

У вас найдется минутка, чтобы  
поговорить о блокчейне?

Гришечко Егор

CodeBeavers



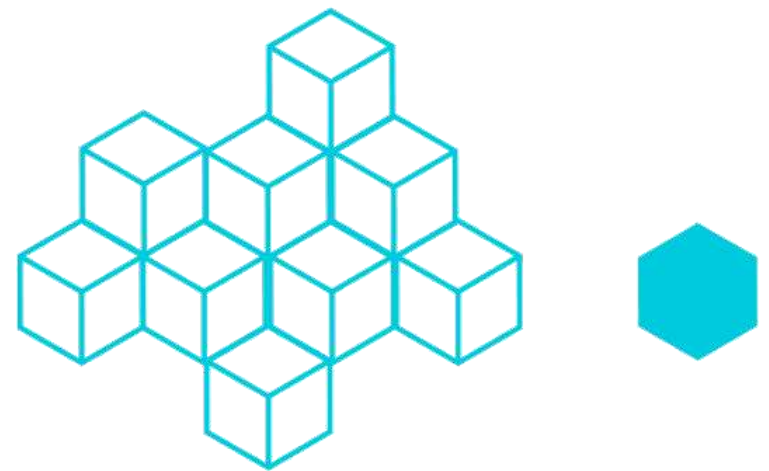
# Что такое блокчейн

**Блокчейн** ([англ.](#) *blockchain* или *block chain*) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков ([связный список](#)), содержащих информацию. Чаще всего копии цепочек блоков хранятся и [независимо друг от друга \(чрезвычайно параллельно\)](#) обрабатываются на множестве разных компьютеров.

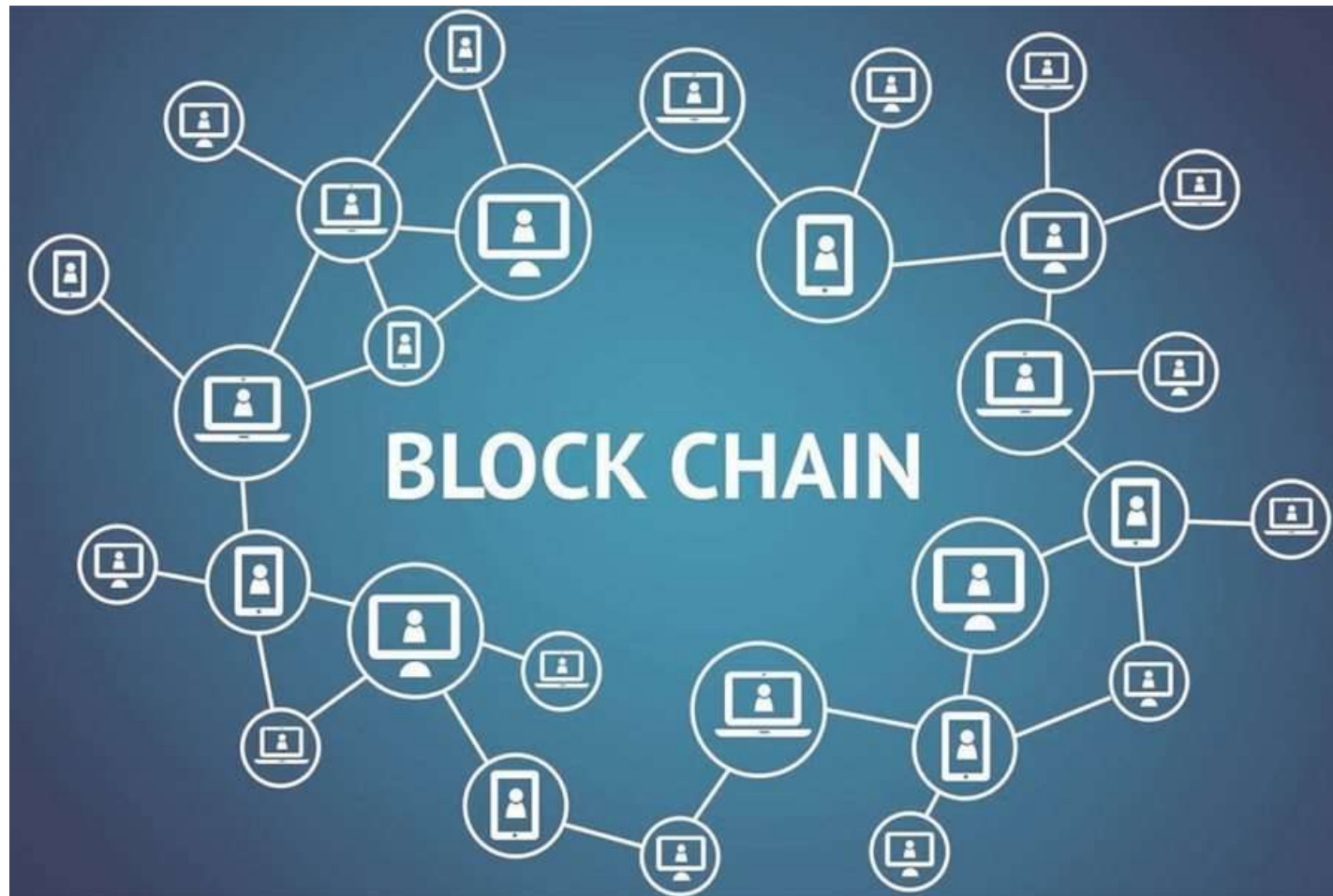


# Что такое блокчейн

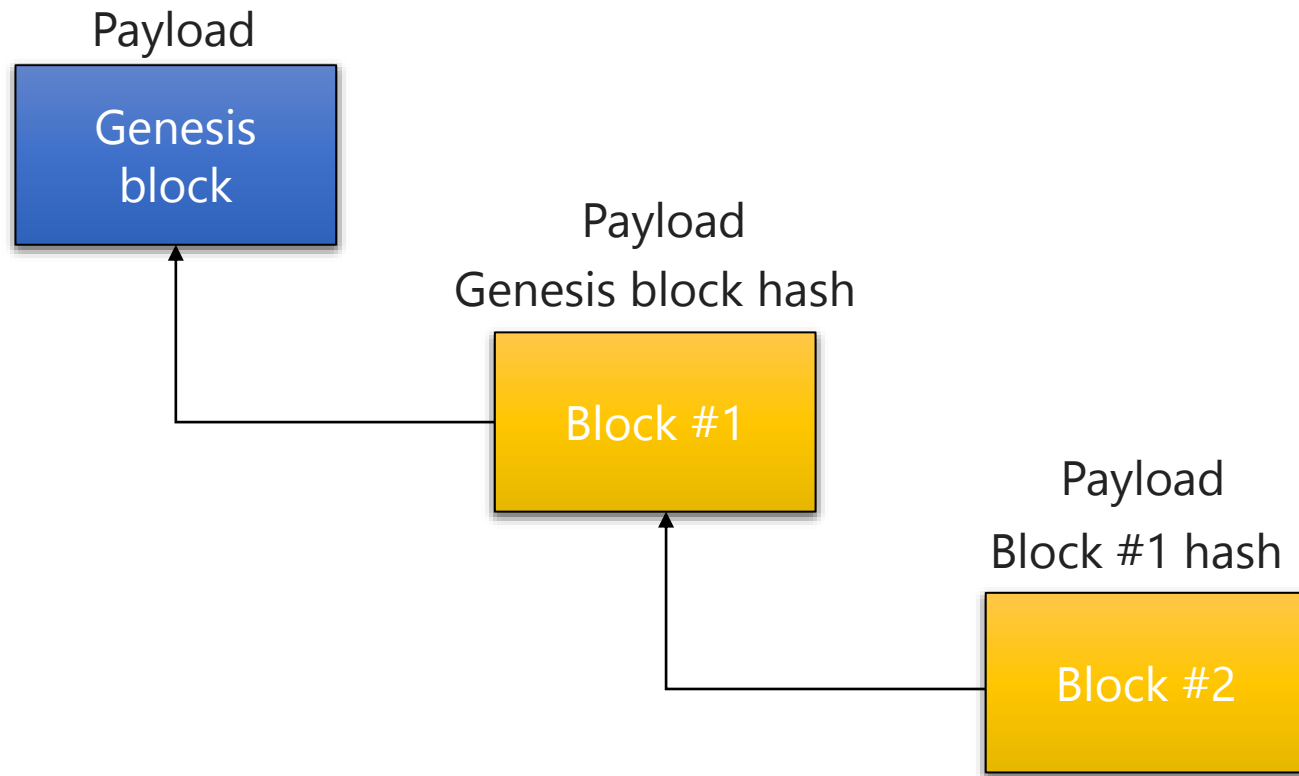
- Распределенная и децентрализованная (чаще всего) база данных
- Ведется всеми участниками сети (чаще всего)
- Для внесения данных необходим консенсус (чаще всего)
- Базовая единица хранения – блок
- Данные имутабельны



# Что такое блокчейн

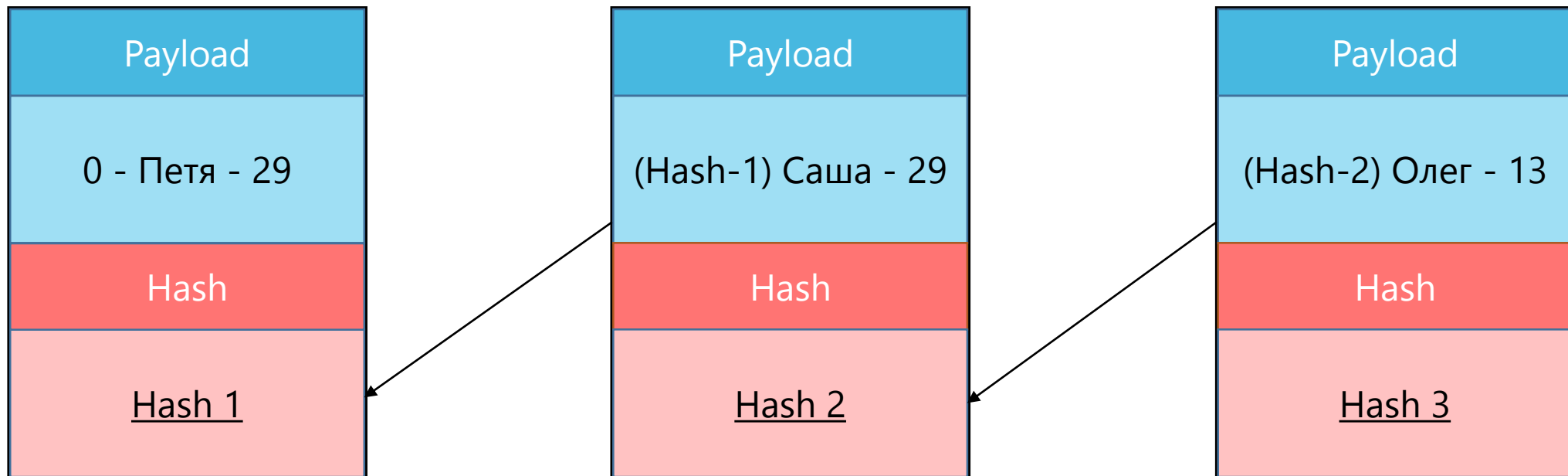


# Устройство блокчейна

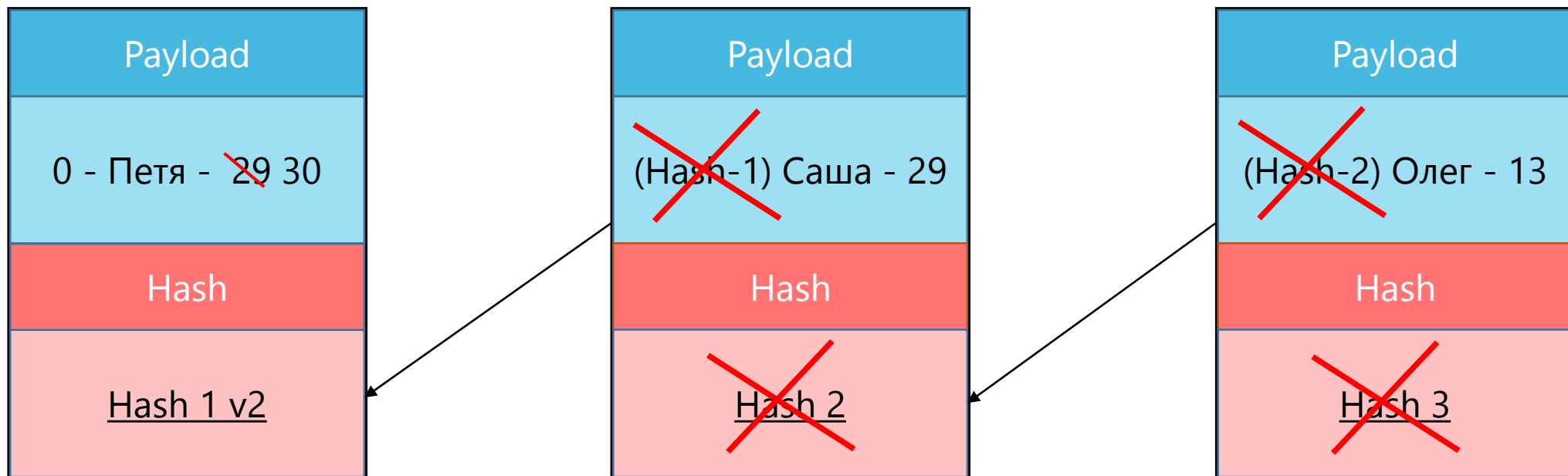


- Блоки связаны хэш указателями
- Блоки невозможно изменить
- Каждый участник сети хранит у себя **копию** всей информации

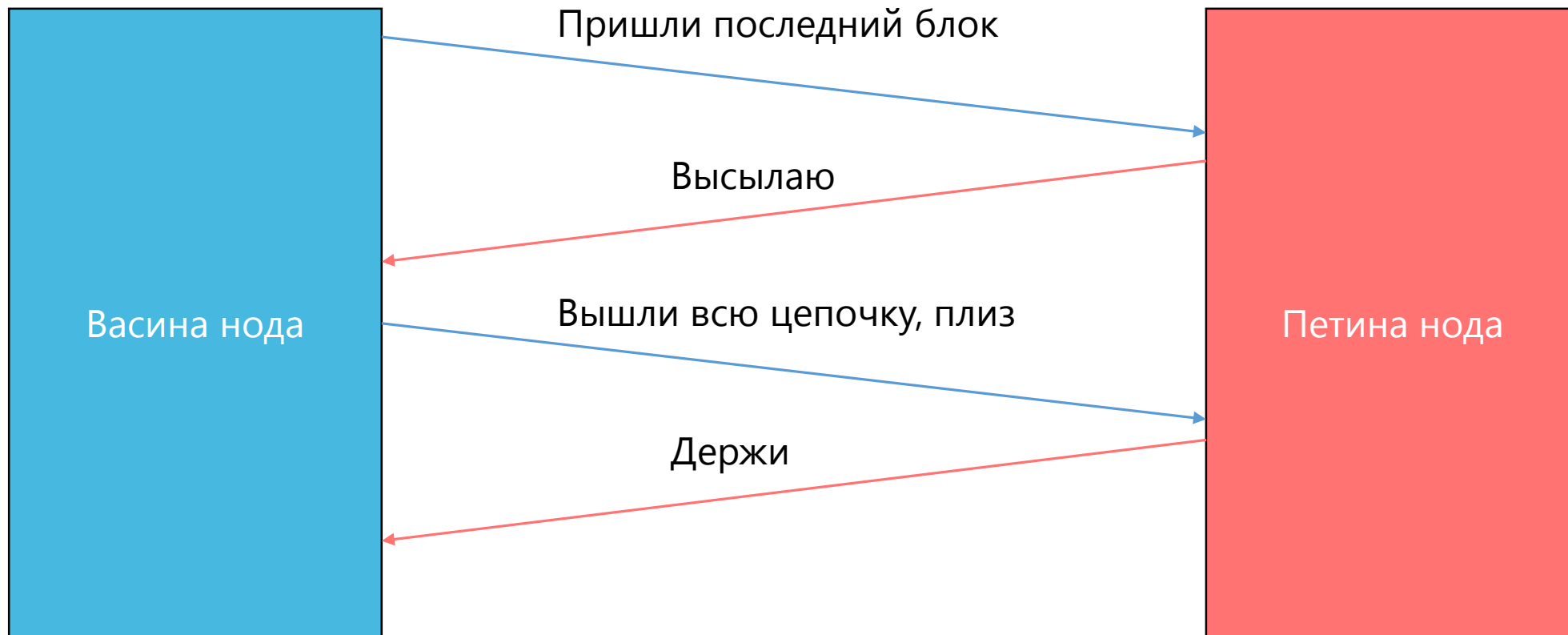
# Более наглядно



# Более наглядно

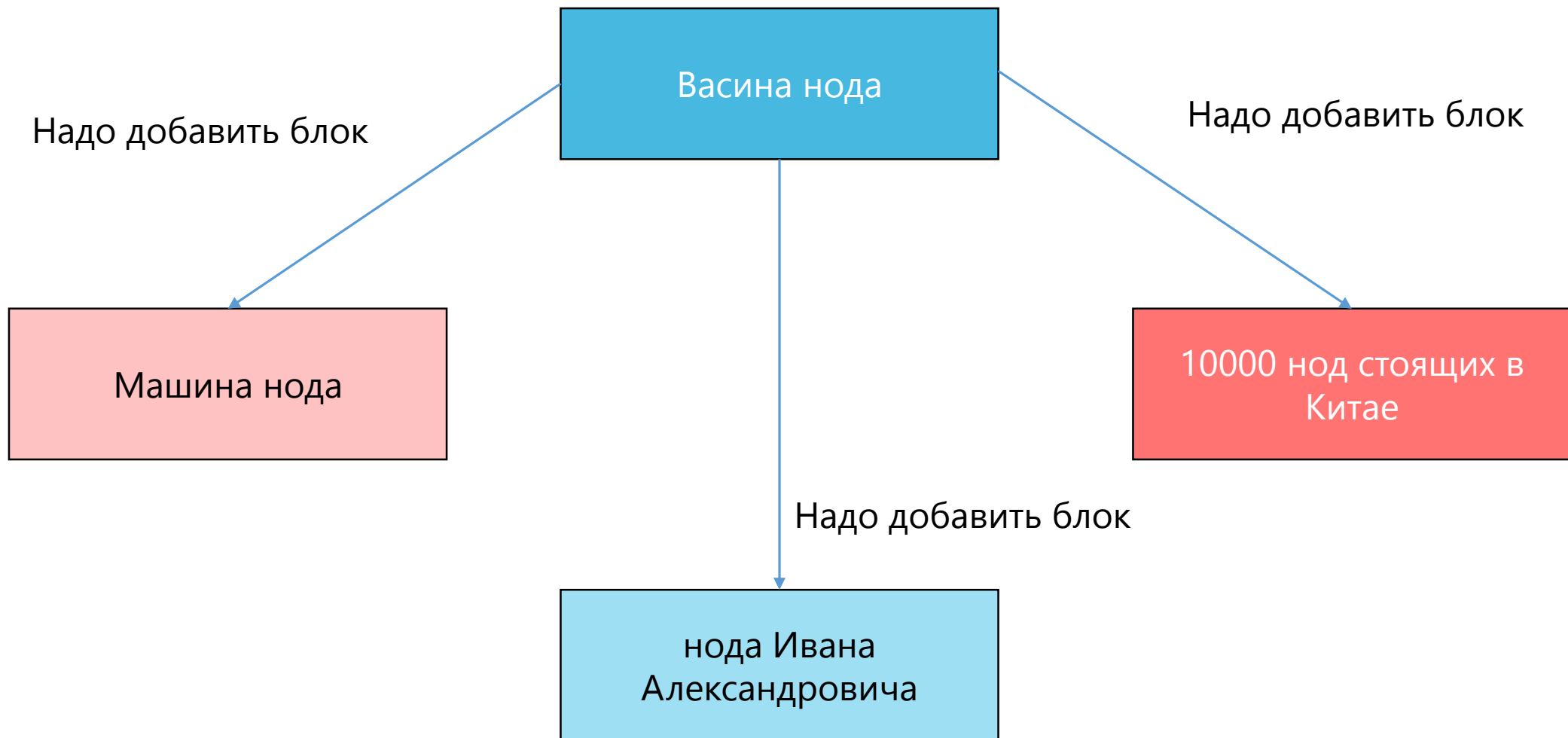


# Как это будет работать





# Как это будет работать

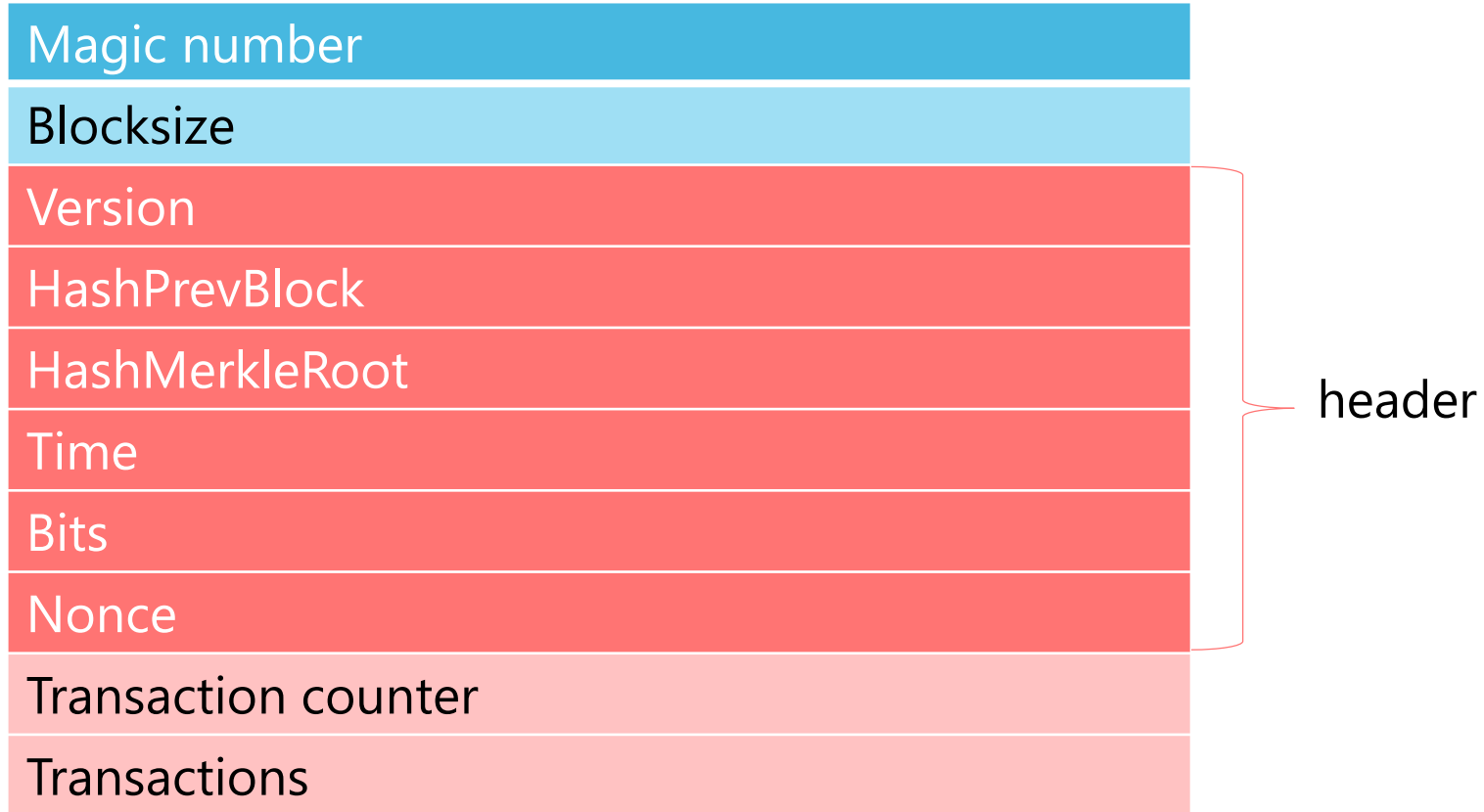


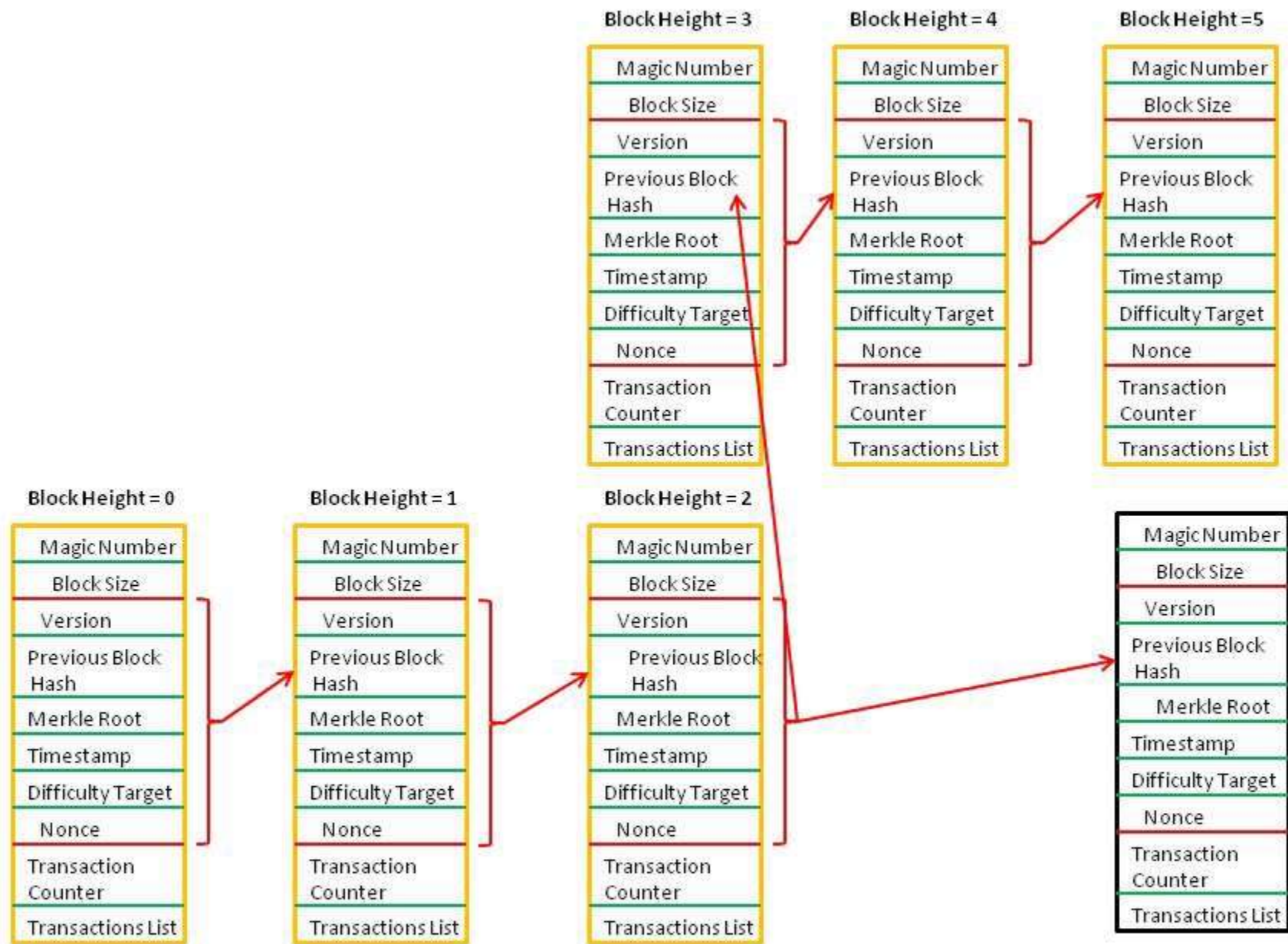


# Bitcoin



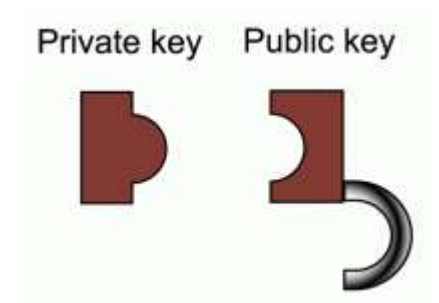
# Bitcoin



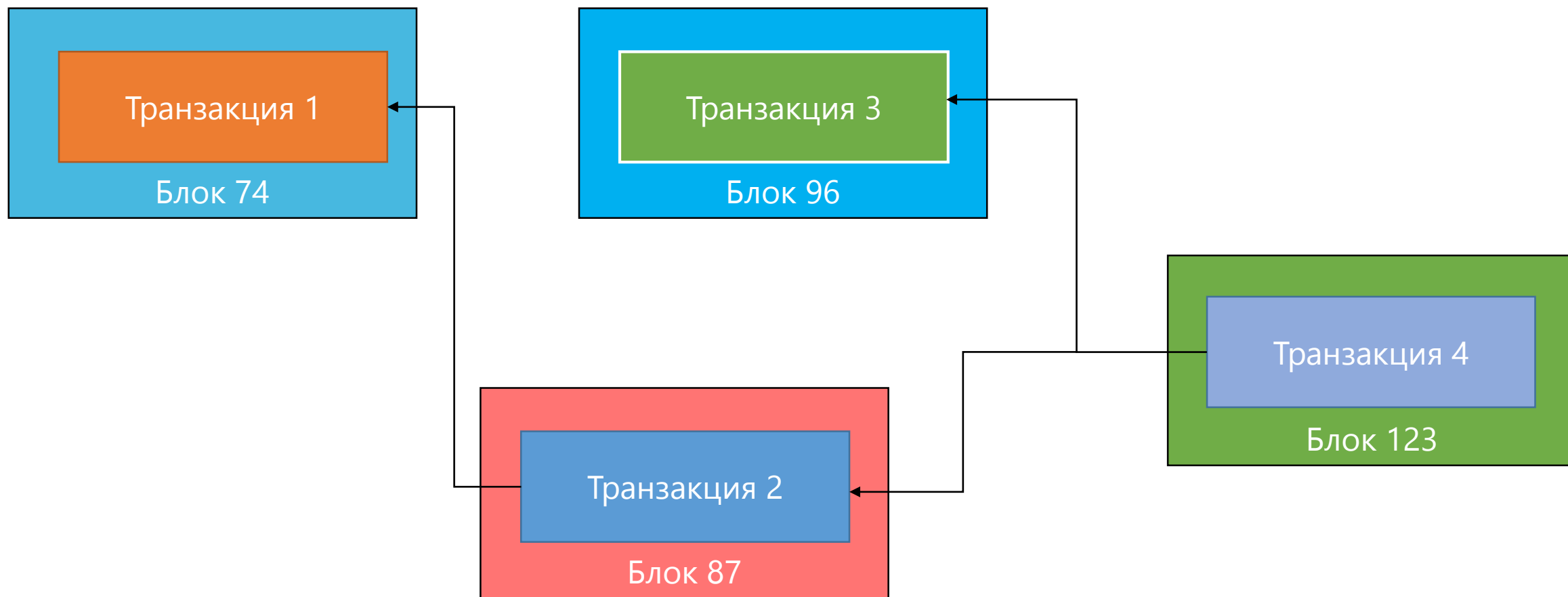


# Что находится в транзакции?

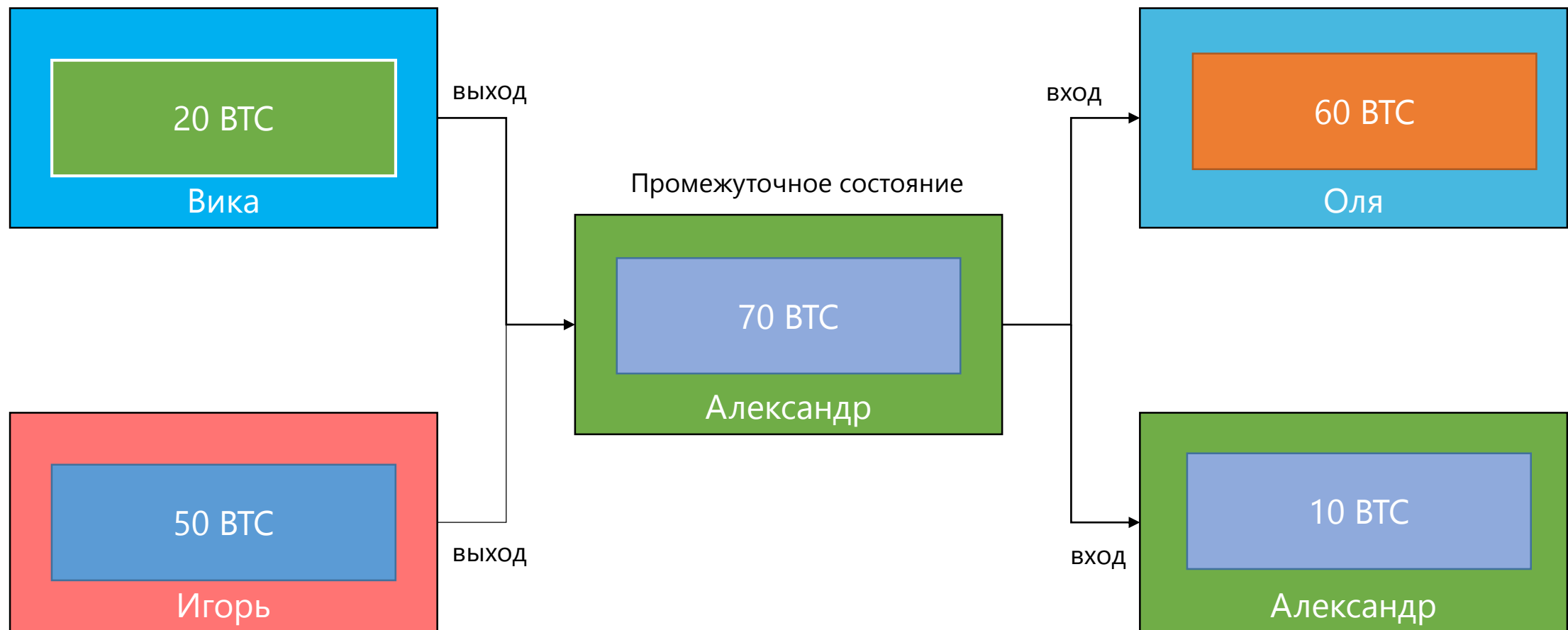
- Цифровая подпись (инициатор подтверждает актуальность)
- Адрес получателя (публичный ключ)
- Информация
- Ссылка на предыдущие транзакции



# Связь транзакций



# Входы и выходы





# Проблемы

- Кто и когда добавляет блоки?
- Что делать, когда возникли конфликты?
- Какие могут быть конфликты?
- Как валидировать блоки?



# Немножечко о майнинге

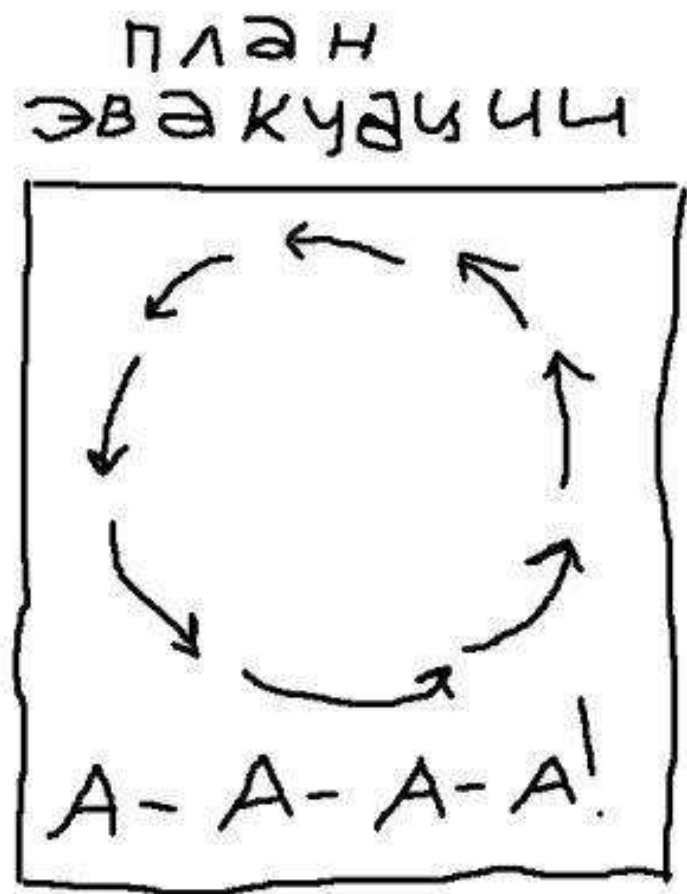


# Майнер

- Записывает транзакции
- Создает новые блоки
- Получает новые деньги от системы (которых раньше не было в сети)
- Тратит много энергии, очень много ☹



# Хаос

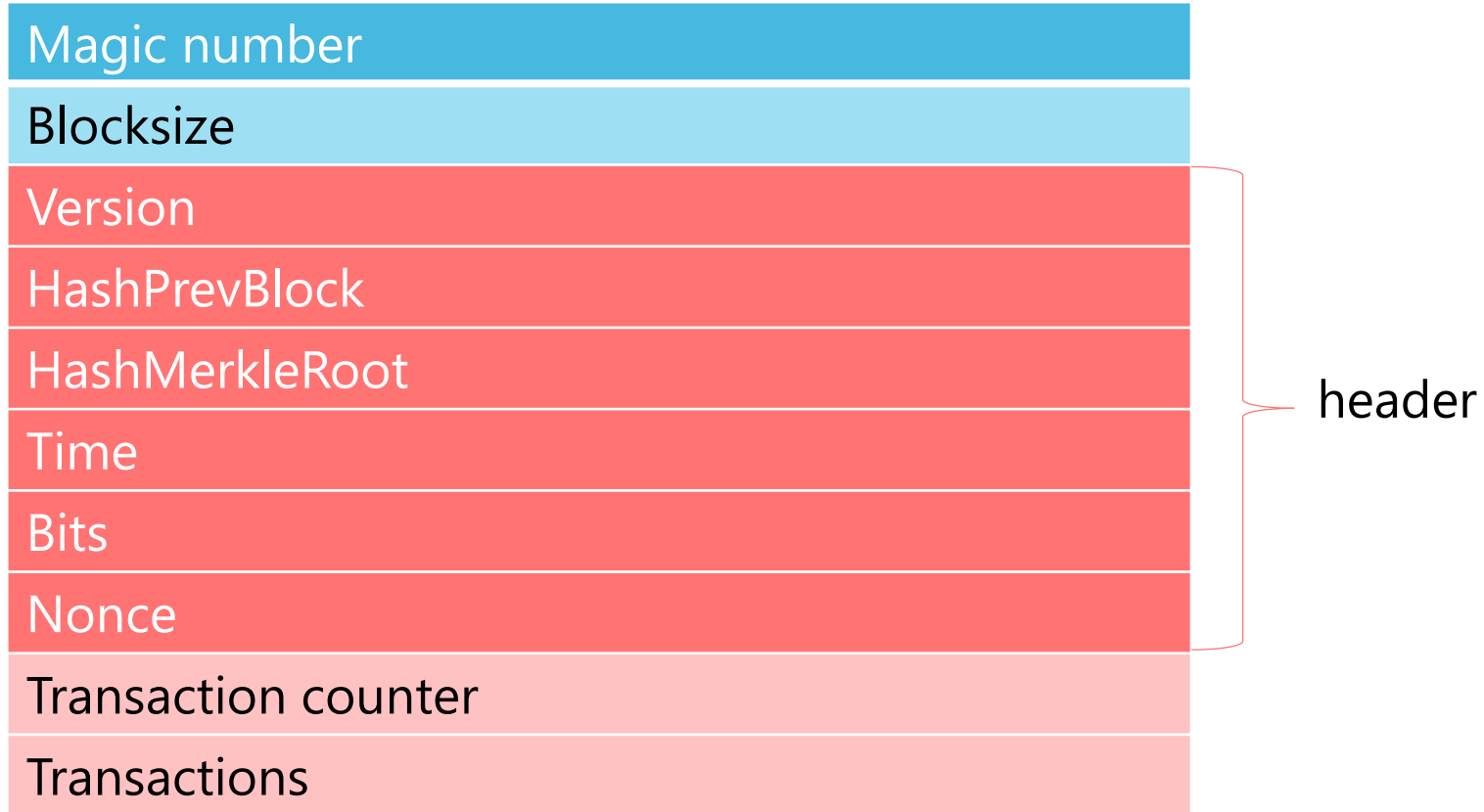


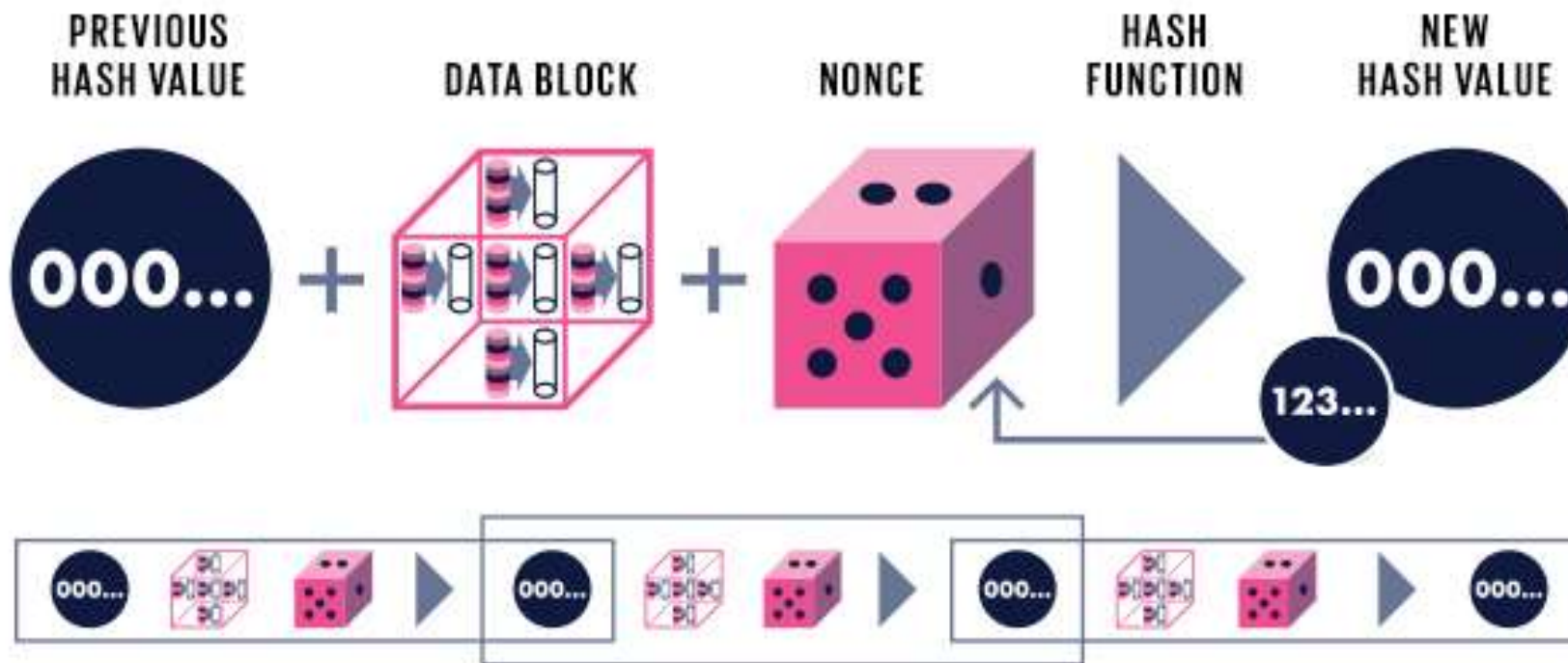
# Алгоритмы консенсуса

- PoW (Proof-of-Work)
- PoS (Proof-of-Stake)
- Proof of Activity
- Delegated Proof of Stake (DPoS)
- Proof of Burn
- Proof of Capacity
- Proof of Storage



# Bitcoin





<https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/>

<https://www.allcryptonews.com/algorithm-proof-of-work-pervoprohodets-i-rodonachalnik-progressivnogo-razvitiya-kriptovalyutnoj-industrii/>

# PoS (Proof-of-Stake)

## Proof-of-Work против Proof-of-Stake



Proof-of-Work требует дорогостоящих вычислений, также известных как майнинг

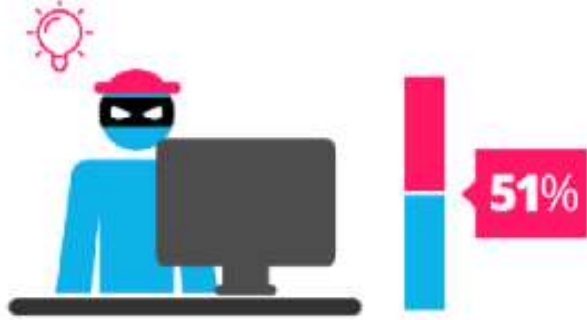


В системе Proof-of-Stake создатель нового блока выбирается системой заранее на основании его личного состояния, то есть доли в общем количестве криптовалюты.

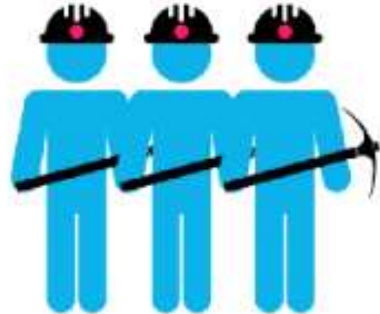
<https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>

<https://ru.insider.pro/tutorials/2017-07-14/proof-work-vs-proof-stake-kak-izmenitsya-ethereum/>





Вознаграждение получает майнер, первым решивший математическую проблему, связанную с блоком



Майнеры в сети соревнуются между собой в поиске решений



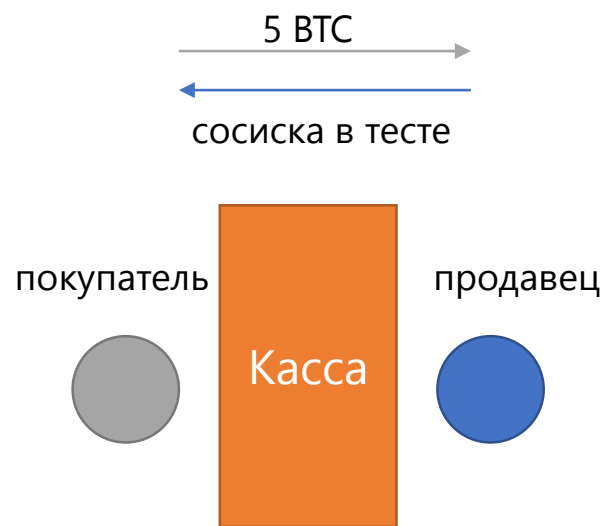
В системе PoS вознаграждение за блок отсутствует в принципе. Доход майнеров составляют исключительно комиссии с транзакций.



Криптовалюты на базе Proof-of-Stake могут быть в тысячи раз более энергоэффективными

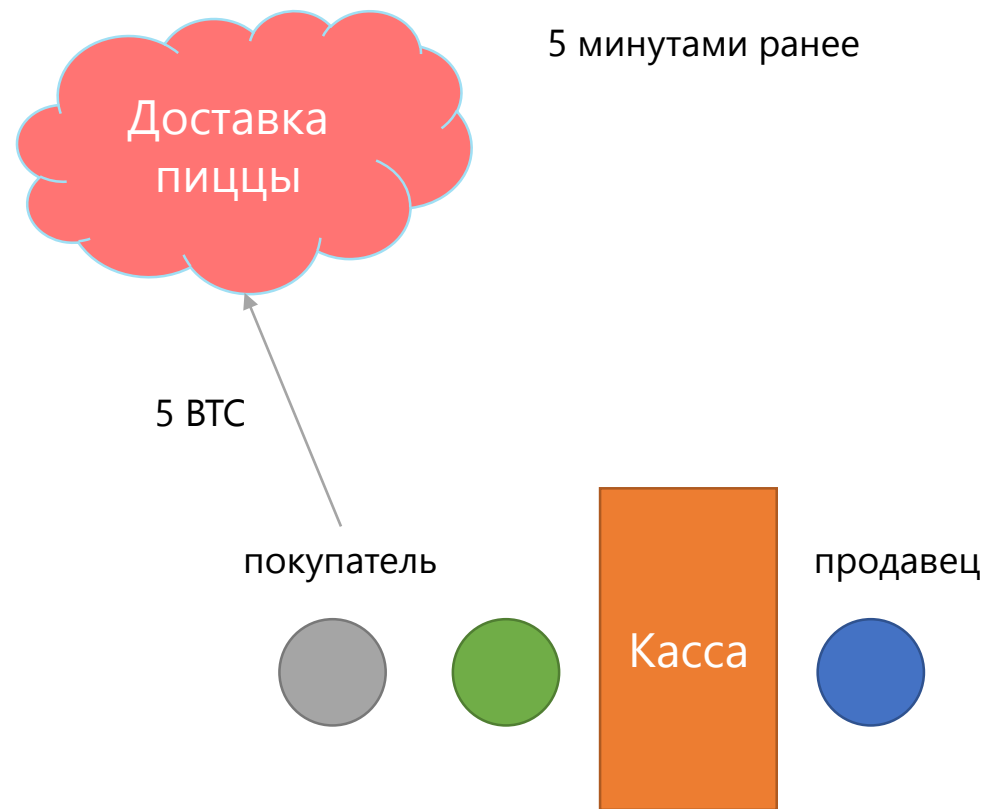
# Double spending

5 BTC

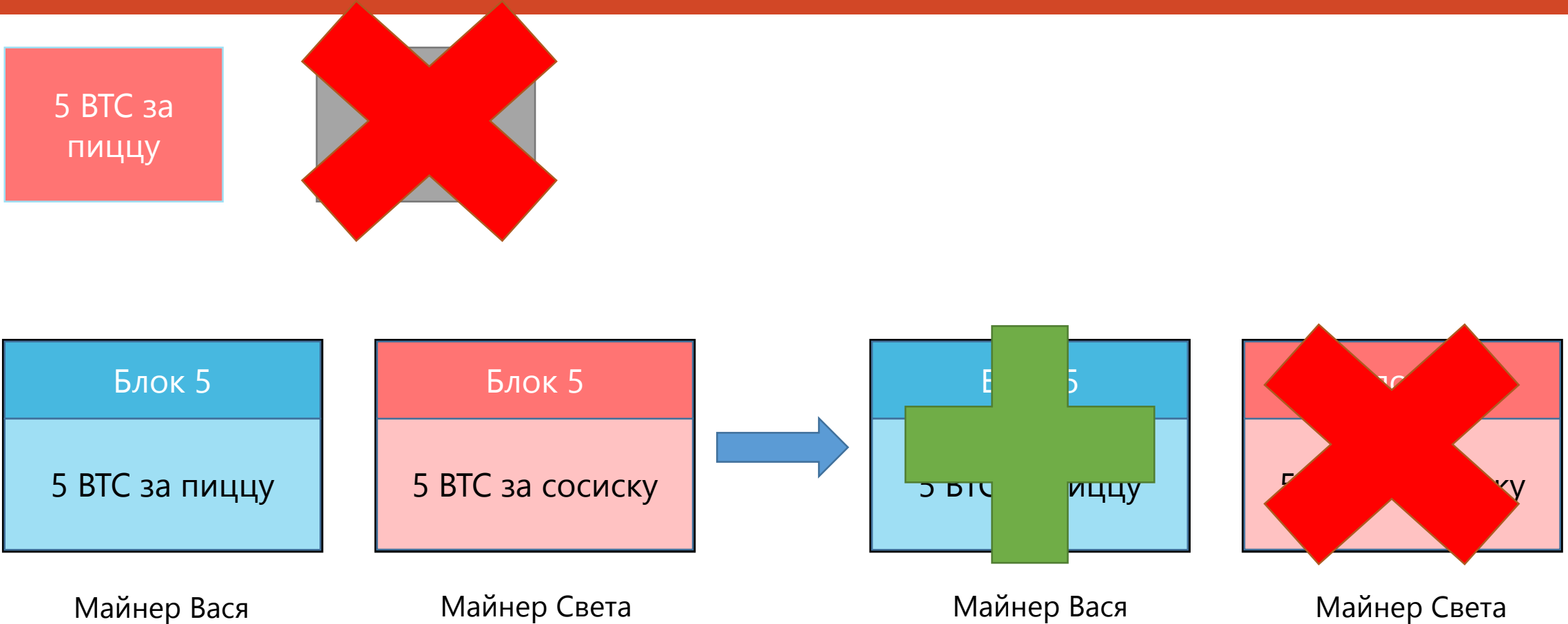


5 минутами ранее

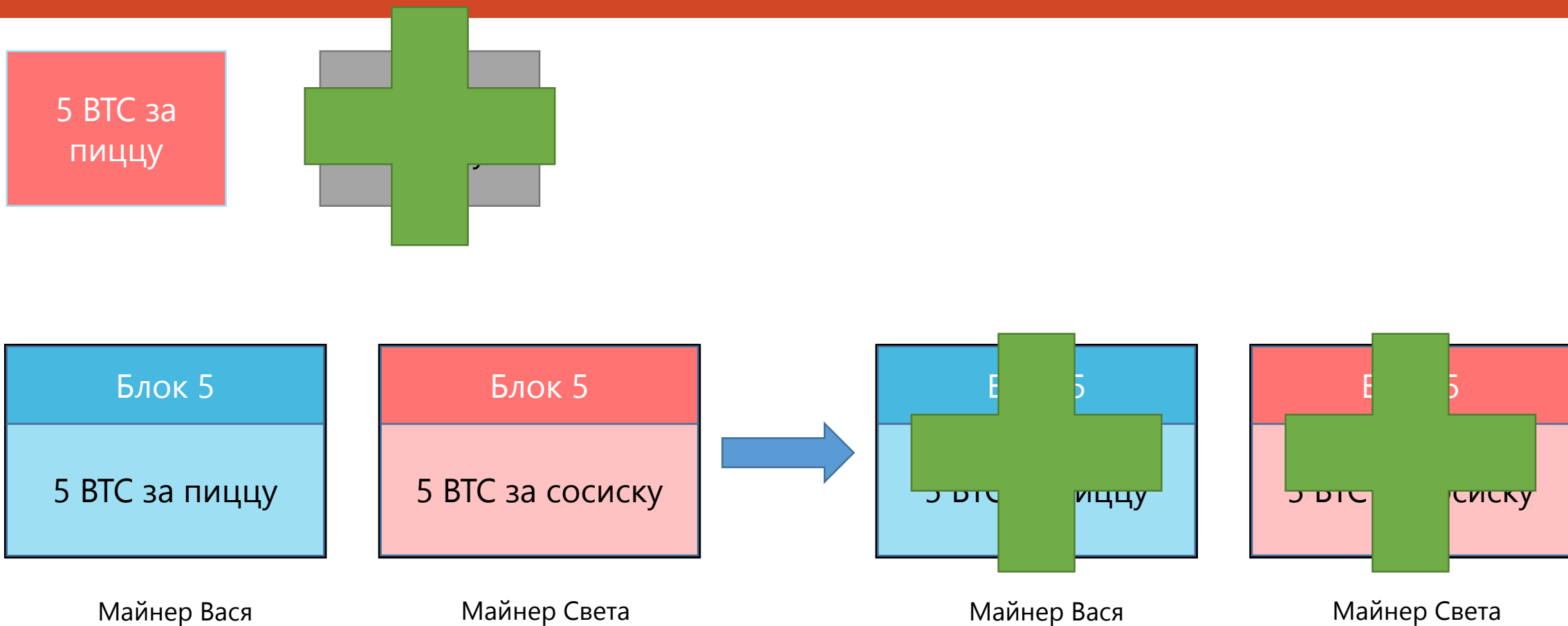
5 BTC



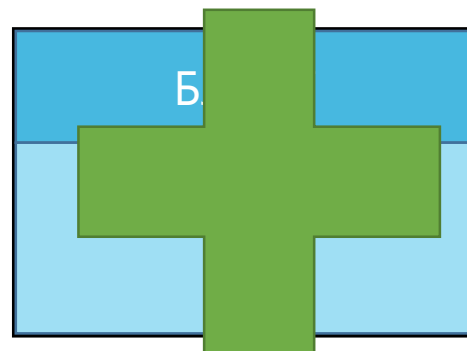
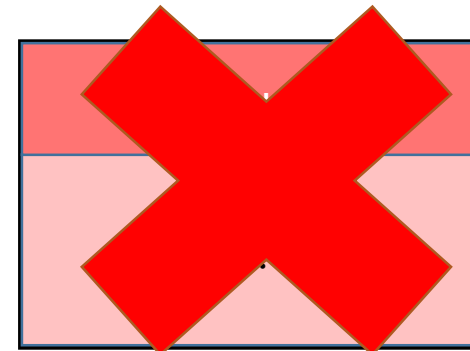
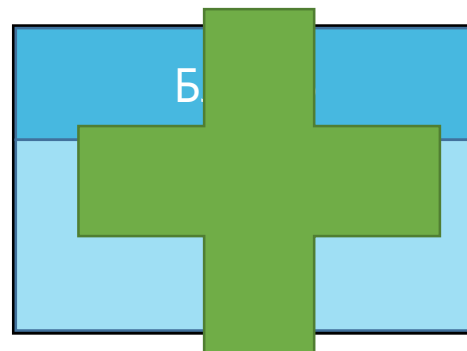
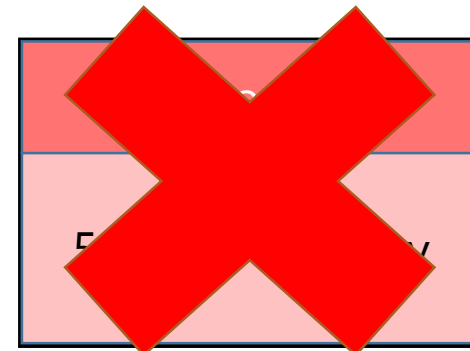
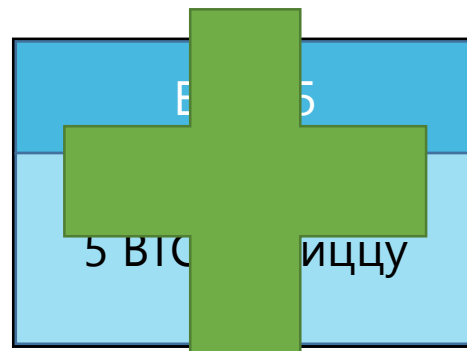
# Место куда попадают транзакции



# Раздвоение цепи



# Место куда попадают транзакции



# А git – это блокчейн?

- Используют одинаковые структуры данных (merkle trees)
- Возможность распределённого хранения
- Отсутствие централизации
- Каждый узел хранит всю историю
- Использует криптографию



# Почему git – это не блокчейн?



# Почему git – это не блокчейн?

- **Консенсус**
- В блокчейне каждый блок верифицируется несколько раз, прежде чем он будет добавлен в цепь
- Гит свободно работает и на одной машине. Представим, ваш SSD посыпался. Если вы не бэкапили данные, потеряете ли вы их? А в блокчейне?
- Гит способен переписывать свою историю: *git push --force, reset --hard*
- Что было в блокчейне – остается в блокчейне

<https://medium.com/@shemnon/is-a-git-repository-a-blockchain-35cb1cd2c491>

<https://stackoverflow.com/questions/46192377/why-is-git-not-considered-a-block-chain>



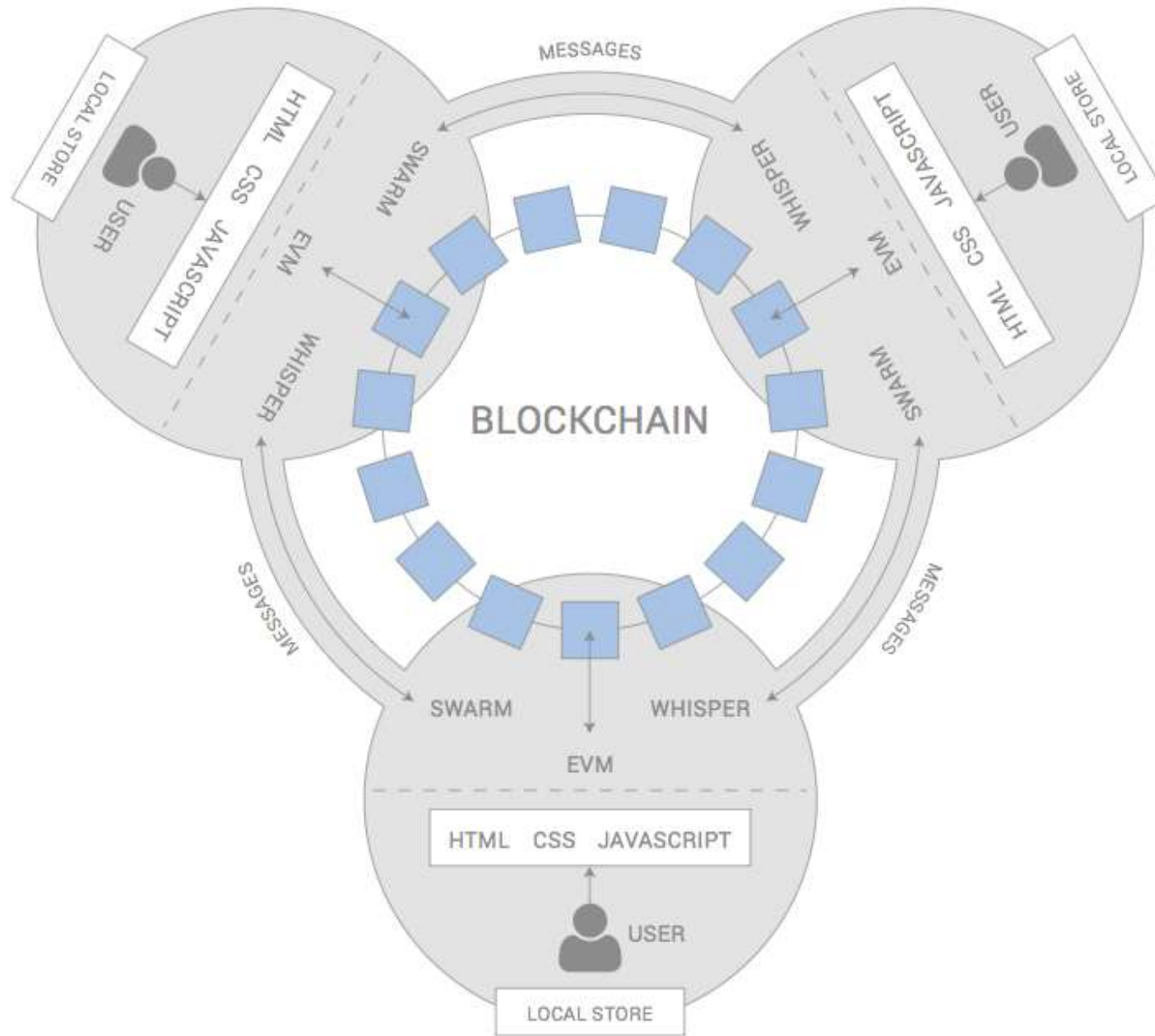
Нечто большее, чем список транзакций



# Что в нем такого крутого?

- Можем запускать вычисления на компьютере майнера
- Глобальный децентрализованный компьютер
- Глобальная децентрализованная виртуальная машина
- Сложный в обращении и очень дорогой компьютер
- Он был первым





# Шокирующая правда об ICO

Шокирующая тайна китайских программистов.  
Чтобы сделать ICO нужно .....



3 вещи



+ 2 вещи



```
import "zeppelin-solidity/contracts/contract/StandardToken.sol";

contract TheSimplestToken is StandardToken {
    string public name = "TheSimplestToken";
    string public symbol = "TST";
    uint public decimals = 18;
    uint public constant INITIAL_SUPPLY = 75 * 10**18;

    function TheSimplestToken(){
        totalSupply = INITIAL_SUPPLY;
        balances[msg.sender] = INITIAL_SUPPLY;
    }
}
```

```
contract Crowdsale {  
  
    address owner;  
    TheSimplestToken public token = new TheSimplestToken();  
  
    uint start = 1516740072;  
    uint period = 28;  
  
    function Crowdsale() {  
        owner = msg.sender;  
    }  
  
    function() external payable {  
        require(now < start + period * 1 days)  
        token.transfer(msg.sender, msg.value);  
    }  
  
}
```



















# Боль

- Развернуть ноду эфира – занятие не для слабонервных
- В эфире нет дробных частей
- Смарт контракты не изменяемы
- Боль с дебаггингом
- Боль из-за сырости Solidity
- Боль с приемом платежей и идентификацией отправителя в биткоине (и не только в нем)



# Большой P.S.

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	 Bitcoin	\$184,442,506,065	\$10,931.40	\$9,187,230,000	16,872,725 BTC	0.99%	
2	 Ethereum	\$92,939,178,274	\$951.30	\$2,669,700,000	97,697,331 ETH	-1.58%	
3	 Ripple	\$44,864,499,135	\$1.15	\$1,155,460,000	39,009,215,838 XRP *	-3.44%	
4	 Bitcoin Cash	\$26,107,107,825	\$1,538.00	\$931,349,000	16,974,713 BCH	0.35%	
5	 Litecoin	\$12,229,838,929	\$221.25	\$972,291,000	55,276,108 LTC	-3.14%	
6	 Cardano	\$10,286,720,798	\$0.396756	\$269,037,000	25,927,070,538 ADA *	-5.07%	
7	 Stellar	\$8,525,524,643	\$0.461649	\$76,198,700	18,467,547,083 XLM *	-2.49%	
8	 <u>NEO</u>	\$8,486,400,000	\$130.56	\$213,126,000	65,000,000 NEO *	-3.51%	



This organization

Search

Pull requests

Issues

Marketplace

Explore



# The Neo Project



<https://neo.org/> [dev@neo.org](mailto:dev@neo.org)

Repositories 15

People 9

## Pinned repositories

[neo](#)

NEO Smart Economy

● C# ★ 2k 🍴 584

[neo-gui](#)

● C# ★ 182 🍴 127

[examples-csharp](#)

● C# ★ 78 🍴 70

[proposals](#)

NEO Enhancement Proposals

★ 64 🍴 31

# Что еще?

## Материалы

<https://www.kaspersky.ru/blog/bitcoin-easy-explanation/12668/> – элементарно о биткоине

<https://forklog.com/chto-takoe-proof-of-work-i-proof-of-stake/> – просто про консенсусы

<https://coinmarketcap.com/currencies/neo/> – The Neo Project

<https://coinspot.io/beginners/chto-takoe-blokchejn-rasskazhem-prostymi-slovami/>

<https://www.youtube.com/watch?v=JquZ7wWtWLY> – хорошая первая половина ролика

<http://www.ledgerprojects.com/how-a-blockchain-works-lets-make-one/>

<https://lhartikk.github.io/> – учебник по построению своей криптовалюты (typescript)

<https://geektimes.ru/company/waves/blog/286896/> – консенсусы

<https://www.youtube.com/watch?v=q6l6adZm40I> – просто про двойную трату

<https://www.youtube.com/watch?v=OD4jGT5yspg> – раздвоение цепи

<http://inaword.ru/smart-kontrakty/> – просто о смартконтрактах для эфира

<http://solidity.readthedocs.io/en/latest/> – Solidity

<https://github.com/OpenZeppelin/zeppelin-solidity>

<https://github.com/trufflesuite/truffle>

## Все закончилось, выдохните!

Ссылки:

- <https://github.com/egorikas/LittleCuteBlockchain> - пример
- <http://egorikas.com> – мой блог
- [egorgrishechko@gmail.com](mailto:egorgrishechko@gmail.com) – мой email