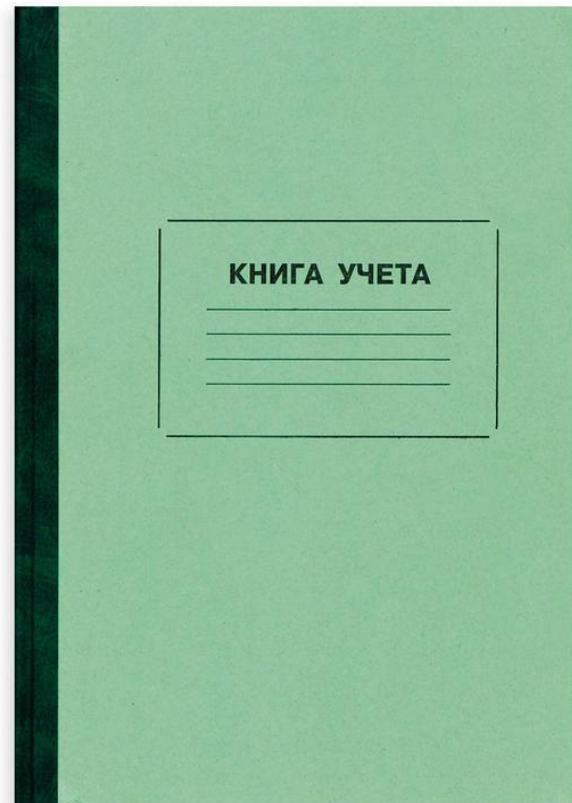


Blockchain for developers

Юрий Кашников
@kayuri

Занял Коле 1000 рублей
Занял Андрею 500 рублей
Коля вернул 500 рублей
Андрей вернул 500
Коля вернул 400 рублей

Колян, где сотэл?



Занял Коле 1000 рублей

-> 58b29ee7f...

Занял Андрею 500 рублей

-> b0ed73325...

Коля вернул 500 рублей

-> da1433e1ec...

Андрей вернул 500

-> b936e34cf...

Коля вернул 400 рублей

-> 27f49573...

Занял Коле 1000 рублей -> 58b29ee7f...

Занял Андрею 500 рублей + 58b29 -> d037...

Коля вернул 500 рублей + d037 -> 1994aae...

Занял Коле 1000 рублей + **X** -> 0...000af

Занял Андрею 500 рублей + 58b29... + **X** -> 0...005c

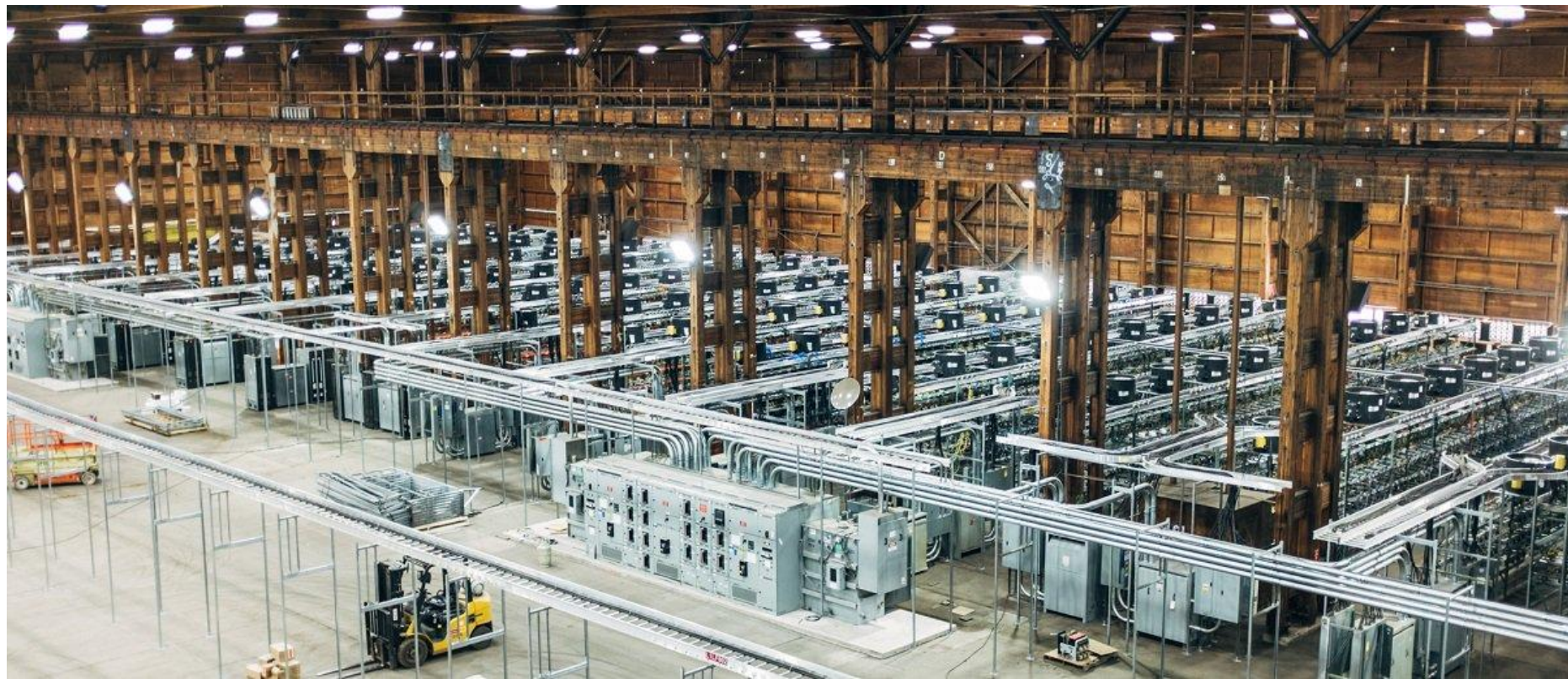
Коля вернул 500 рублей + d037... + **X** -> 0...00be

Решение уравнение **X** (nonce)

Например, хэш с 10 нулями

Только полный перебор

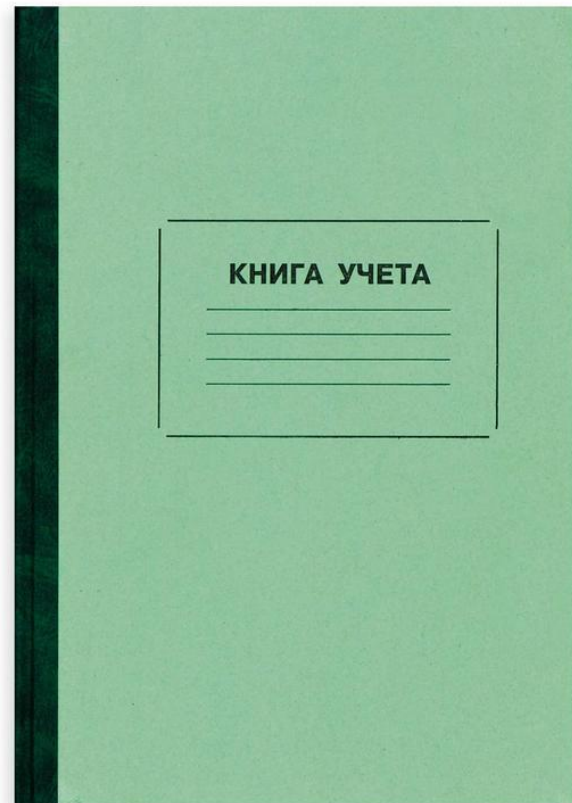
GPU/ASIC



Связный список

Открытый

Бухгалтерская книга (ledger)



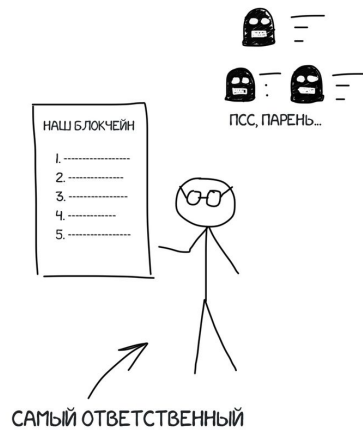
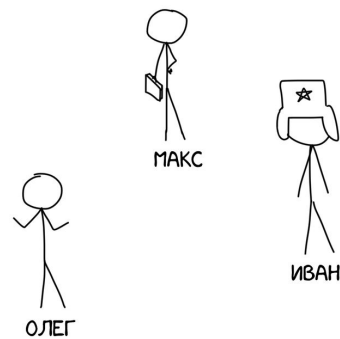


Рис. 1, любезно предоставлен vas3k.ru

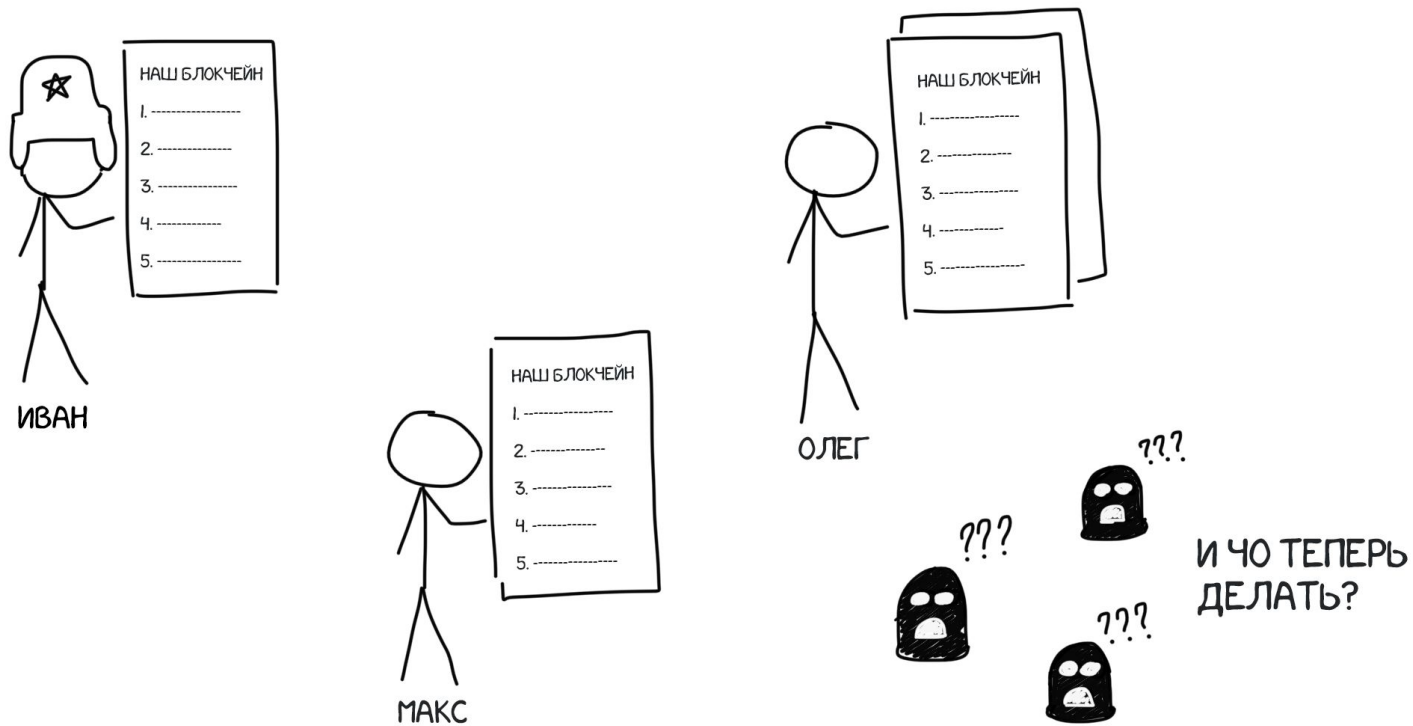


Рис. 2, любезно предоставлен vas3k.ru

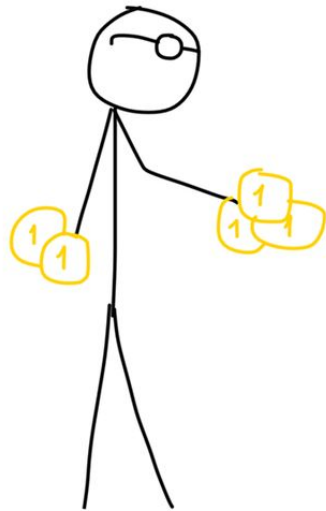
Децентрализация - никто никому не доверяет

У каждого своя копия списка

Публичный ключ - ваш крипто кошелёк

Нет баланса

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»

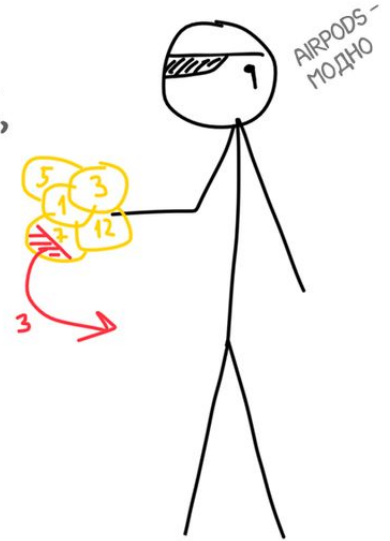


Рис. 3, любезно предоставлен vas3k.ru

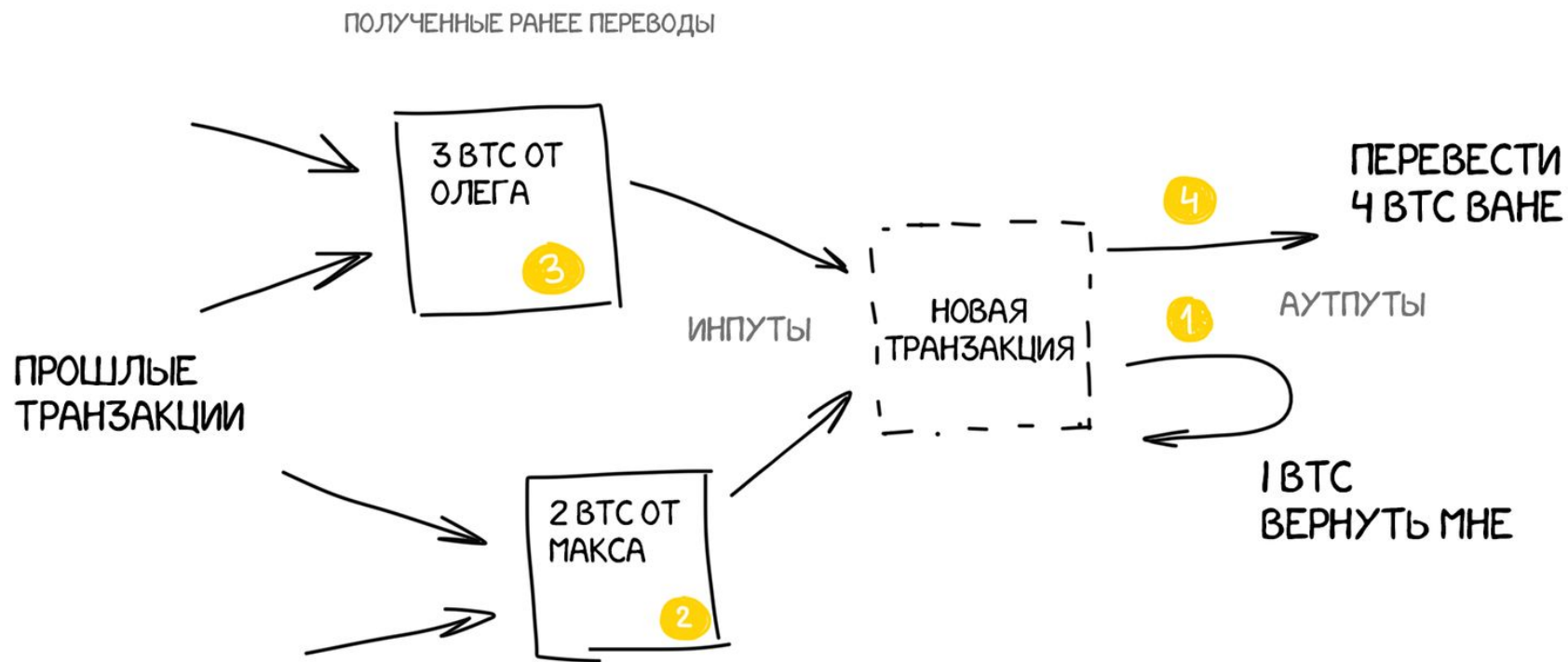


Рис. 4, любезно предоставлен vas3k.ru

Проблема двойной траты

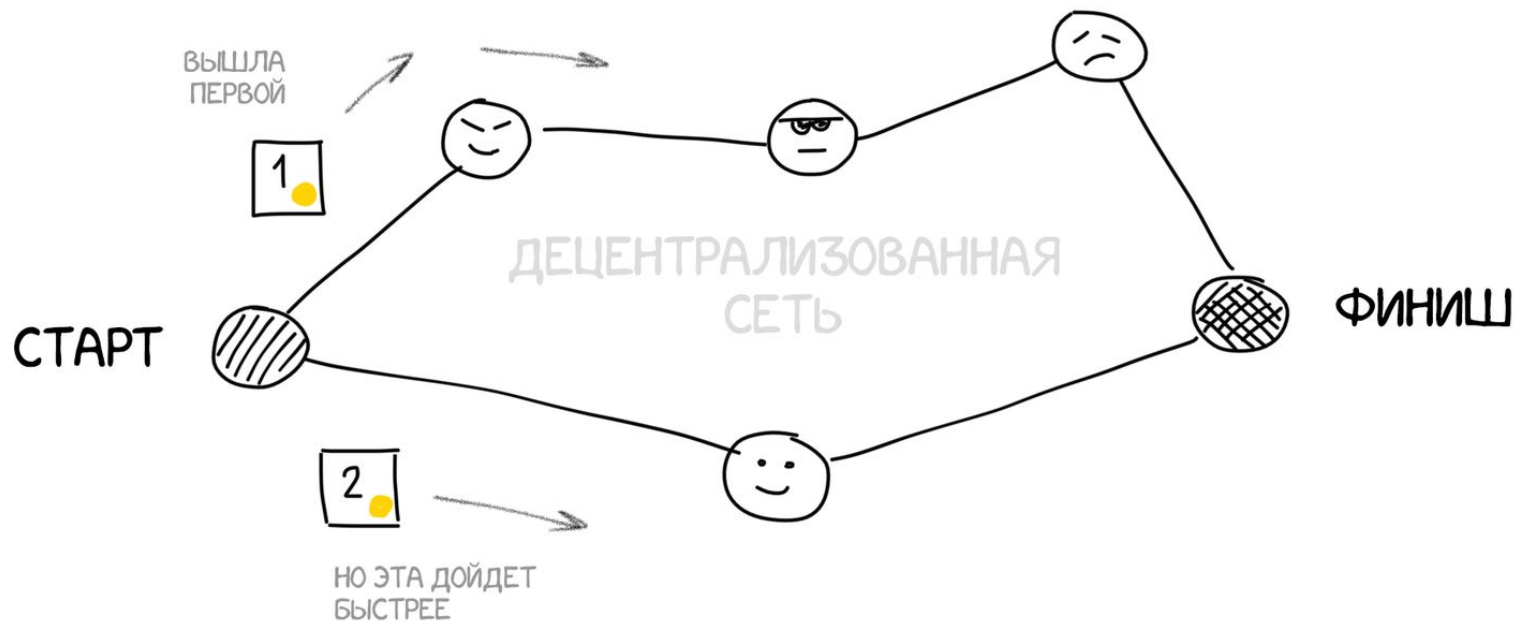
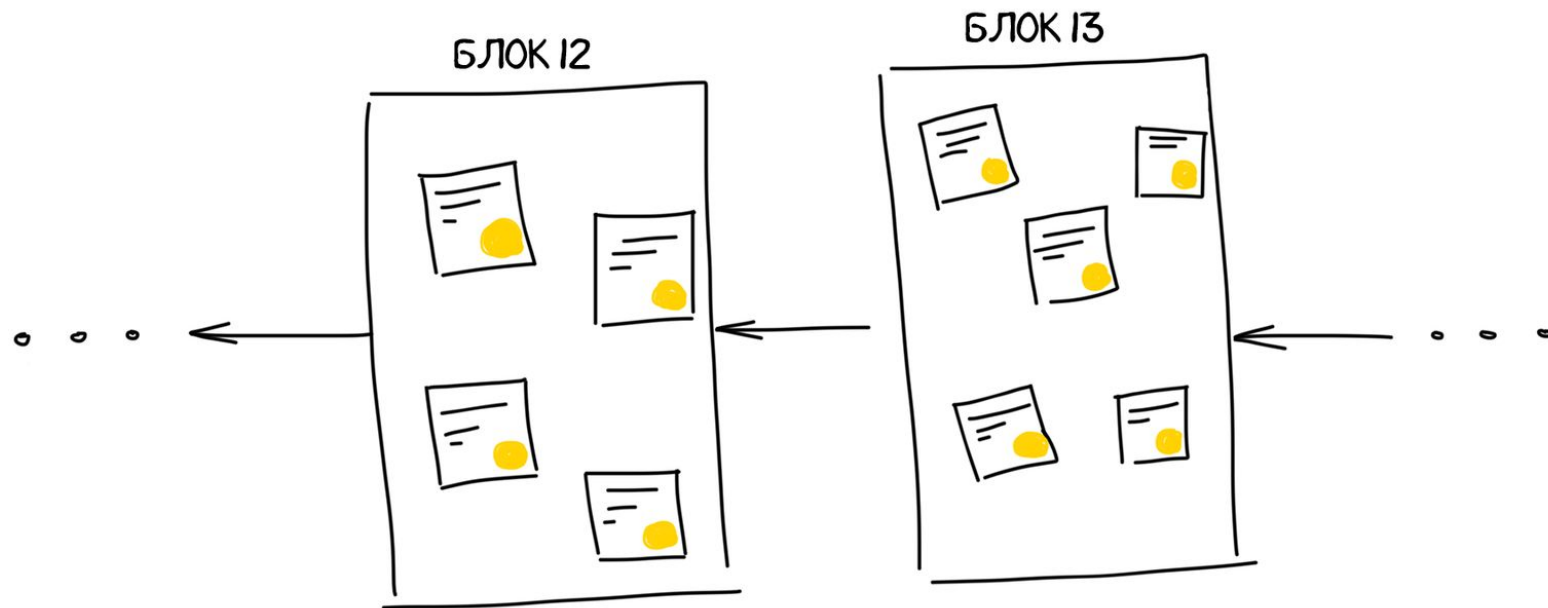


Рис. 5, любезно предоставлен vas3k.ru



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

Рис. 6, любезно предоставлен vas3k.ru

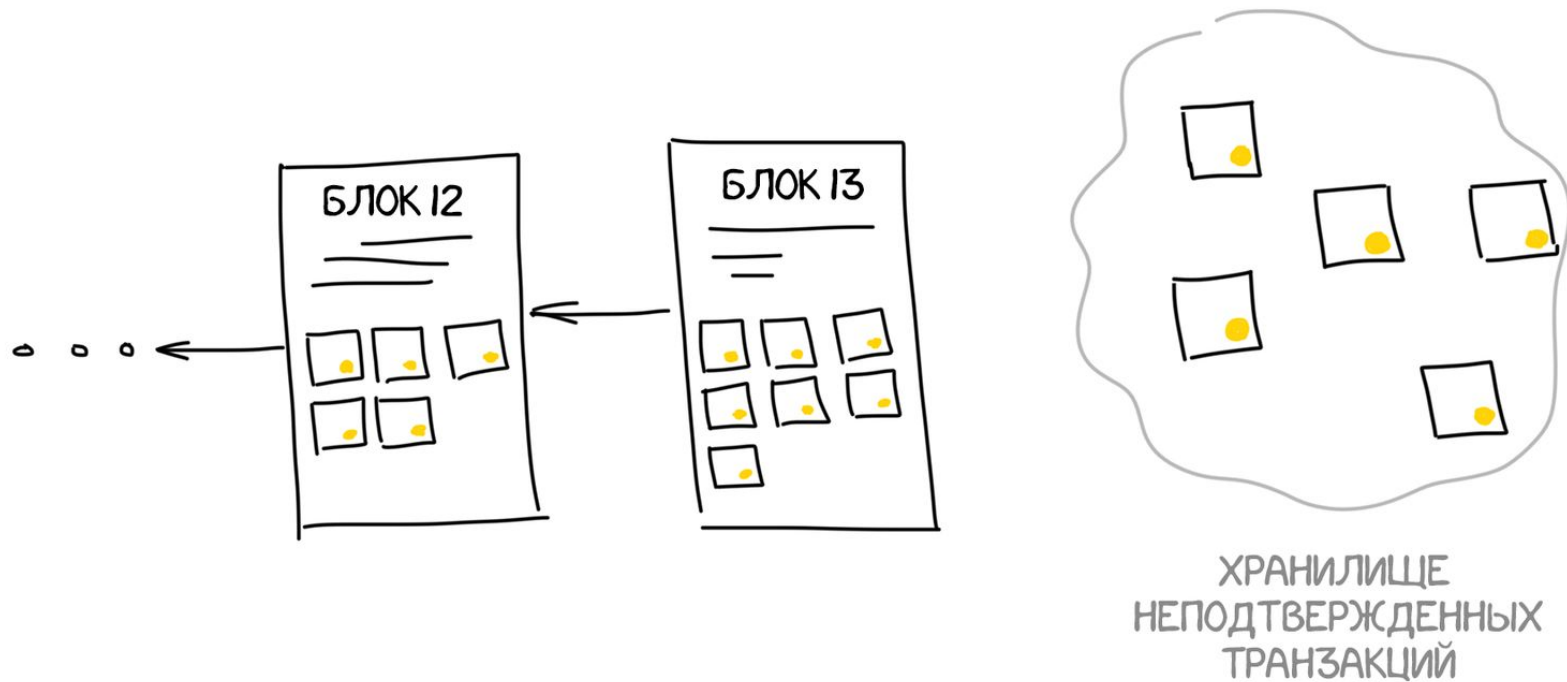


Рис. 6, любезно предоставлен vas3k.ru

ДВЕ ВЕТКИ РАЗДЕЛИВШЕГОСЯ БЛОКЧЕЙНА ЯВЛЯЮТСЯ ПРАВИЛЬНЫМИ.
ОДНИ КОМПЬЮТЕРЫ СЕТИ СЧИТАЮТ ПРАВИЛЬНОЙ ОДНУ,
ДРУГИЕ - ДРУГУЮ

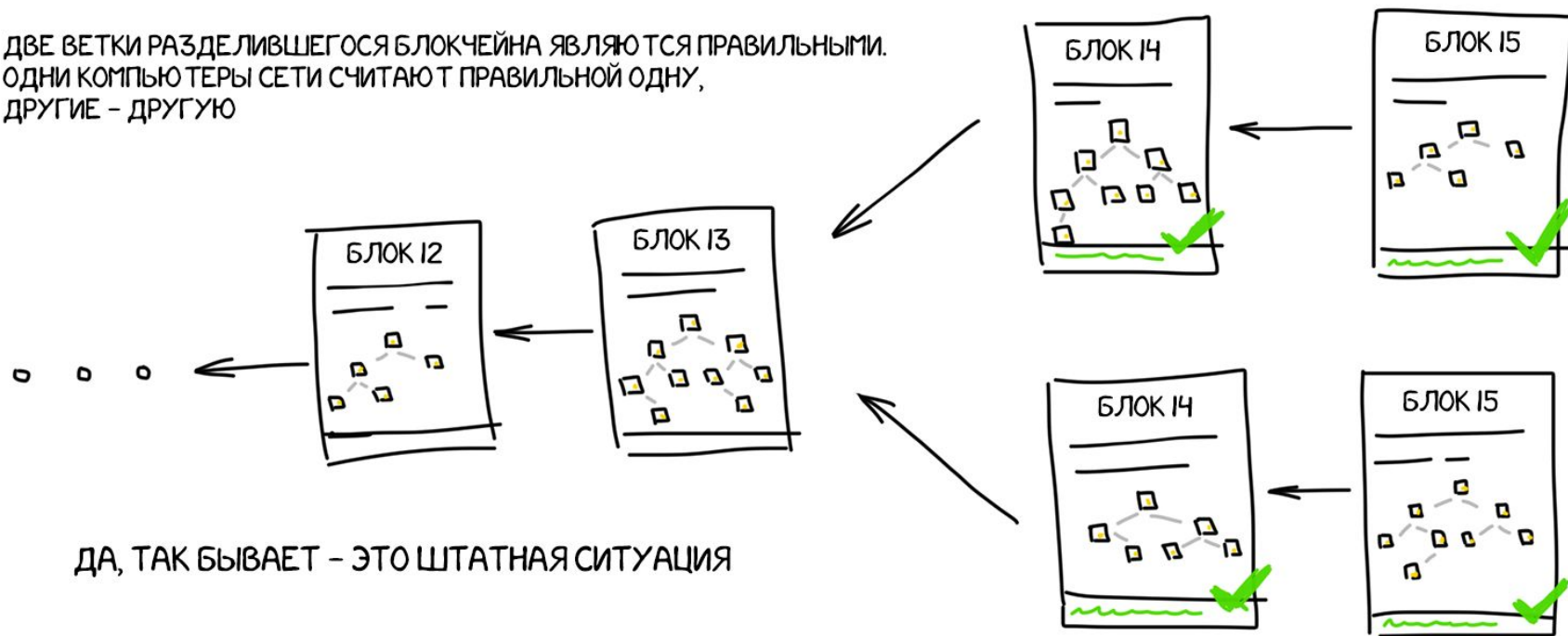
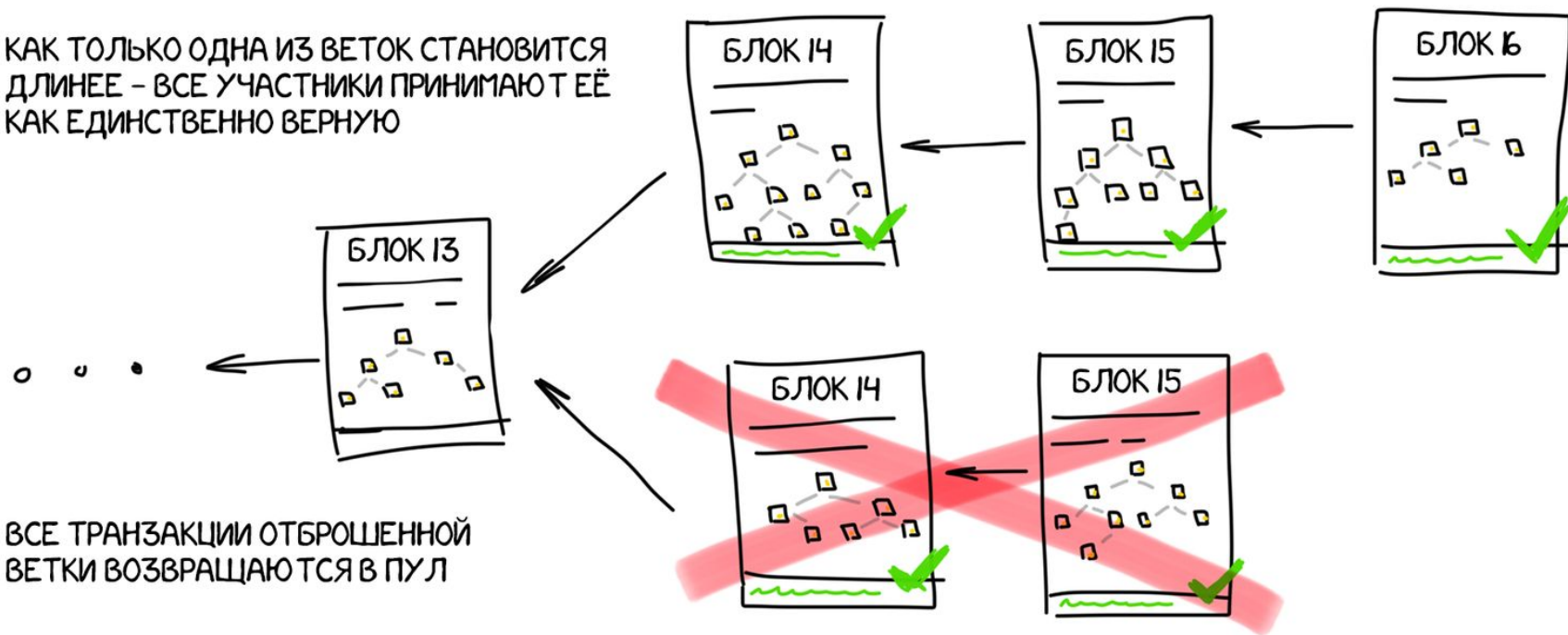


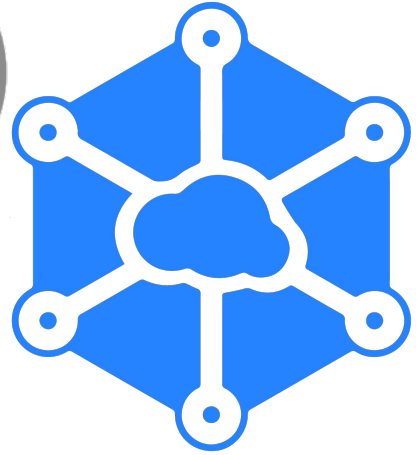
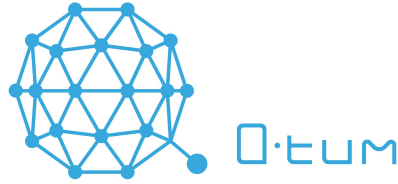
Рис. 7, любезно предоставлен vas3k.ru

КАК ТОЛЬКО ОДНА ИЗ ВЕТОК СТАНОВИТСЯ
ДЛИНЕЕ – ВСЕ УЧАСТНИКИ ПРИНИМАЮТ ЕЁ
КАК ЕДИНСТВЕННО ВЕРНУЮ



ВСЕ ТРАНЗАКЦИИ ОТБРОШЕННОЙ
ВЕТКИ ВОЗВРАЩАЮТСЯ В ПУЛ

Рис. 8, любезно предоставлен vas3k.ru



STORJ



Monero, ZCash, Dash - анонимность

Storj - блокчейн AWS

Augur - рынок предсказаний

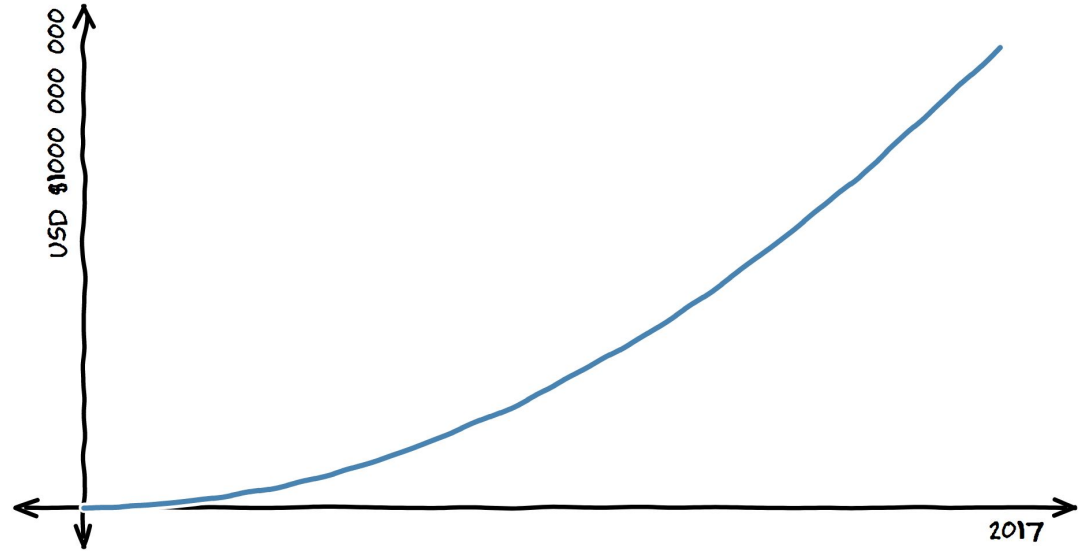
Litecoin, Waves, BCash - быстрее, выше, сильнее

INITIAL COIN OFFERING

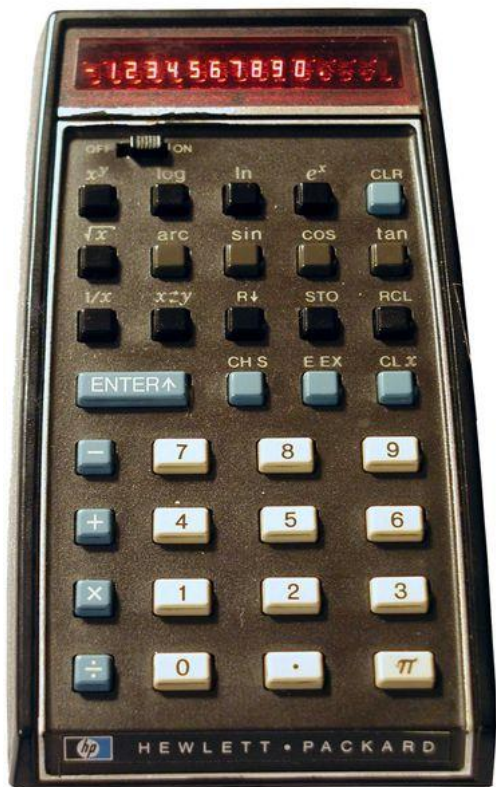
Mastercoin \$5 млн в 2013

Bancor \$150 млн в 2016

Block.one \$185 млн в 2017



Большинство блокчейнов выглядят примерно так:



В лучшем случае вот так:



А хотелось бы вот так:





ethereum



Ethereum

- Встроенный язык программирования
- Два типа аккаунтов:
 - Пользовательские (управляются приватными ключи)
 - Контракты (управляются кодом)
- Можно создавать любые приложения при помощи контрактов

Что умеют контракты?

Можно слать ETH

Читать/писать в storage

Вызывать другие контракты

Полнота по Тьюрингу

```
contract HelloWorld {  
    string msg;  
  
    function HelloWorld() {  
        Msg = "Hello, World!";  
    }  
  
    function foo () public returns (string) {  
        return msg;  
    }  
}
```

```
contract Bomberman {  
  
    function Halt () {  
        uint j = 0;  
        uint sum = 0;  
        for (i = 0; i < 10; j++) {  
            sum += 5;  
        }  
    }  
}
```

Gas

Тьюринг полный?

Проблема останова

За проезд
передаём!



Хотите свой токен и ICO? Пожалуйста!

```
contract ERC20 {  
    function totalSupply() constant returns (uint totalSupply);  
    function balanceOf(address _owner) constant returns (uint balance);  
    function transfer(address _to, uint _value) returns (bool success);  
    function transferFrom(address _from, address _to, uint _value) returns  
(bool success);  
    function approve(address _spender, uint _value) returns (bool success);  
    function allowance(address _owner, address _spender) constant returns  
(uint remaining);  
    event Transfer(address indexed _from, address indexed _to, uint _value);  
    event Approval(address indexed _owner, address indexed _spender, uint  
_value);  
}
```


CryptoKitties

Collectible.

Breedable.

Adorable.



CryptoKitties

Котик за 250 ETH (~\$113k)

\$1 000 000 за первые дни

Уронили сетку на пол



Collectible

Каждый котёнок уникален

Только один владелец

Можно продавать котят



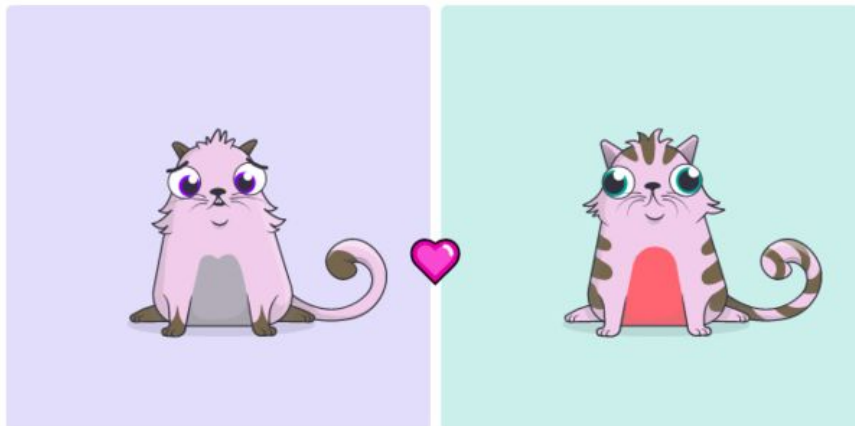
котёнок Ника Джонсона, деньги от продажи пошли
в благотворительный фонд worldbuilders.org

Breedable

Your two lovely Kitties will soon be
parents!

Kitty #285718 will lay an egg

Kitty #294088 will be the sire



Kitty 285718 · Gen 3

Swift

Kitty 294088 · Gen 4

Snappy

С точки зрения разработчика?

~ 2000 строк кода на Solidity

~ 1500 строк тестов на JS с Mocha и Chai

Новый стандарт ERC721 :)

Продуманная bounty program -> меньше багов

KittyAccessControl админка для CEO, CFO, COO

KittyBase базовые структуры данных и события

KittyOwnership управление “владением” котятами (ERC721)

KittyBreeding вязка котиков, предложения по вязки +ГеннаяИнженерия©

KittyAuctions покупка/продажа котиков (ну почти)

KittyMinting создание gen0 котиков

Полезное

1. [Bitcoin: A Peer-to-Peer Electronic Cash System](#)
2. [DEVCON1: Understanding the Ethereum Blockchain Protocol](#)
3. [Bounty program for CryptoKitties smart contract](#)
4. [Блокчейн изнутри: как устроен биткоин](#)
5. [Как устроен Ethereum и смарт-контракты](#)



Спасибо Вастрику!

vas3k.ru

kayuri.github.io/GDGNsk2017.pdf