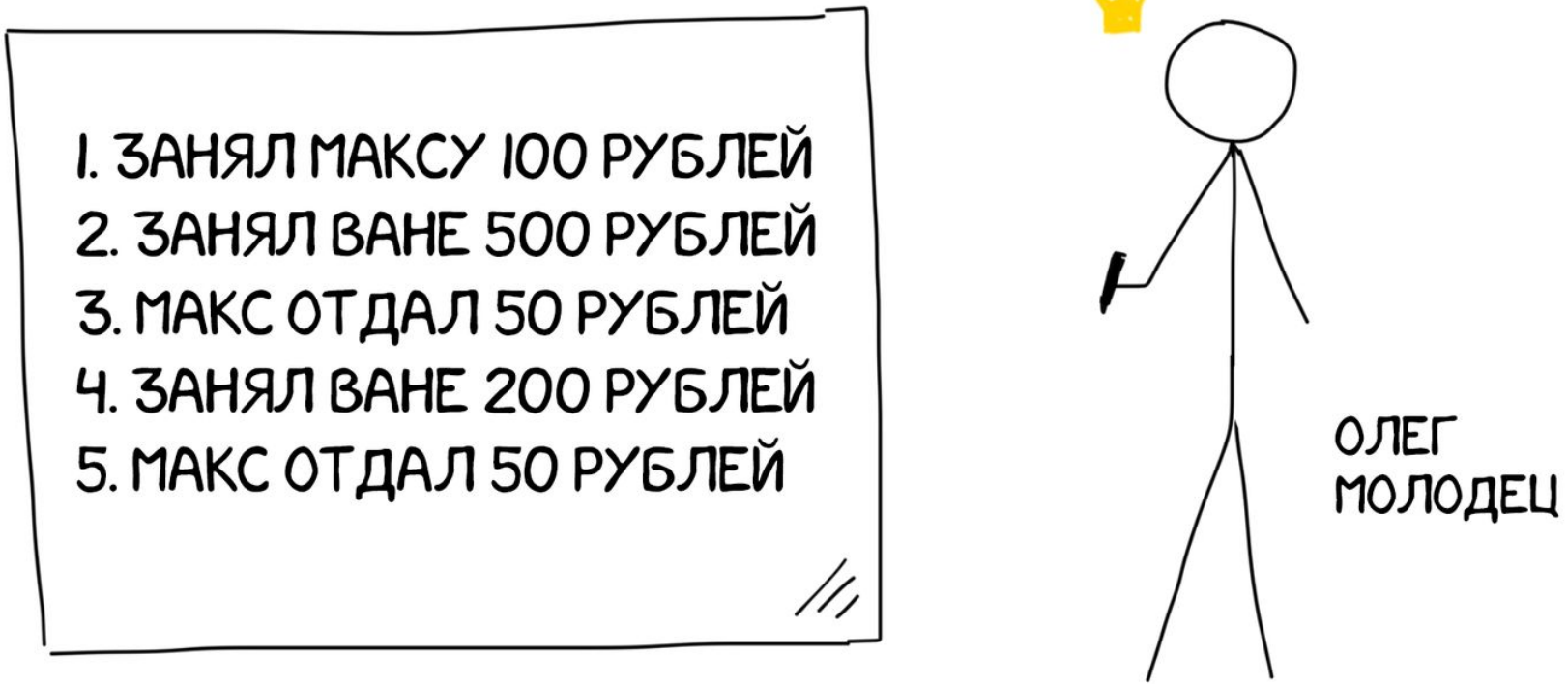
BlockChain технологии

Основы: зачем нам блокчейн?

Блокчейн появился вместе с биткоином, но может использоваться независимо от него и даже модифицироваться. Любой может сделать свой блокчейн хоть у себя на ноутбуке.

Список, который нельзя изменить



Список, который нельзя изменить

СТРОКА: ВАСТРИК

ХЕШ: 110A84203960300D21F1C422FAA76089C9
D912345DA701AB09E5A02920F95059E

СТРОКА: ВАСТРИК.

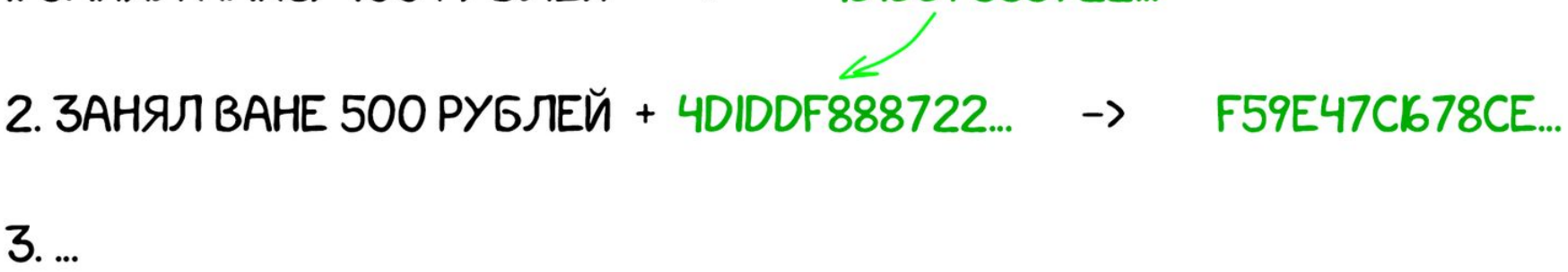
ХЕШ: 7D762A3227E6B1A66F49A54B7C749FA8
B5E5C733B15C05F7B4DF9BA2D9AEEC00

Список, который нельзя изменить

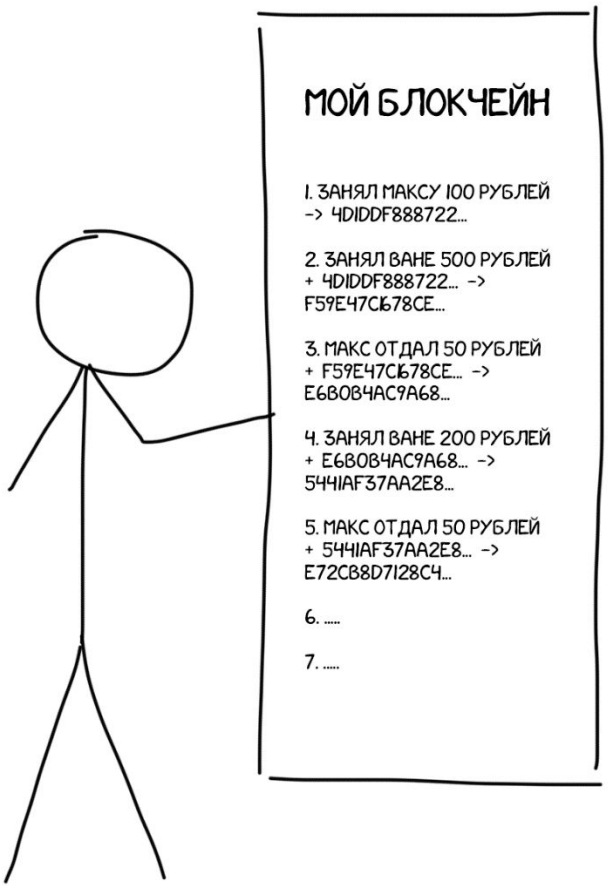
SHA-256

1. ЗАНЯЛ МАКСУ 100 РУБЛЕЙ	->	4D1DDF888722...
2. ЗАНЯЛ ВАНЕ 500 РУБЛЕЙ	->	74CA68E54029...
3. МАКС ОТДАЛ 50 РУБЛЕЙ	->	0F32DE069639...
4. ЗАНЯЛ ВАНЕ 200 РУБЛЕЙ	->	4FC7534C7E2B...
5. МАКС ОТДАЛ 50 РУБЛЕЙ	->	F41223E2DEAF...

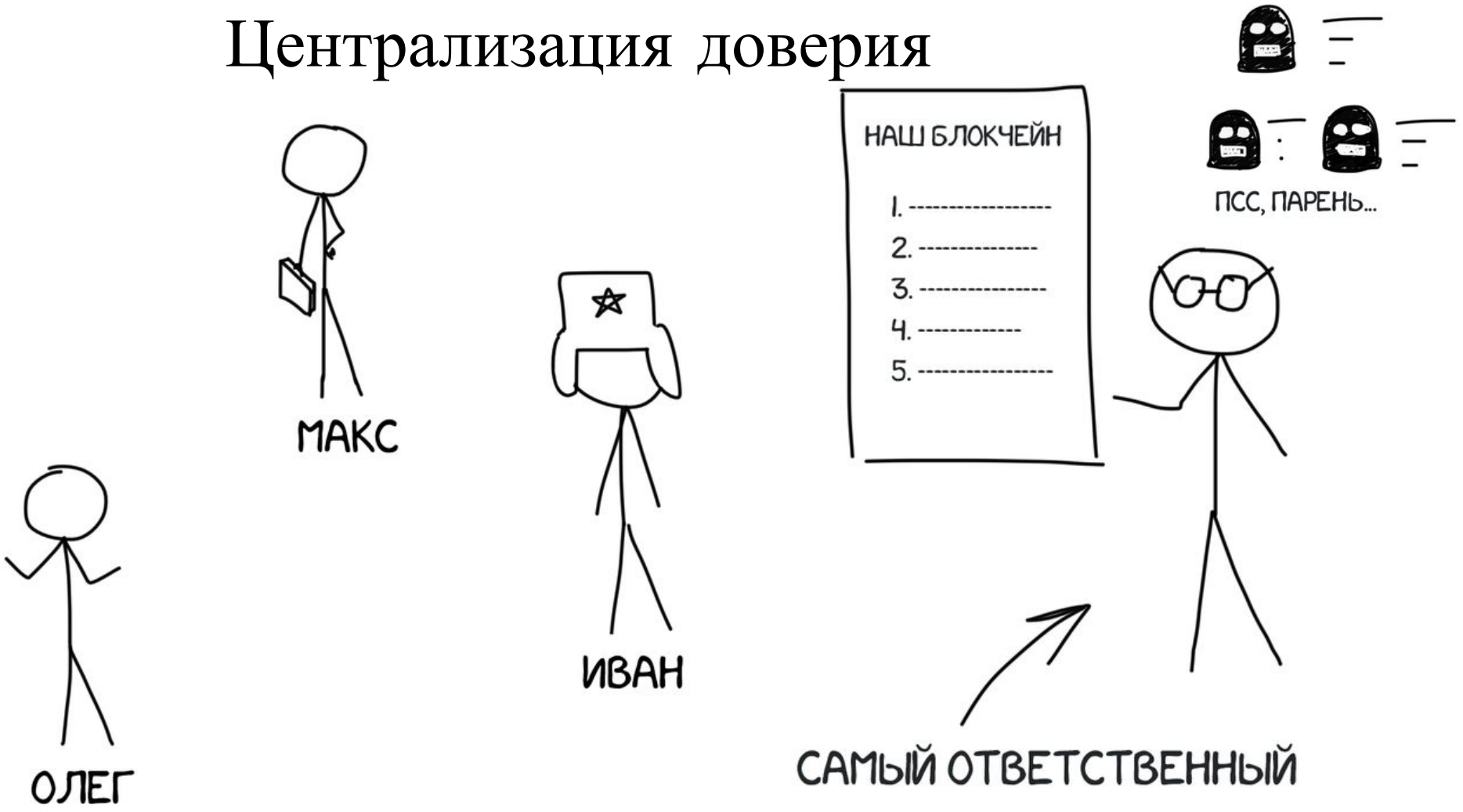
Список, который нельзя изменить



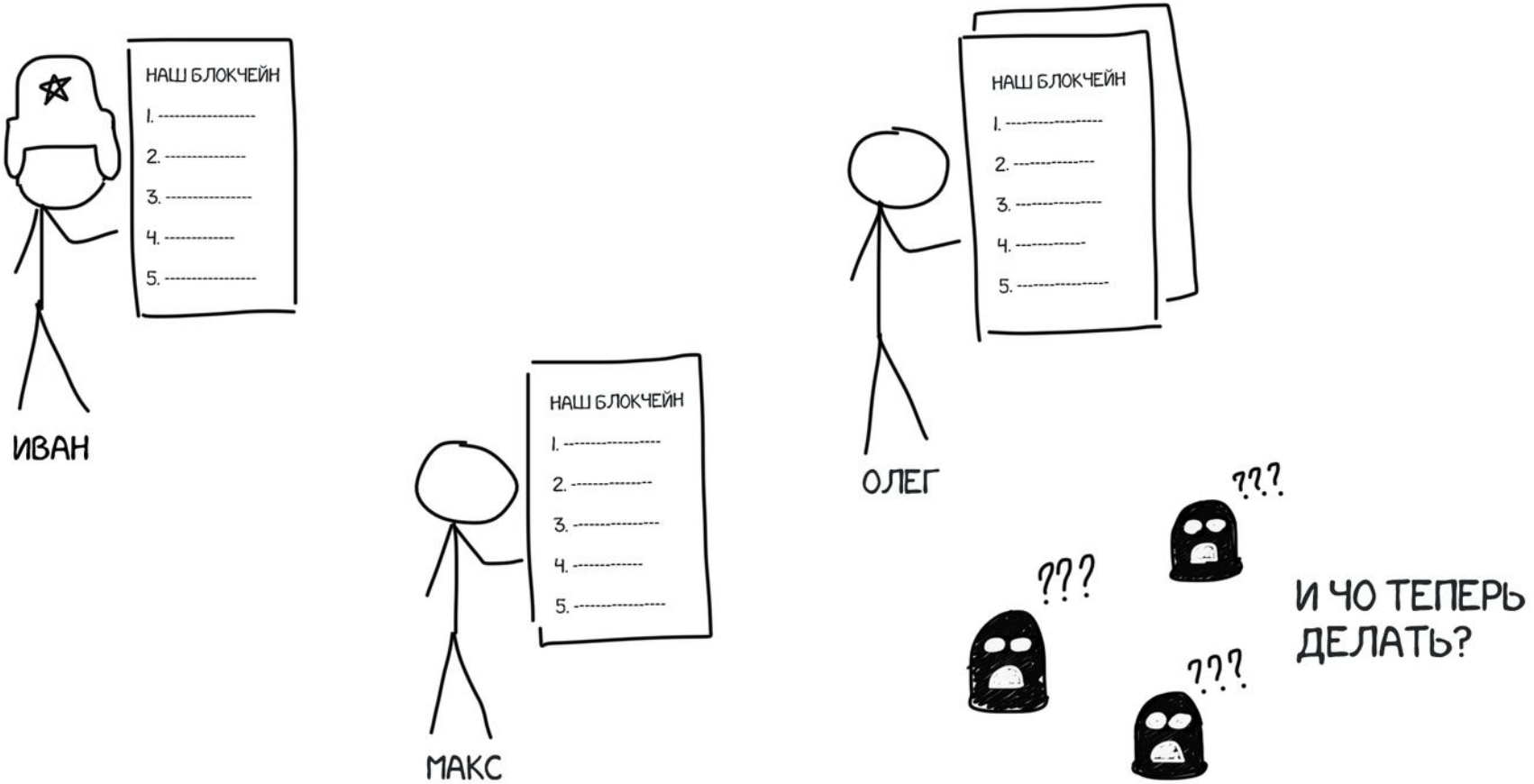
Список, который нельзя изменить



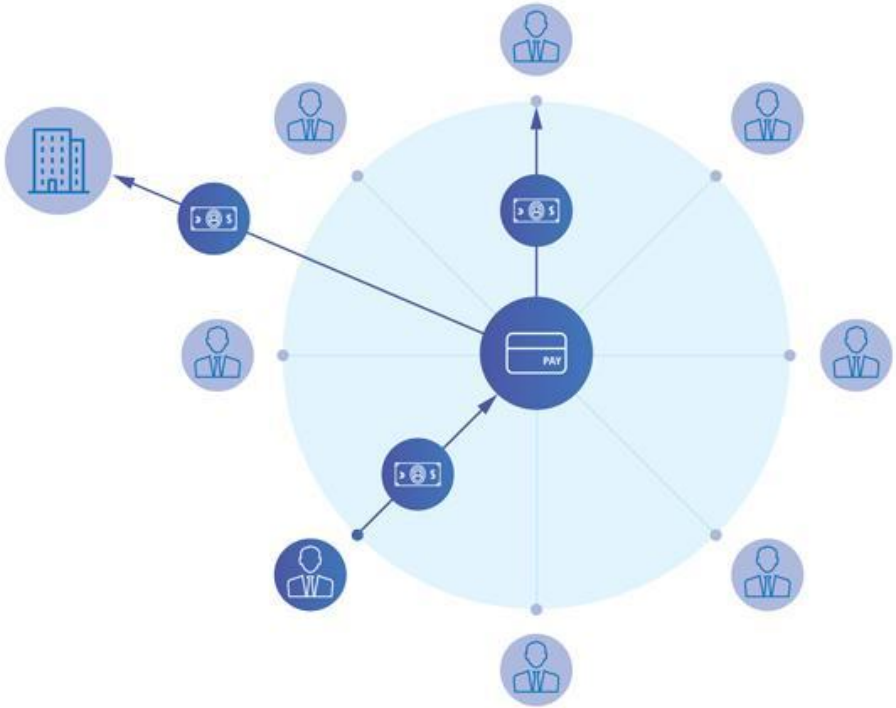
Централизация доверия



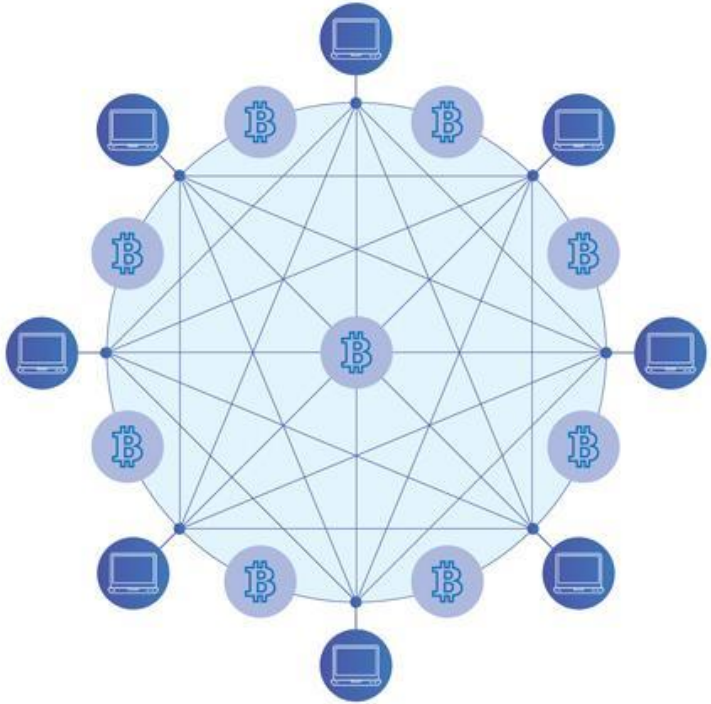
Децентрализация: никто не доверяет никому



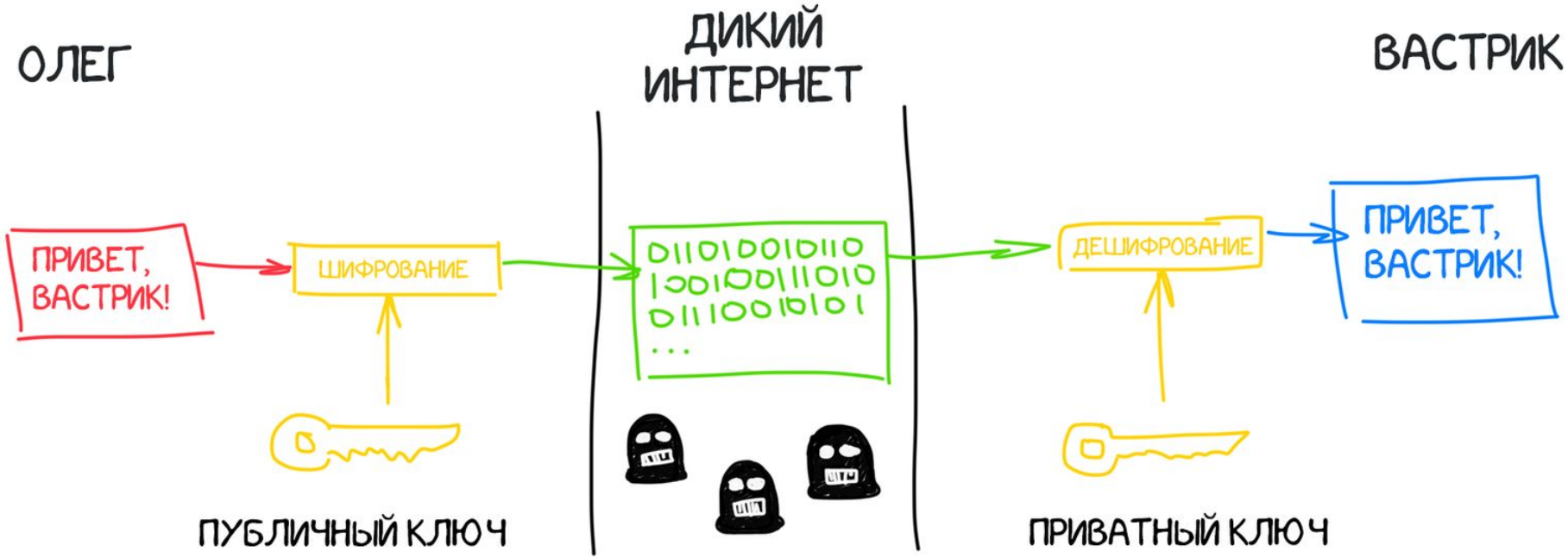
ЦЕНТРАЛИЗОВАННАЯ СИСТЕМА



БЛОКЧЕЙН-СЕТЬ

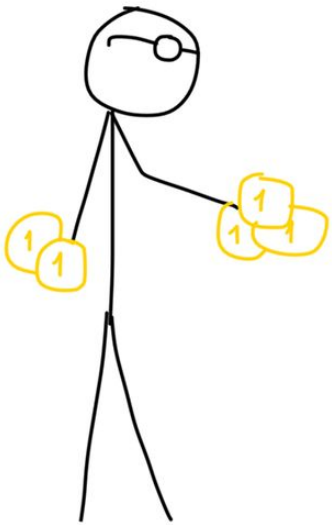


Транзакции


ОЛЕГ
ДИКИЙ ИНТЕРНЕТ
ВАСТРИК
ПРИВЕТ, ВАСТРИК!
ШИФРОВАНИЕ
ДЕШИФРОВАНИЕ
ПРИВЕТ, ВАСТРИК!
ПУБЛИЧНЫЙ КЛЮЧ
ПРИВАТНЫЙ КЛЮЧ

Транзакции

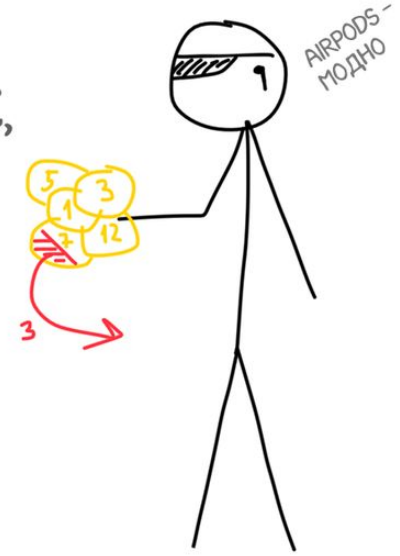
КЛАССИЧЕСКИЕ ТРАНЗАКЦИИ



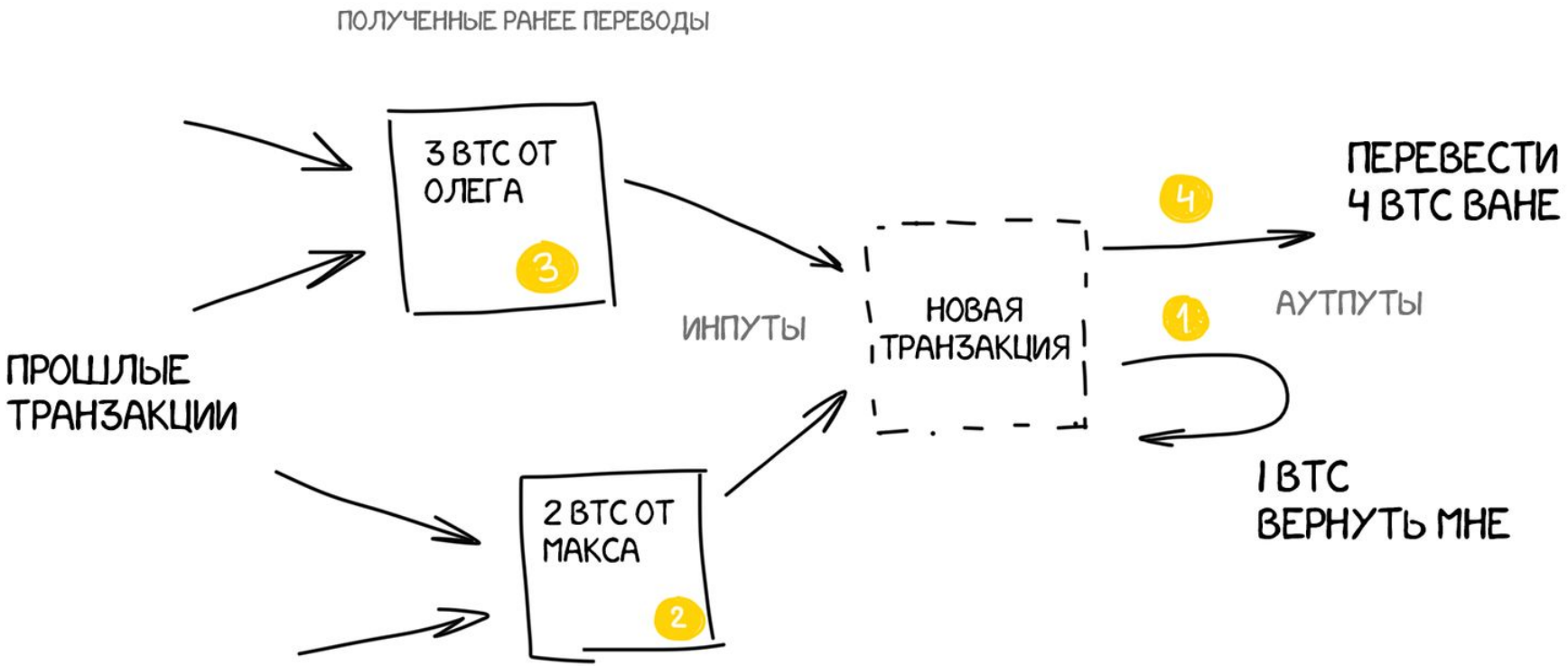
«У МЕНЯ ЕСТЬ 5 РУБЛЕЙ, ДЕРЖИ 3»

ТРАНЗАКЦИИ В БЛОКЧЕЙНЕ

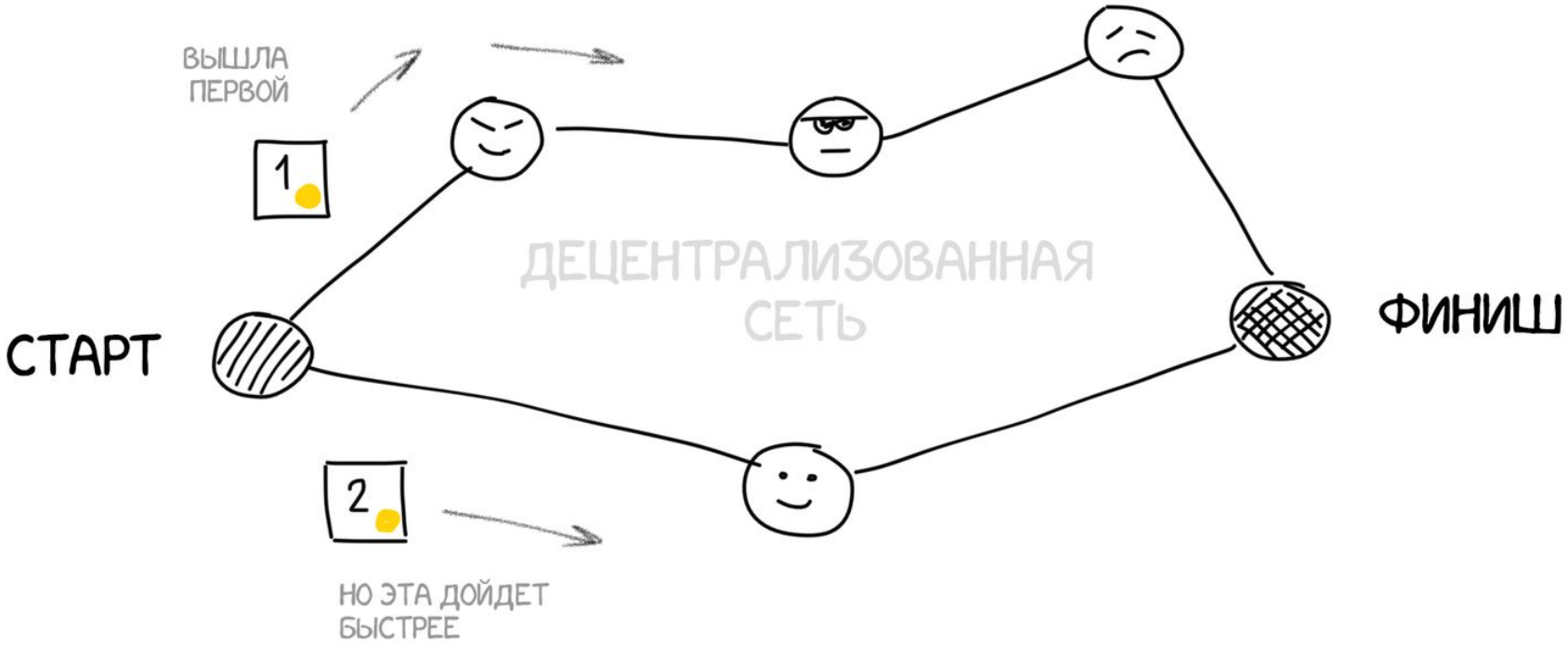
«ДЕРЖИ 25 BTC, ИЗ КОТОРЫХ 5 МНЕ ДАЛ ВАНЯ, 12 МАКС, ..., И ВЕРНИ 3 BTC СДАЧИ»



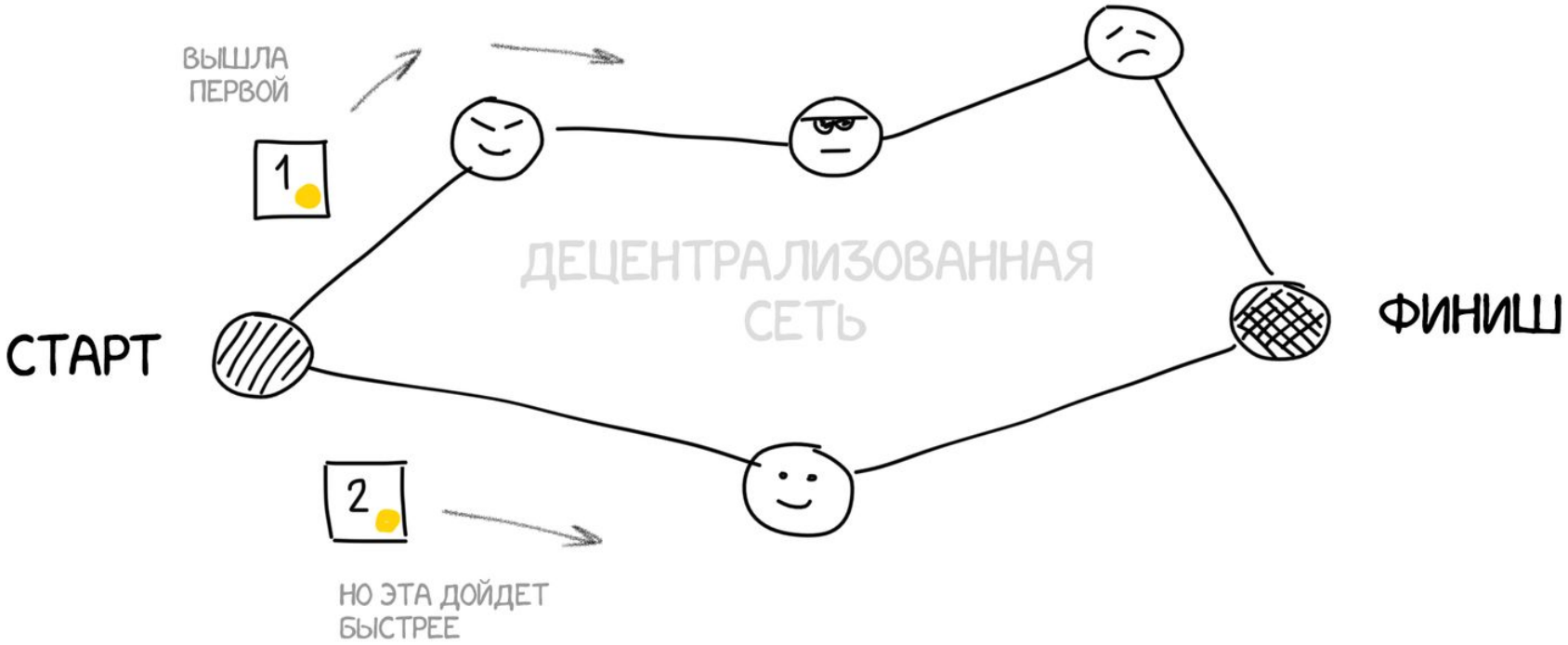
Транзакции


ПОЛУЧЕННЫЕ РАНЕЕ ПЕРЕВОДЫ
3 BTC ОТ ОЛЕГА
3
ПРОШЛЫЕ ТРАНЗАКЦИИ
ИНПУТЫ
НОВАЯ ТРАНЗАКЦИЯ
4
ПЕРЕВЕСТИ 4 BTC ВАНЕ
1
АУТПУТЫ
1 BTC ВЕРНУТЬ МНЕ
2 BTC ОТ МАКСА
2

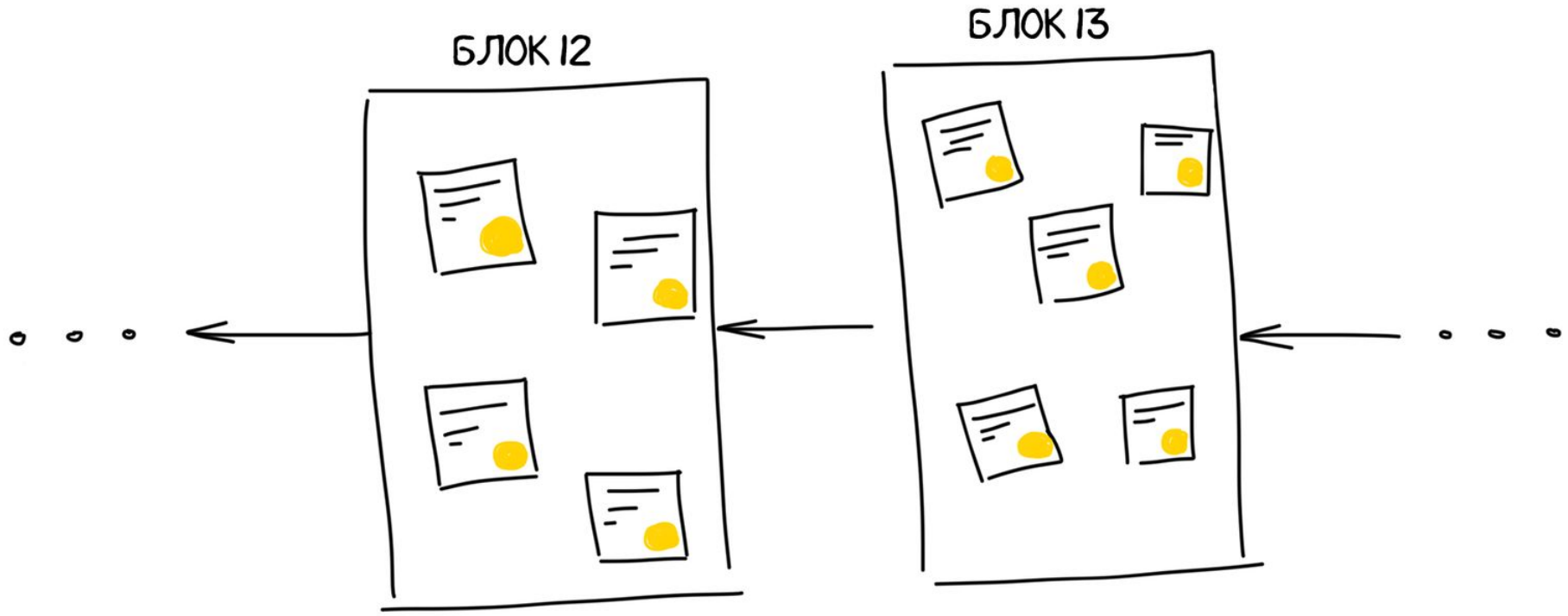
Проблема двойной траты



Проблема двойной траты

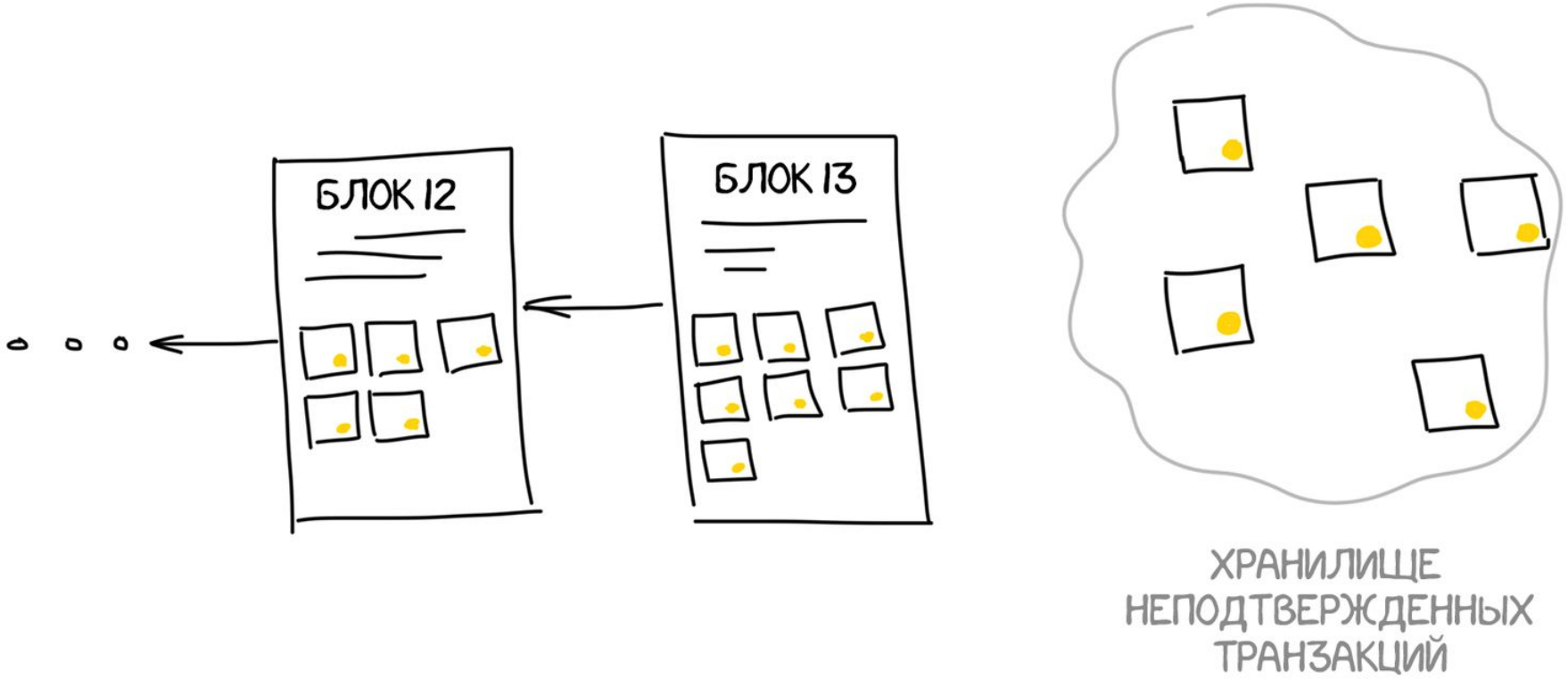


Проблема двойной траты

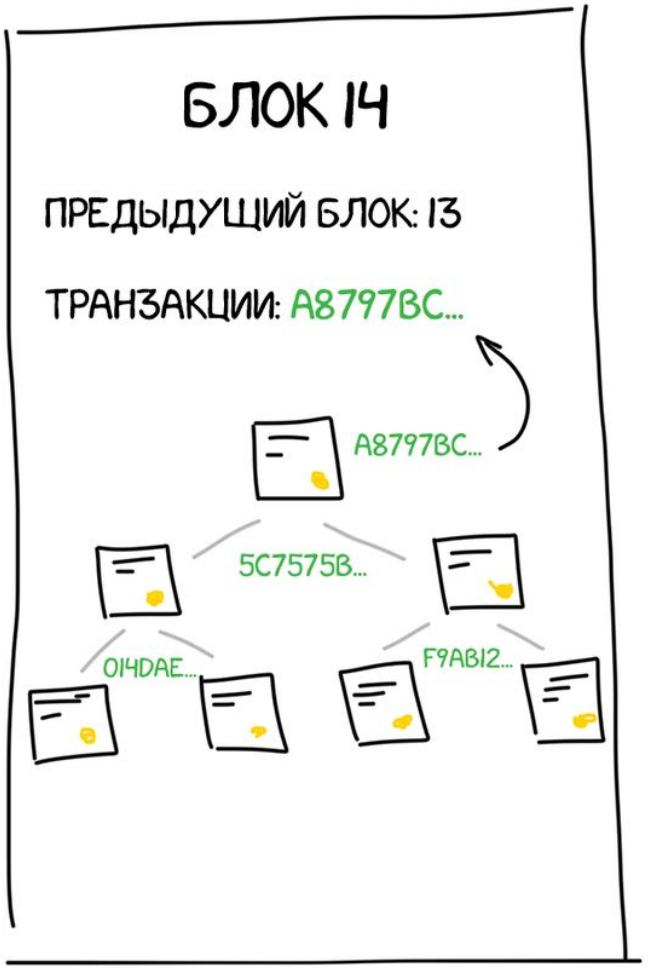


ЕСЛИ ДОБАВЛЯТЬ ТРАНЗАКЦИИ БЛОКАМИ РАЗ В 10 МИНУТ,
ТО НЕ БУДЕТ ВОПРОСОВ КТО БЫЛ ПЕРВЫМ

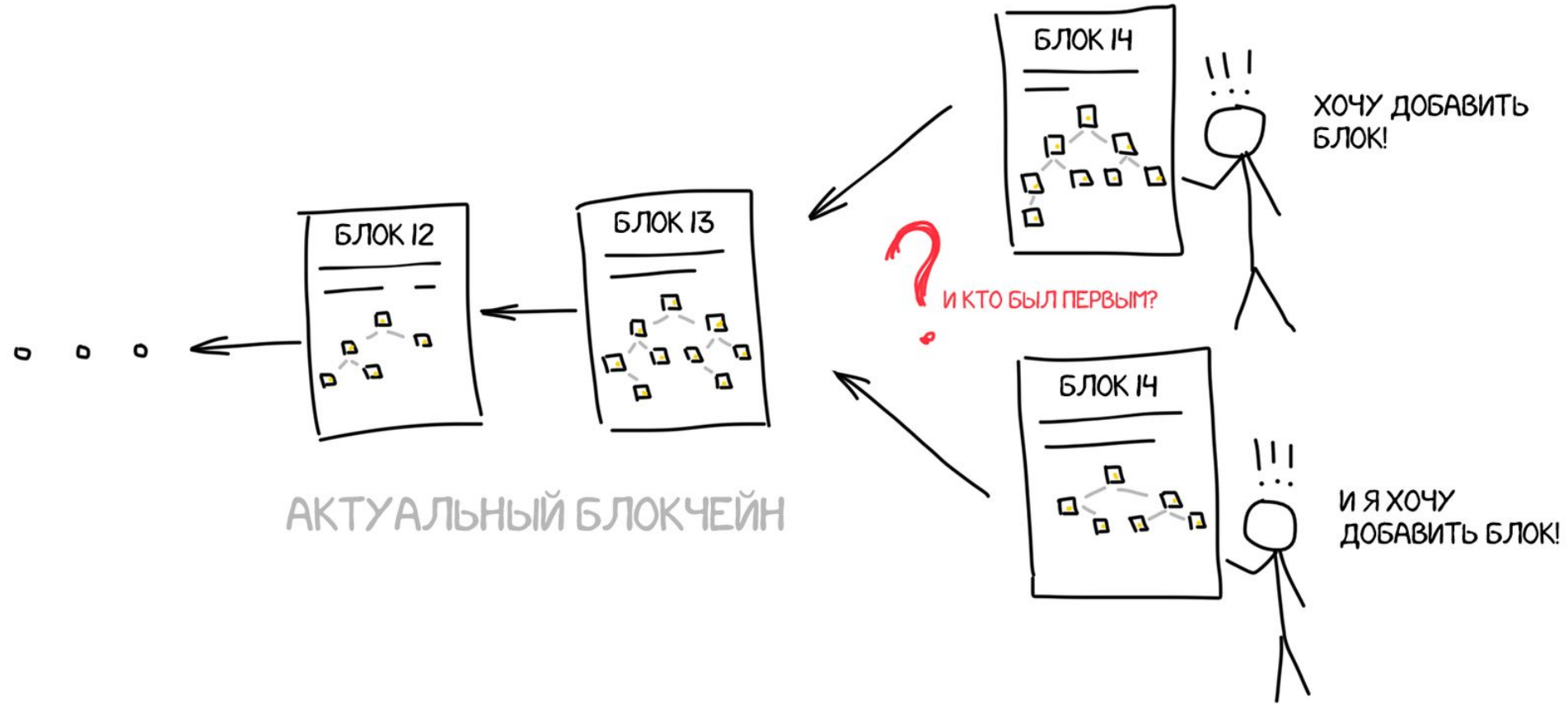
Блоки — основа блокчейна



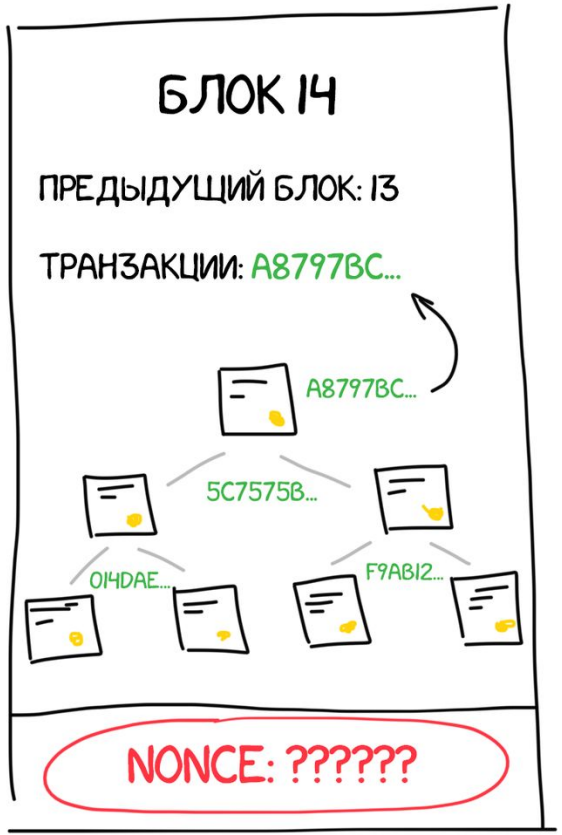
Дерево Меркла

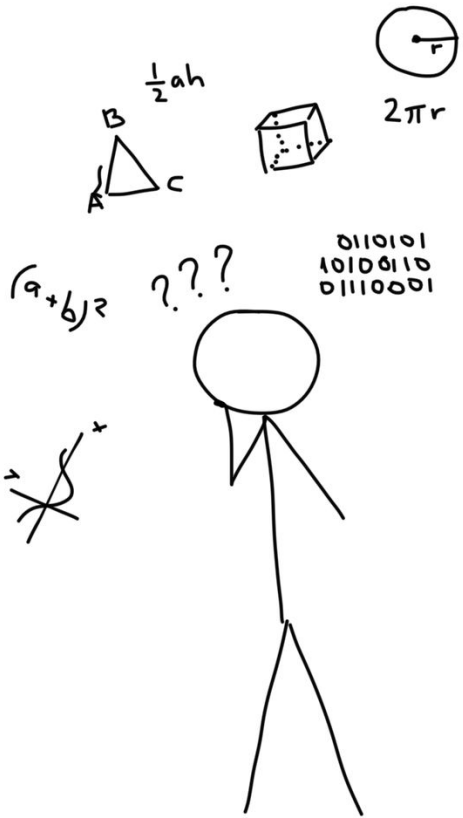


Майнинг


БЛОК 12
БЛОК 13
БЛОК 14
ХОЧУ ДОБАВИТЬ БЛОК!
И КТО БЫЛ ПЕРВЫМ?
БЛОК 14
И Я ХОЧУ ДОБАВИТЬ БЛОК!
АКТУАЛЬНЫЙ БЛОКЧЕЙН

Майнинг


БЛОК 14
ПРЕДЫДУЩИЙ БЛОК: 13
ТРАНЗАКЦИИ: A8797BC...
A8797BC...
5C7575B...
014DAE...
F9AB12...
NONCE: ??????

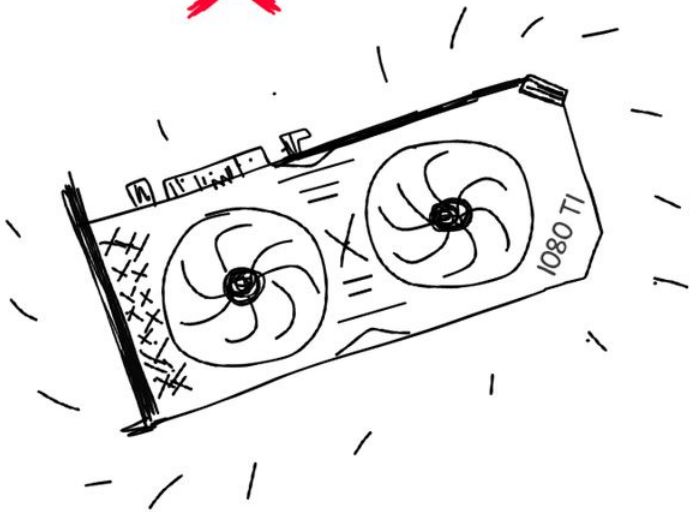

B
A
C
2πr
?.?.?

Майнинг

NONCE = 22811 -> ХЕШ: AF59CCA1A3EF5DC66B08...

NONCE = 15887893 -> ХЕШ: E62B2C97D079BE77...

ВЕЧНОСТЬ СПУСТЯ



NONCE = 54235341236123445 63... ->
ХЕШ: 0000000000010139AD76...

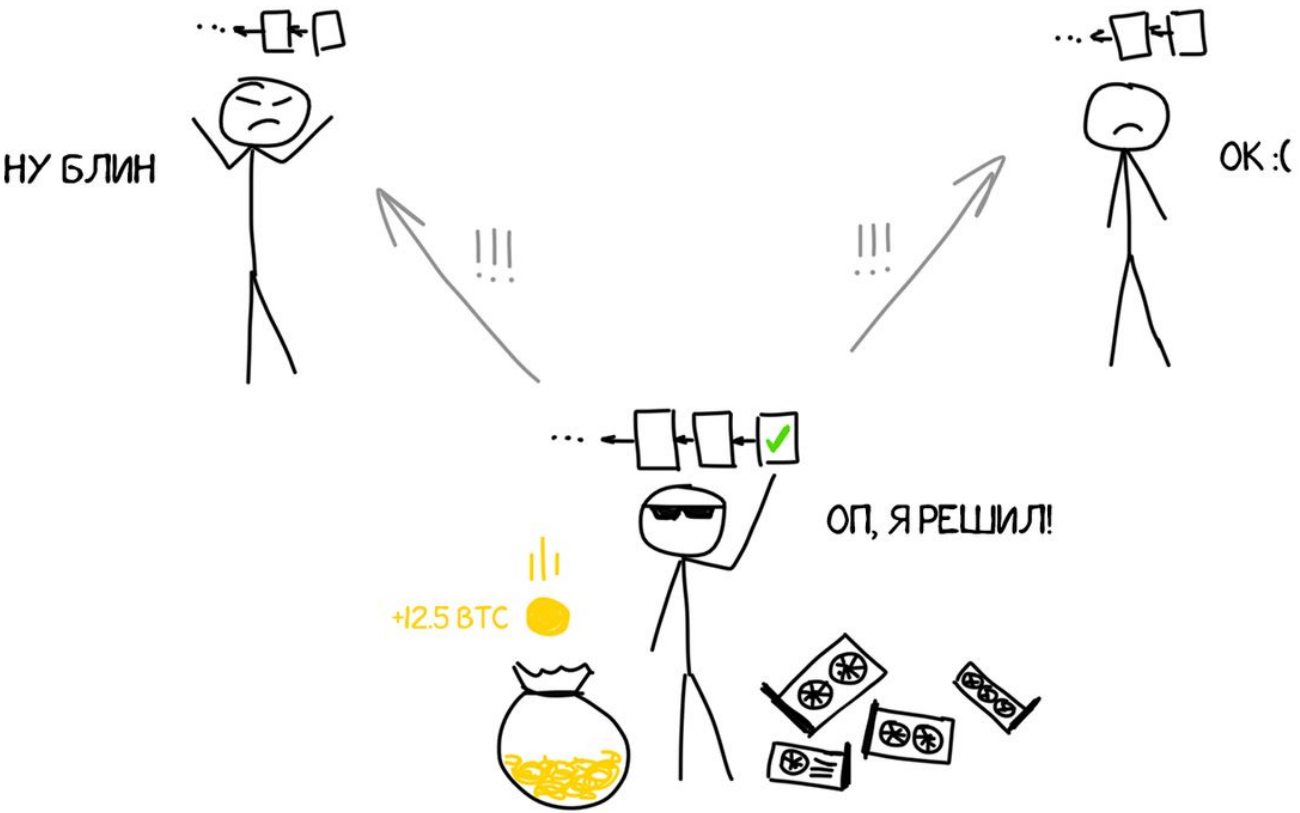
ДЕСЯТЬ НУЛЕЙ В НАЧАЛЕ!

Видеокарты с их сотнями параллельных ядер, решают эту задачу быстрее любого CPU

Ферма из восьми GTX 1070

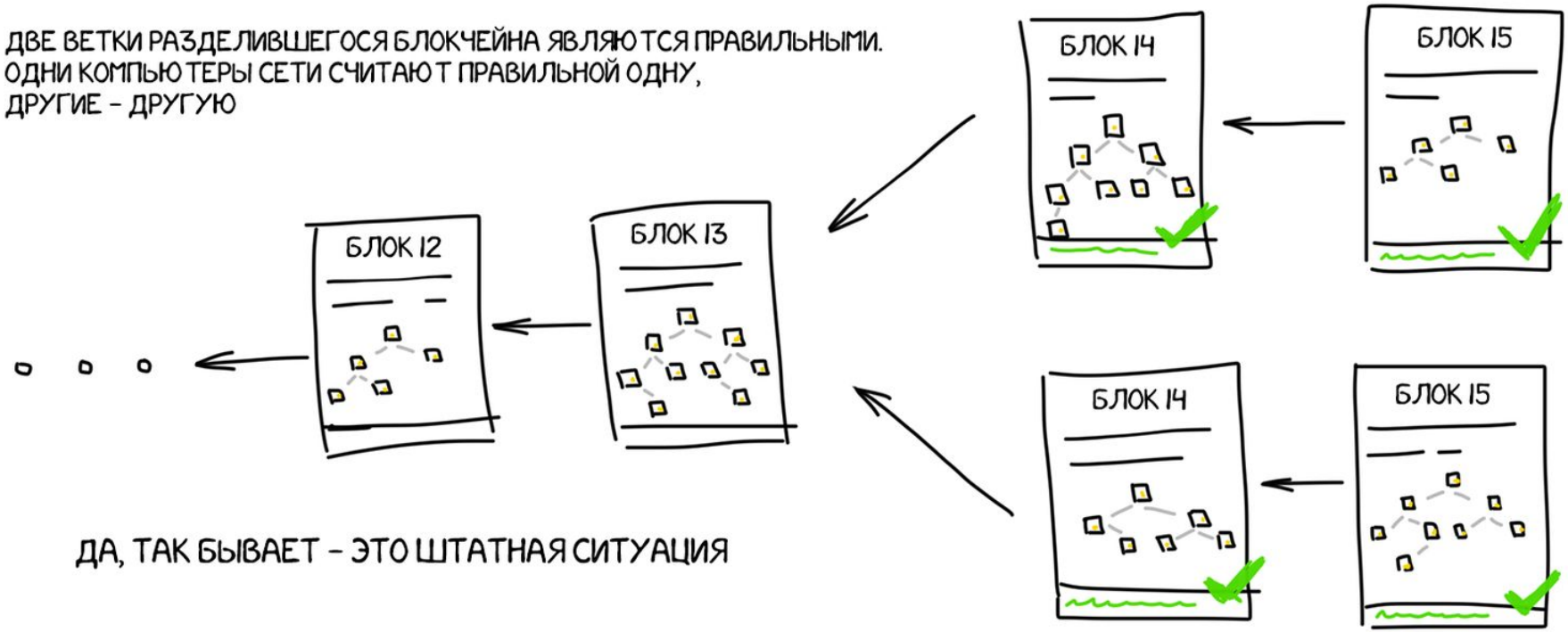
Доход			
	за сутки	за неделю	за месяц
ETH	0.040459	0.283213	1.21377
Расход электричества, кВт			
	за сутки	за неделю	за месяц
кВт	28.8	201.6	864
RUB	89.28	624.96	2678.4

Майнинг

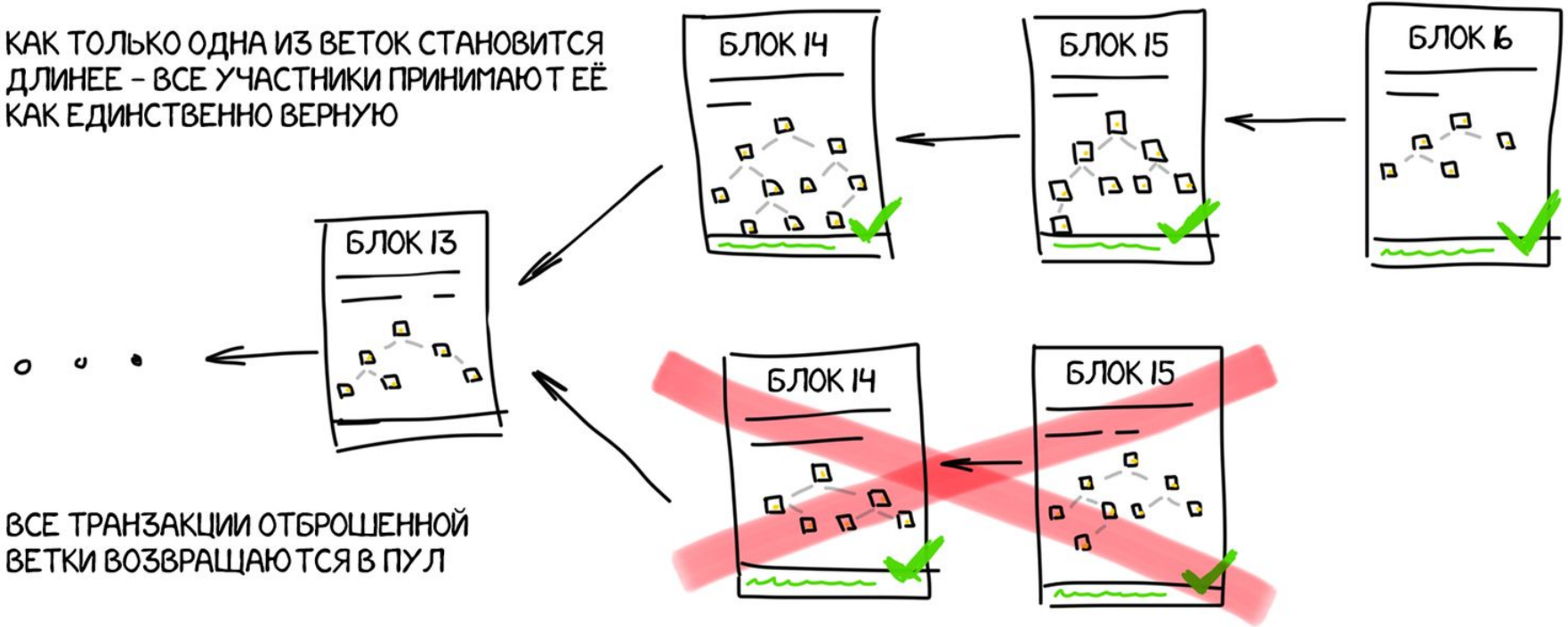


Любой блокчейн существует только пока существуют его майнеры.

Форки


ДВЕ ВЕТКИ РАЗДЕЛИВШЕГОСЯ БЛОКЧЕЙНА ЯВЛЯЮТСЯ ПРАВИЛЬНЫМИ.
ОДНИ КОМПЬЮТЕРЫ СЕТИ СЧИТАЮТ ПРАВИЛЬНОЙ ОДНУ,
ДРУГИЕ – ДРУГУЮ
БЛОК 12
БЛОК 13
БЛОК 14
БЛОК 15
БЛОК 14
БЛОК 15
ДА, ТАК БЫВАЕТ – ЭТО ШТАТНАЯ СИТУАЦИЯ

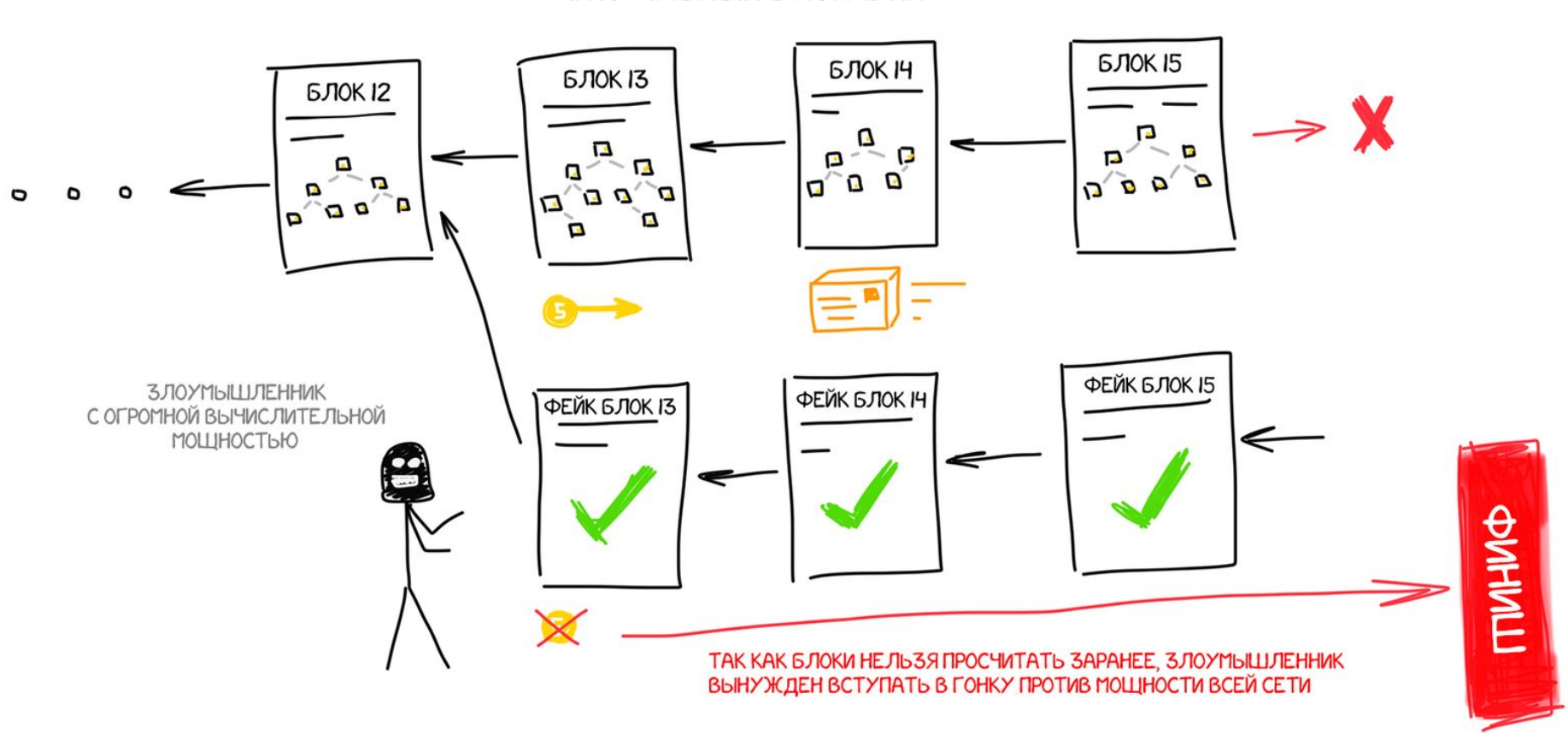
Форки


КАК ТОЛЬКО ОДНА ИЗ ВЕТОК СТАНОВИТСЯ ДЛИНЕЕ – ВСЕ УЧАСТНИКИ ПРИНИМАЮТ ЕЁ КАК ЕДИНСТВЕННО ВЕРНУЮ
БЛОК 13
БЛОК 14
БЛОК 15
БЛОК 16
БЛОК 14
БЛОК 15
ВСЕ ТРАНЗАКЦИИ ОТБРОШЕННОЙ ВЕТКИ ВОЗВРАЩАЮТСЯ В ПУЛ

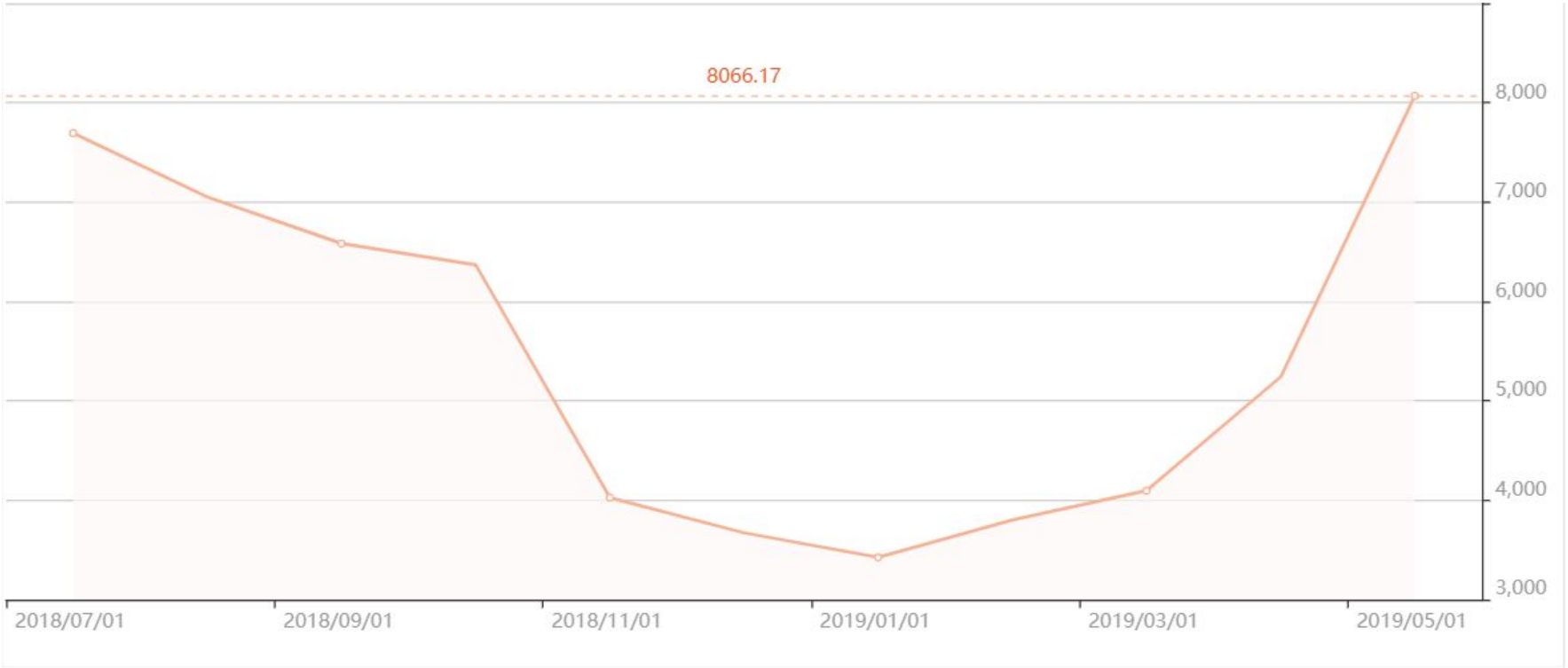
Атака **«51%»**


ПЫТАЕМСЯ ОБМАНУТЬ БЛОКЧЕЙН, УНИЧТОЖИВ СВОЮ ТРАНЗАКЦИЮ
БЛОК 12
БЛОК 13
БЛОК 14
БЛОК 15
ПОКУПАЮ ЗА 5 BTC
ОК, ДЕРЖИ
???
ТЕПЕРЬ НУЖНО «ВСЕГО-ЛИШЬ» СГЕНЕРИРОВАТЬ БОЛЕЕ ДЛИННУЮ ЦЕПОЧКУ, В КОТОРОЙ НЕ БУДЕТ ЭТИХ 5 BTC

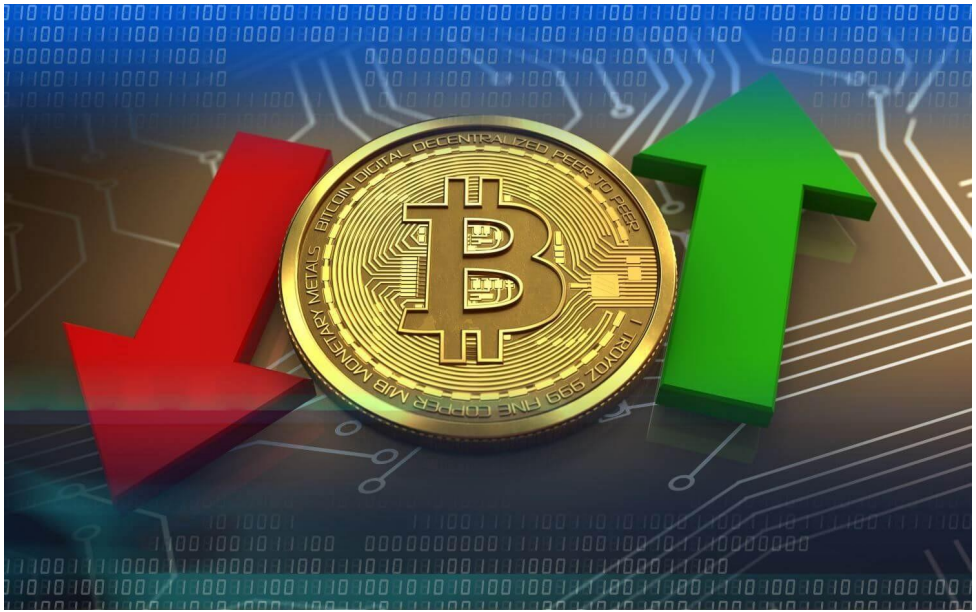
Атака «51%»

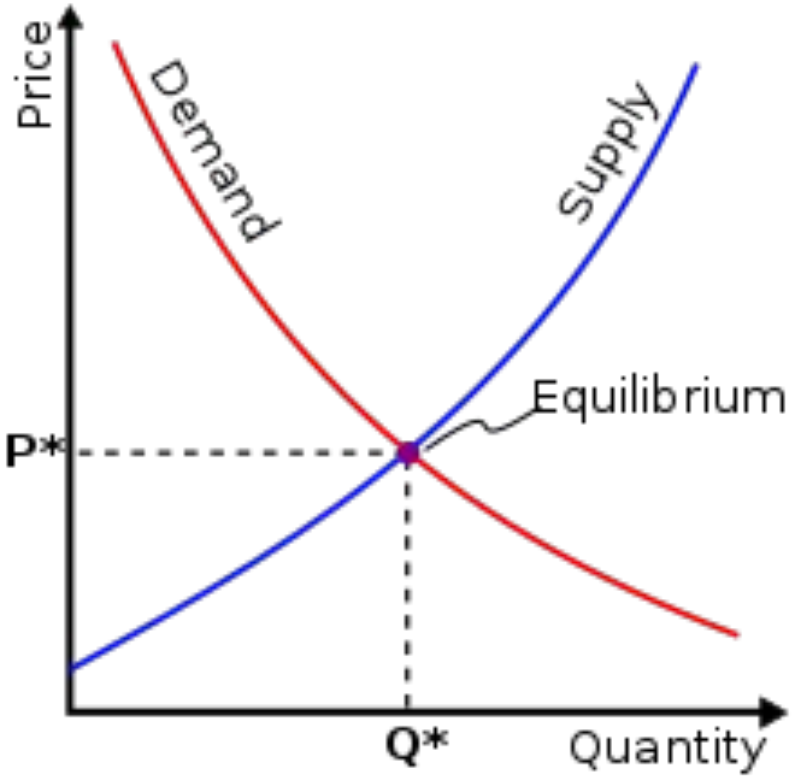

АКТУАЛЬНЫЙ БЛОКЧЕЙН
БЛОК 12
БЛОК 13
БЛОК 14
БЛОК 15
ЗЛОУМЫШЛЕННИК
С ОГРОМНОЙ ВЫЧИСЛИТЕЛЬНОЙ
МОЩНОСТЬЮ
ФЕЙК БЛОК 13
ФЕЙК БЛОК 14
ФЕЙК БЛОК 15
ФИНИШ
ТАК КАК БЛОКИ НЕЛЬЗЯ ПРОСЧИТАТЬ ЗАРАНЕЕ, ЗЛОУМЫШЛЕННИК
ВЫНУЖДЕН ВСТУПАТЬ В ГОНКУ ПРОТИВ МОЩНОСТИ ВСЕЙ СЕТИ

Курс **Bitcoin** за последний год

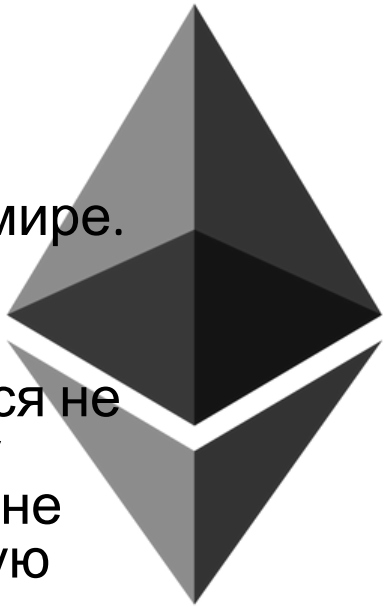


Закон спроса и предложения





Ethereum



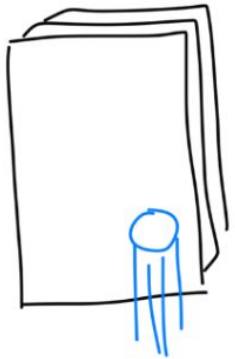
Ethereum — второй по популярности блокчейн-проект в мире.

Биткоин был точкой, с которой всё началось. Он оказался не просто системой денежных переводов, он показал миру новый способ организации сети, где гарантии завязаны не на посредников и «соглашения пользователя», а на голую математику.

Ethereum взял идею блокчейна за основу, и применил для решения более широкого класса задач. Гарантировать не только валидность денежных переводов, но и вообще любых условий и сделок. И даже автоматизировать создание таких условий.

Контракты

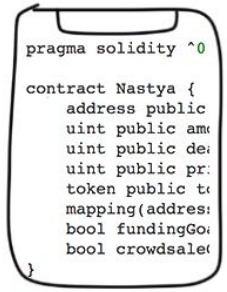
ТУПОЙ ДОГОВОР



- ДУШНАЯ БУМАЖКА С ПЕЧАТЬЮ
- НЕ ДАЁТ НИКАКИХ ГАРАНТИЙ
- УБИВАЕТ ДЕРЕВЬЯ
- ТРЕБУЕТ 50 ЮРИСТОВ

НЕ ТВОЙ БРО

УМНЫЙ КОНТРАКТ



- ПРЕКРАСНЫЙ КОД
- ПОДТВЕРЖДЕН МАТЕМАТИКОЙ
- Я ПРОГРАММИСТ, МЕНЯ НЕОБМАНЕШЬ
- ЛЮБОЙ МОЖЕТ НАПИСАТЬ СВОЙ

ТВОЙ БРО

Смарт-контракт

1. СОЗДАЁМ НЕЗАВИСИМОЕ ХРАНИЛИЩЕ, КУДА КАЖДЫЙ МОЖЕТ ПОЛОЖИТЬ, НО НЕ МОЖЕТ ВЗЯТЬ

2. ОЛЕГ КЛАДЁТ В ЭТО ХРАНИЛИЩЕ ДЕНЬГИ ЗА АРЕНДУ

3. НАСТЯ КЛАДЁТ ТУДА КОД ОТ ДВЕРИ СВОЕЙ КВАРТИРЫ

4. ОЛЕГУ ВЫСЫЛАЕТСЯ ЭТОТ КОД, НАСТЕ – ПОДТВЕРЖДЕНИЕ АРЕНДЫ НА ВЫБРАННЫЕ ДАТЫ

Смарт-контракт

5. ЕСЛИ ОЛЕГ ПРИЕЗЖАЕТ И ВВОДИТ КОД, НАСТЕ ПЕРЕЧИСЛЯЕТСЯ СУММА ПРЕДОПЛАТЫ

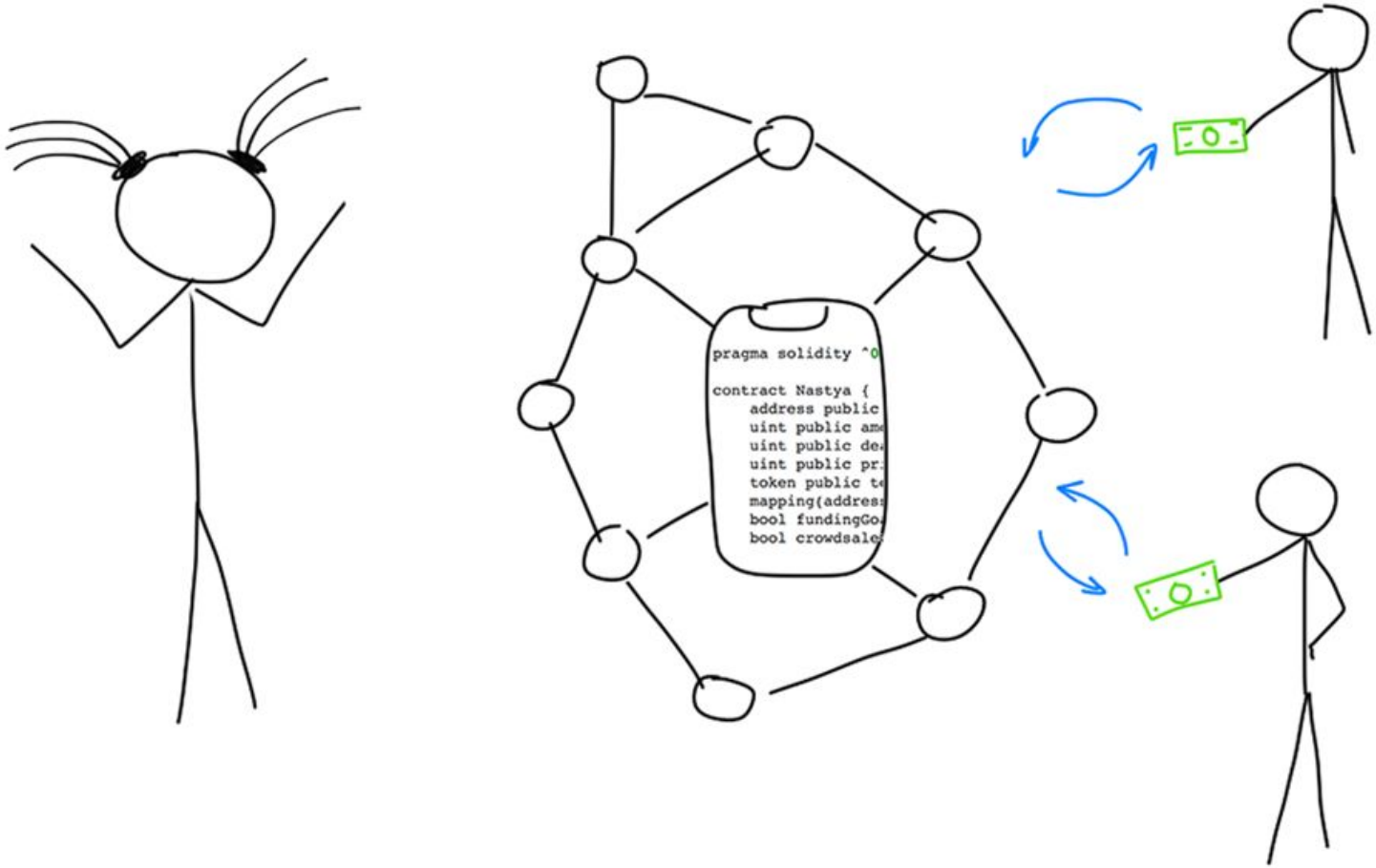
6. ЕСЛИ КОД НЕ ПОДХОДИТ, ОЛЕГУ ВОЗВРАЩАЕТСЯ ВСЯ СУММА И КОНТРАКТ АННУЛИРУЕТСЯ

7. ЕСЛИ ОЛЕГ НЕ ПРИЕЗЖАЕТ, НАСТЕ ПЕРЕЧИСЛЯЕТСЯ СУММА НЕУСТОЙКИ, А ОЛЕГУ ВОЗВРАЩАЕТСЯ ОСТАТОК

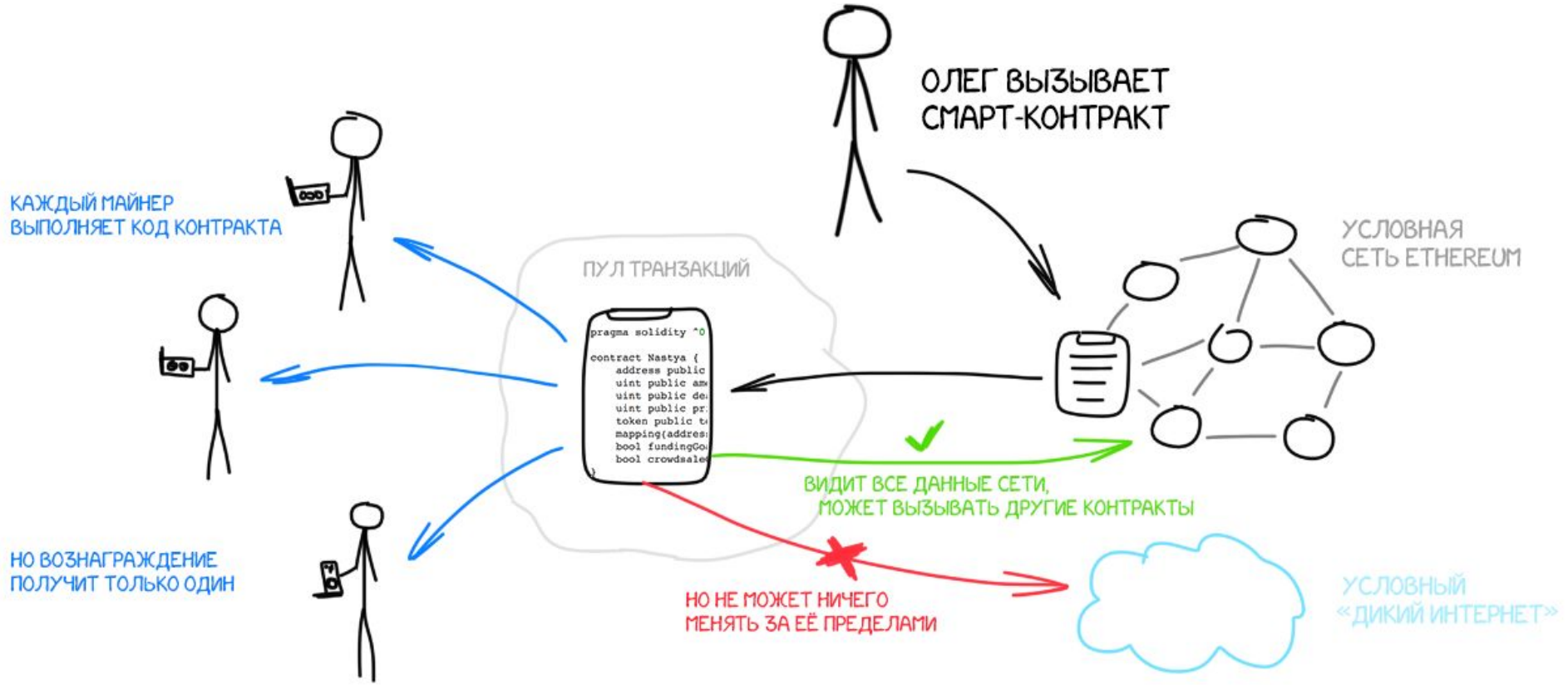
8. ЕСЛИ ВСЁ ХОРОШО, ТО ПО ОКОНЧАНИЮ СРОКА АРЕНДЫ НАСТЕ ПЕРЕЧИСЛЯЕТСЯ ОСТАТОК СУММЫ

9. ХРАНИЛИЩЕ УНИЧТОЖАЕТСЯ, КОНТРАКТ СЧИТАЕТСЯ ИСПОЛНЕННЫМ

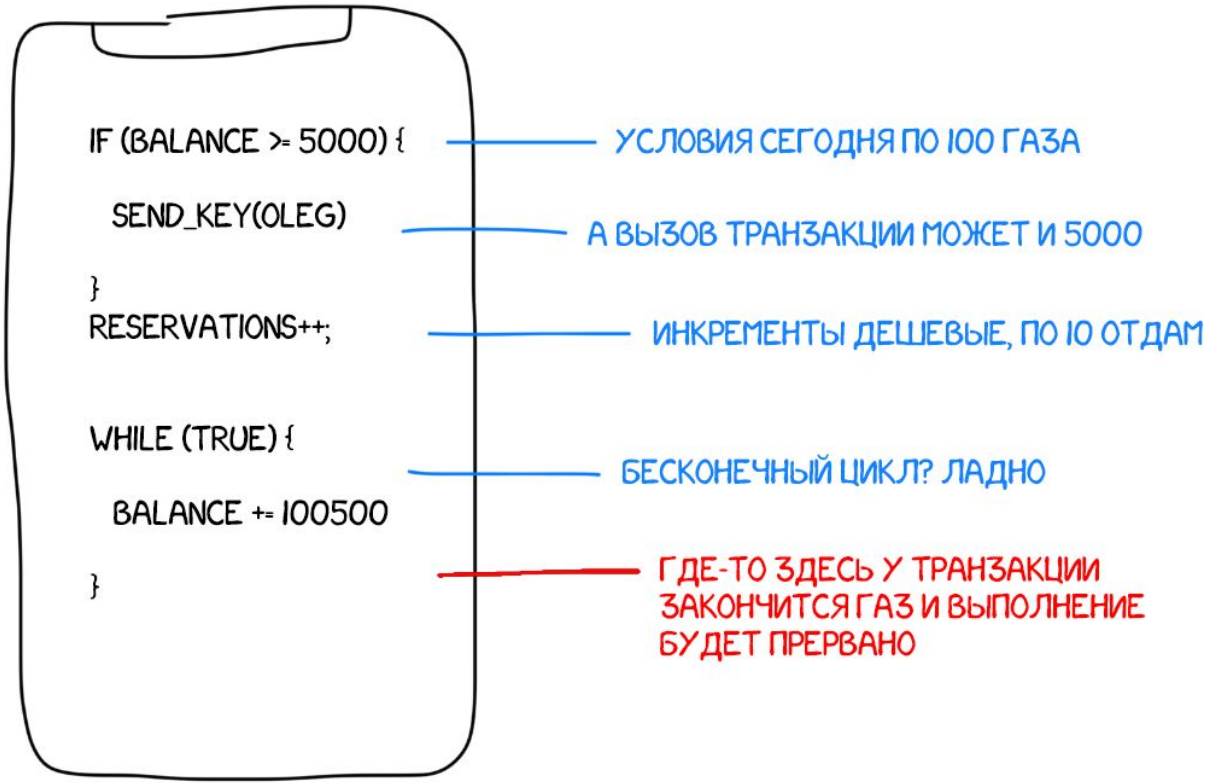
Смарт-контракты



Блокчейн сеть со смарт-контрактами



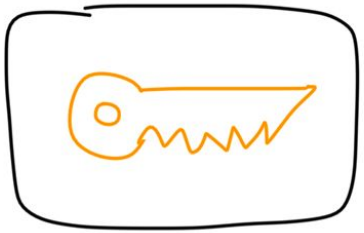
Газ



ГАЗ В ETHEREUM ОПЛАЧИВАЕТ ВЫЧИСЛЕНИЯ МАЙНЕРОВ И ЗАЩИЩАЕТ ОТ DDOS В КОДЕ

Адреса

КОШЕЛЬКИ

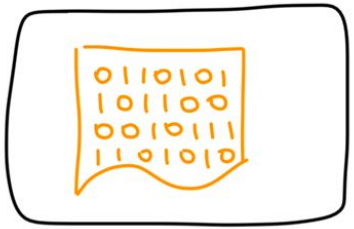


- УПРАВЛЯЮТСЯ ПРИВАТНЫМИ КЛЮЧАМИ

- МОГУТ СОЗДАВАТЬ ТРАНЗАКЦИИ

- МОГУТ ХРАНИТЬ КОИНЫ НА БАЛАНСЕ. РАСПОРЯЖАЕТСЯ ИМИ ВЛАДЕЛЕЦ АККАУНТА

КОНТРАКТЫ

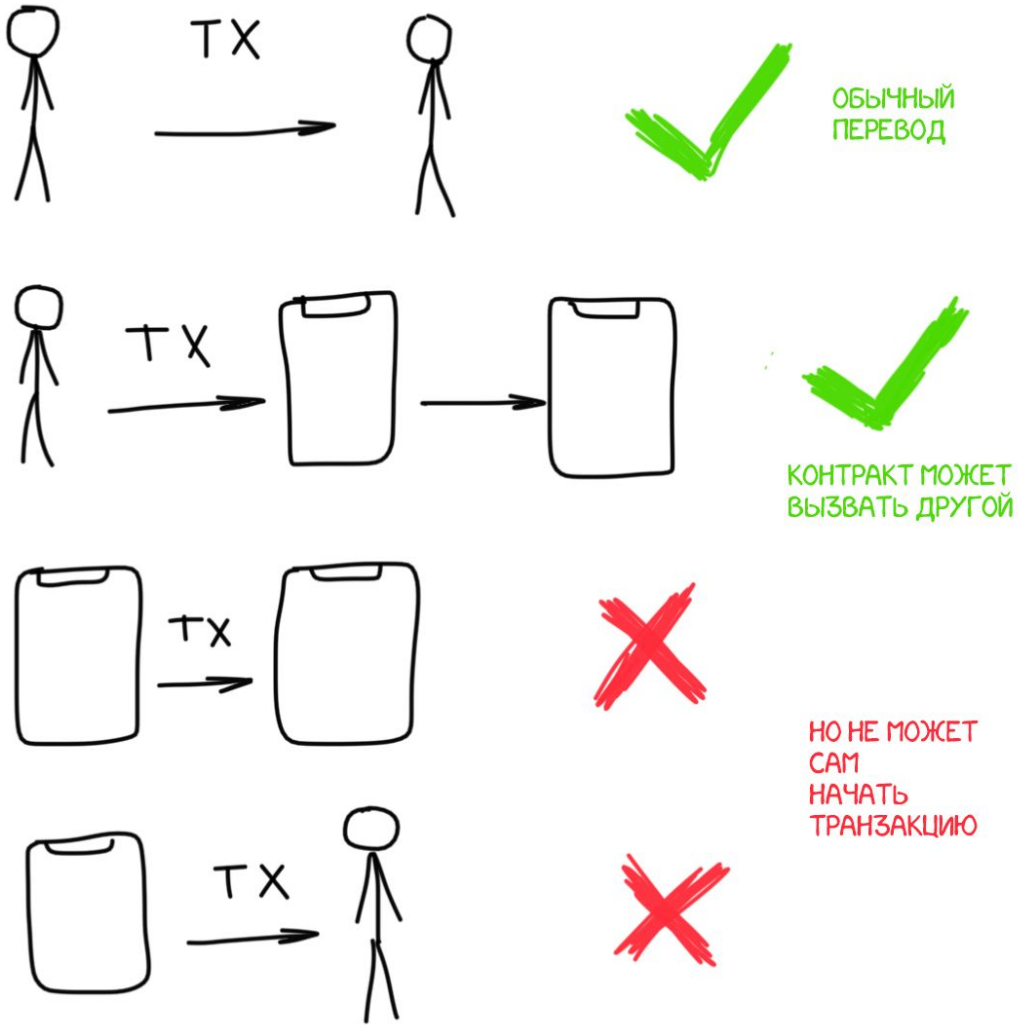


- УПРАВЛЯЮТСЯ СОБСТВЕННЫМ КОДОМ

- МОГУТ СОЗДАВАТЬ ТРАНЗАКЦИИ ТОЛЬКО В ОТВЕТ НА ВХОДЯЩИЕ ТРАНЗАКЦИИ

- ТОЖЕ МОГУТ ХРАНИТЬ КОИНЫ НА БАЛАНСЕ, НО РАСПОРЯЖАЮТСЯ ИМИ АЛГОРИТМ САМОГО КОНТРАКТА.

(ЕСЛИ СОЗДАТЕЛЬ ЗАЛОЖИЛ В КОД ВОЗМОЖНОСТЬ ИХ ВЫВОДА – ПОЖАЛУЙСТА, НО ВСЕ ЭТО УВИДЯТ)


TX
ОБЫЧНЫЙ ПЕРЕВОД
TX
КОНТРАКТ МОЖЕТ ВЫЗВАТЬ ДРУГОЙ
TX
НО НЕ МОЖЕТ САМ НАЧАТЬ ТРАНЗАКЦИЮ
TX

Транзакция

1. АДРЕС ПОЛУЧАТЕЛЯ

2. СУММА ПЕРЕСЫЛАЕМЫХ BTC

3. СПИСОК ИНПУТОВ НА ЭТУ СУММУ

   НАДО НАБРАТЬ ИЗ БЛОКЧЕЙНА ВХОДЯЩИХ ТРАНЗАКЦИЙ НА НУЖНУЮ СУММУ

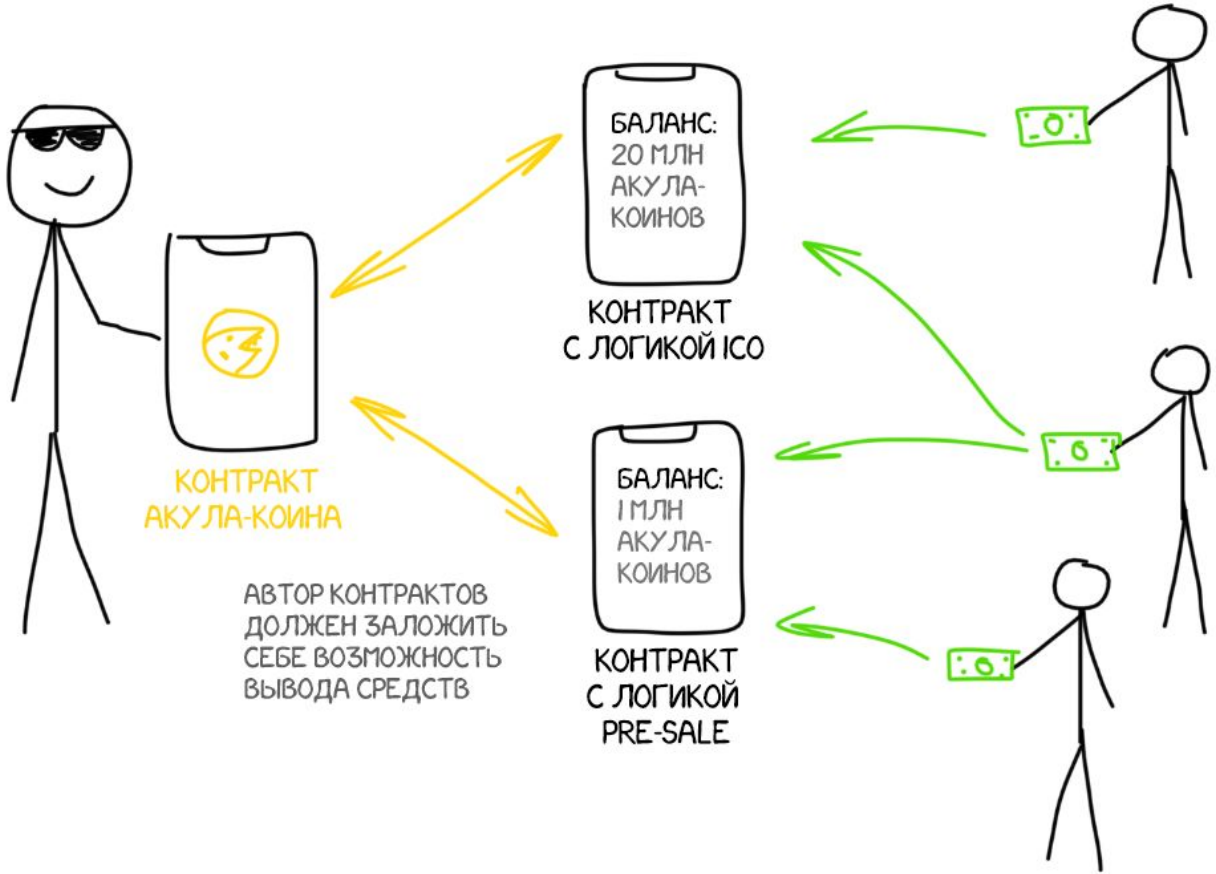
4. РАЗМЕР КОМИССИИ

   ВЫЧИТАЕТСЯ ИЗ СУММЫ ИНПУТОВ, ЛИШНЕЕ ВОЗВРАЩАЕТСЯ

5. ПУБЛИЧНЫЙ КЛЮЧ ДЛЯ ПРОВЕРКИ ПОДПИСИ

   НУЖЕН ЧТОБЫ УДОСТОВЕРИТЬСЯ, ЧТО ВЫ ДЕЙСТВИТЕЛЬНО АВТОР ТРАНЗАКЦИИ

ICO


БАЛАНС:
20 МЛН
АКУЛА-
КОИНОВ
КОНТРАКТ
С ЛОГИКОЙ ICO
КОНТРАКТ
АКУЛА-КОИНА
АВТОР КОНТРАКТОВ
ДОЛЖЕН ЗАЛОЖИТЬ
СЕБЕ ВОЗМОЖНОСТЬ
ВЫВОДА СРЕДСТВ
БАЛАНС:
1 МЛН
АКУЛА-
КОИНОВ
КОНТРАКТ
С ЛОГИКОЙ
PRE-SALE

Читаем подробнее:

https://vas3k.ru/blog/blockchain/

https://vas3k.ru/blog/ethereum/