта становится менее привлекательной для использования.

Атака издалека

Оперируя наборами транзакций в блоке, атакующий может строить альтернативный блокчейн быстрее настоящего.

Новому участнику непонятно, какой блокчейн является истинным.

Атака взятками

Атакующий получает товары или услуги за транзакцию.

Атакующий объявляет награду за строительство альтернативного блокчейна без проведенной транзакции.

Атакующий платит взятки пока система не выберет альтернативный блокчейн.

Атака накоплением возраста монет

$hash(B, hash(B_{prev}), A, t) <= bal(A)*age(A)*M/D$

Атакующий должен завести несколько счетов и долго не тратить с них деньги для повышения age(A).

Во время атаки этими счетами он быстрее остальной сети создает блоки для своего блокчейна, который не содержит транзакции оплаты.

Атака предвычислением

$hash(B, hash(B_{prev}), A, t) <= bal(A)*M/D$

Атакующий анализирует A_i всех абонентов сети и подбирает транзакции в текущем блоке так, чтобы быть первым, кто решит следующий блок.

Сложность зависит от количества участников сети и доли атакующего.

DPoS

DPoS (delegated PoS) – система PoS с делегированием.

В системе выбирается небольшая доверенная группа пользователей – делегатов.

Каждый новый блок для принятия в блокчейн должен быть подписан несколькими делегатами.

Делегаты получают награду за свою деятельность, но могут быть оштрафованы, если совершат атаку на систему.

Обычно делегат должен сделать гарантийный депозит, где средства временно блокируются.

Защита от атак

“Ничего на кону” - использование DPoS, штраф за поддержку нескольких блокчейнов.

“Атака издалека” - установка максимальной точки ветвления (в Nxt – не более 720 блоков). Новый пользователь загружает блокчейн из доверенного источника.

“Атака взятками” - использование DPoS, штрафы за поддержку второй блокчейн.

“Атака накоплением возраста монет” - установление максимального возраста монет (обычно 90 дней).

“Атака предвычислением” - использование DPoS, поскольку последний блок изменяется после подписи делегатами.

https://sesc-infosec.github.io/