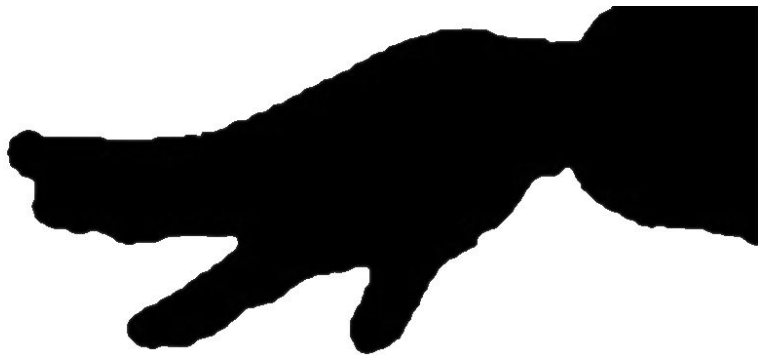


Как работают транзакции



Лекция 2

Что такое эллиптическая кривая?

Что такое ECDSA?

Как генерируется bitcoin адрес?

Обозначения

tx – транзакция

txid – id транзакции. Хеш-значение от тела транзакции

Script – скриптовый язык, который описывает правила проверки

UTXO – Unspent Transaction Output (не потраченные выходы)

fee – комиссия

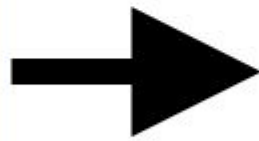
KeyPair – ключевая пара (открытый и личный)

Address – хеш открытого ключа

Wallet – программа кошелёк

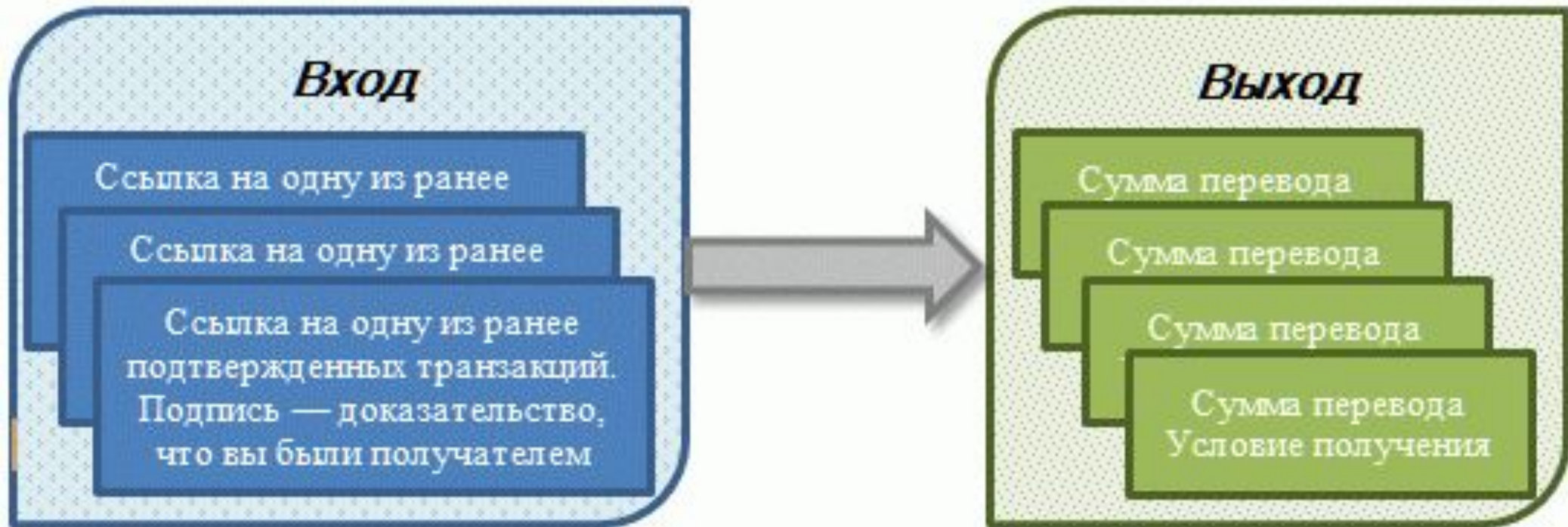
заголовок

**ВХОДНЫЕ
МОНЕТЫ**



**ВЫХОДНЫЕ
МОНЕТЫ**

Транзакция



Input

Поле	Значение
prev_hash	Хеш-значение предыдущей транзакции
out_no	Порядковый номер выхода этой транзакции
script	Доказательство того, что может быть потрачен

Output

Поле	Значение
value	Количество отправляемых bitcoins
script	Описание того, как и кем может быть потрачен

ЭЦП отправителя

Хеш - идентификатор транзакции

Header

Inputs

Outputs

Input-0

Input-1

Output-0

Output-1

```
{
  "hash": "2db75c76aac5f5a9b4b6908793492e66af3d97eb3c27524cca5b33ba0221974f",
  "ver": 1,
  "vin_sz": 2,
  "vout_sz": 2,
  "lock_time": 0,
  "size": 372,
  "in": [
    {
      "prev_out": {
        "hash": "74b5043d57d9581fb3d01d8380f1f938b81985a71644012f2671dca74fb00c72",
        "n": 0
      },
      "scriptSig": "304402205855c83280fa213404588f84bb42e491625cc959f7f117c2a2a67dbcd1c4e5fd022077bc09bb79a654e81202ea7057f90b42790e976d3dc2c293762e2ed96bc0e0b50102aa45f0b5679963bdb155a6899dbab9f7c8a0d526090f57868ab4d4511b787960"
    },
    {
      "prev_out": {
        "hash": "895be57d19de7a5826e0f72e6ca9d61351fd8280200a20761e6874759a1f562c",
        "n": 1
      },
      "scriptSig": "304402205bd5b49259aefb7b389241f48f9d4ac1eb13312ff2d9183888e24f07eb819d0a02207966833fe59e6def3f15a56ee7b1f6d99205b2b1c6324df299a3e0f2810a4f980102d4bb0f8b86fd1ac716d98e7e664676cb597d80f04b3d7f8f0cc707a8f98f5cc3"
    }
  ],
  "out": [
    {
      "value": "0.01241702",
      "scriptPubKey": "OP_DUP OP_HASH160 46b7ceaa8916e13fbefdca32d4009d117d95b9e9OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": "0.01587348",
      "scriptPubKey": "OP_DUP OP_HASH160 00d5316b74c52cfe75f7e676812f1c78e95fbe48OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

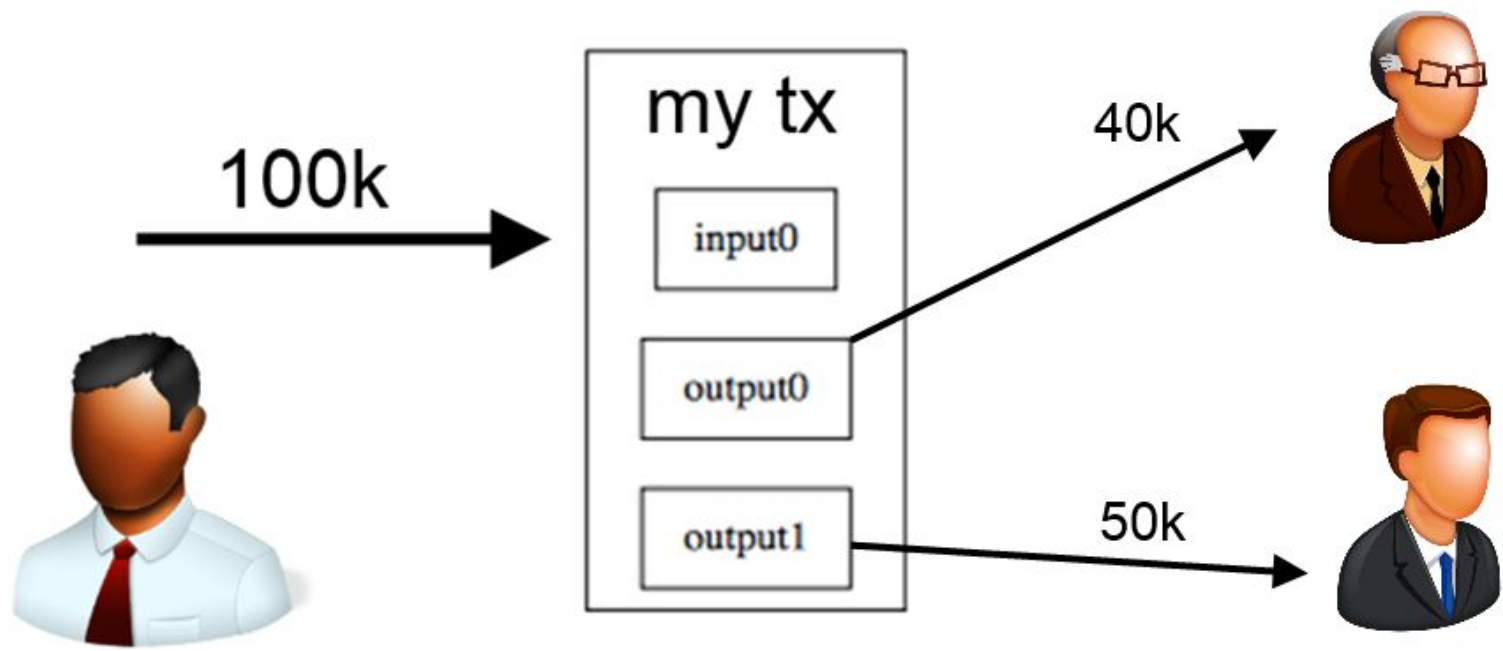


```
{
  "hash": "b8ddb8d91f18c9ad80727c2f05f96d1c0db0ba204f0233f3725ae39bcd074ffd",
  "ver": 1,
  "vin_sz": 1,
  "vout_sz": 1,
  "lock_time": 0,
  "size": 191,
  "in": [
    {
      "prev_out": {
        "hash": "09173d4cb8cc71e1cfcdb0446c9886b7cc1e0875290b1e1566belfala4df0f4a",
        "n": 14
      },
      "scriptSig": "304402202d42afd73aec0fb7d91db750b1be61ad2103378d9fe39cde24f8b12351b3
08ad02200cad5e7c3a0e0fc98dbfe0bfb820c85ea317896e44c9b4a3a2d2bdfecdc2ecf201
031eac46e3a4e001f2c1e937e0b2c5027fa3f2d405c59df5a2b2233fdc6b671c53"
    }
  ],
  "out": [
    {
      "value": "0.03400000",
      "scriptPubKey": "OP_DUP OP_HASH160 e936205ce69349818cd510ca982c2e76a03ec967
OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

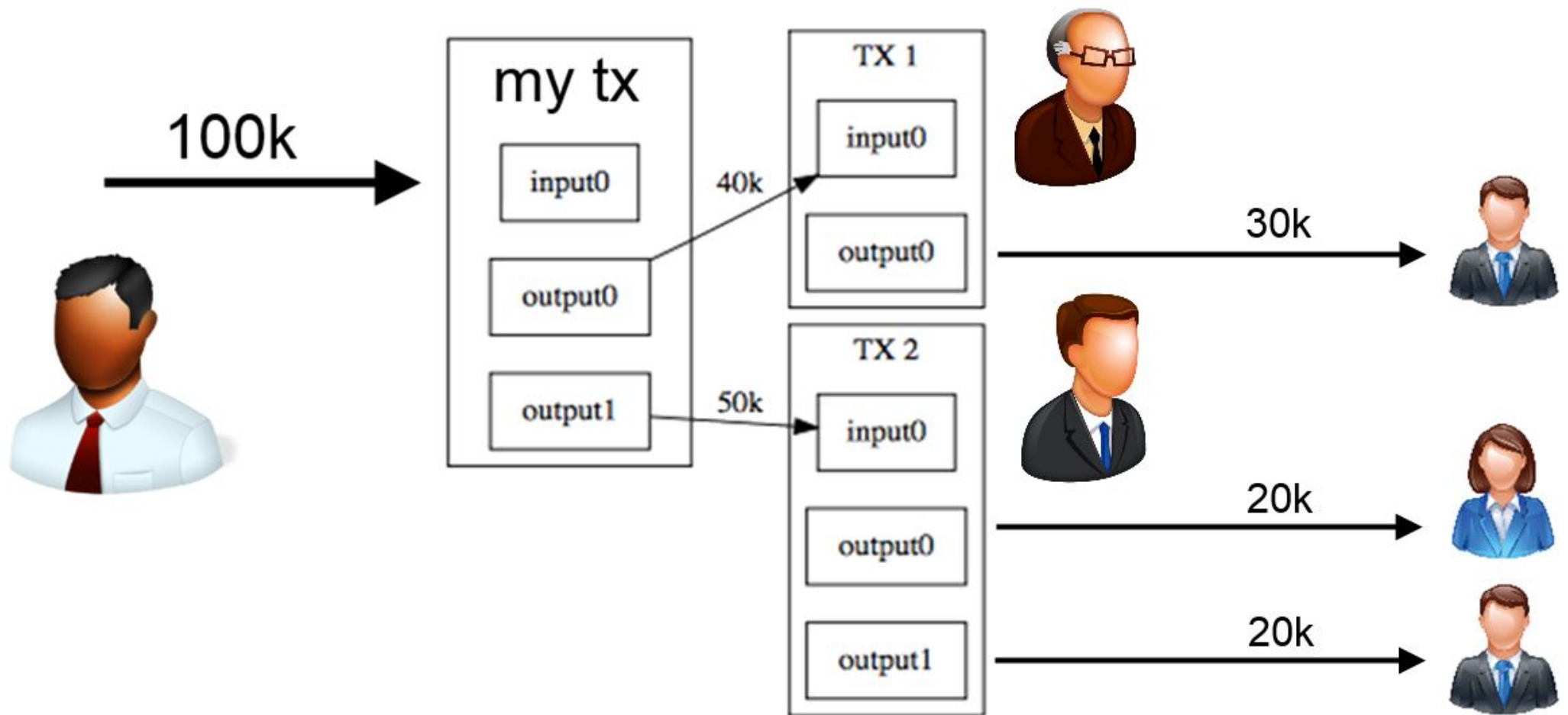
```
{
  "hash": "b8ddb8d91f18c9ad80727c2f05f96d1c0db0ba204f0233f3725ae39bcd074ffd",
  "ver": 1,
  "vin_sz": 1,
  "vout_sz": 1,
  "lock_time": 0,
  "size": 191,
  "in": [
    {
      "prev_out": {
        "hash": "09173d4cb8cc71e1cfcdb0446c9886b7cc1e0875290b1e1566belfala4df0f4a",
        "n": 14
      },
      "scriptSig": "304402202d42afd73aec0fb7d91db750b1be61ad2103378d9fe39cde24f8b12351b3
08ad02200cad5e7c3a0e0fc98dbfe0bfb820c85ea317896e44c9b4a3a2d2bdfecdc2ecf201
031eac46e3a4e001f2c1e937e0b2c5027fa3f2d405c59df5a2b2233fdc6b671c53"
    }
  ],
  "out": [
    {
      "value": "0.03400000",
      "scriptPubKey": "OP_DUP OP_HASH160 e936205ce69349818cd510ca982c2e76a03ec967
OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

Сдача

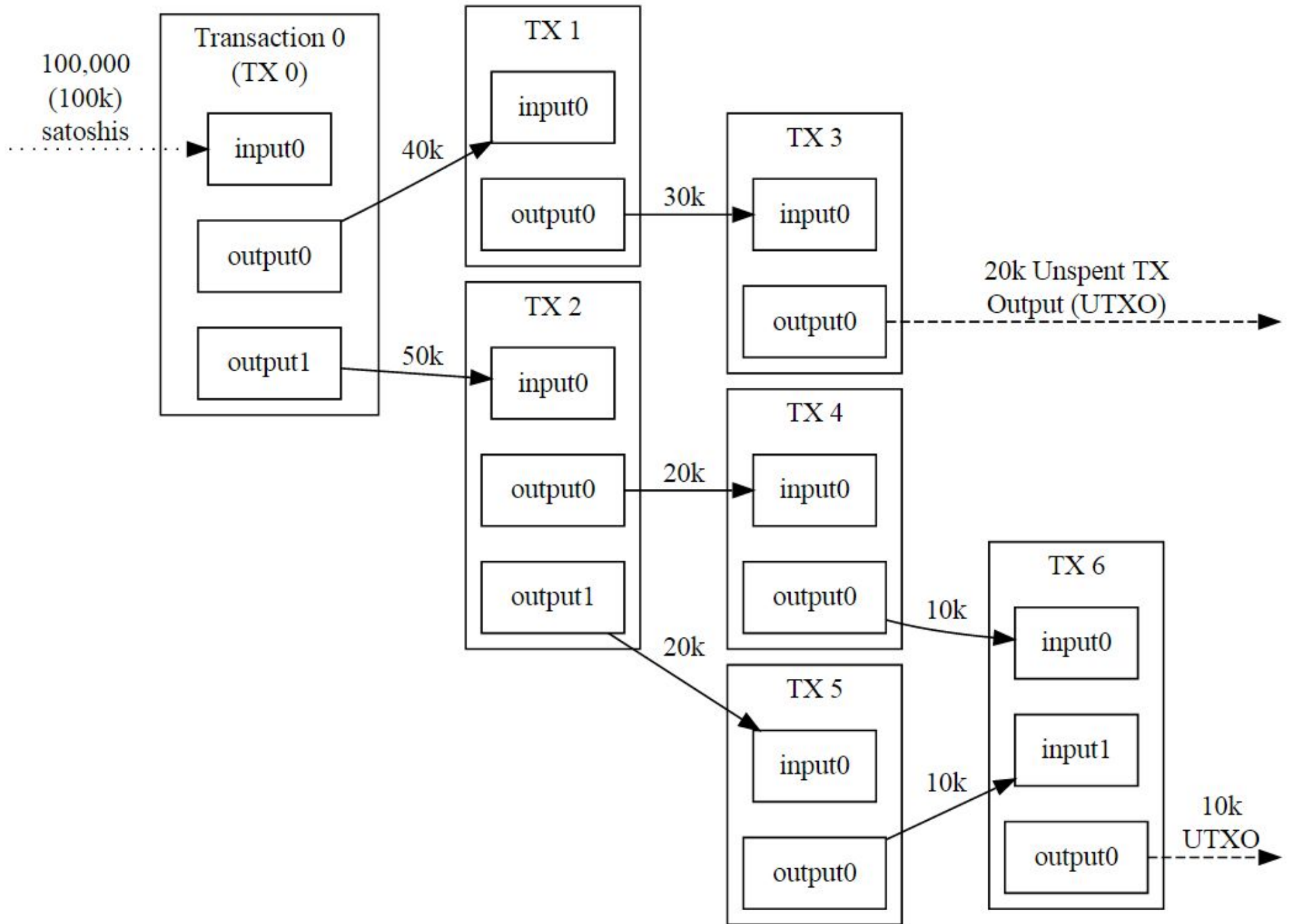
Комиссии



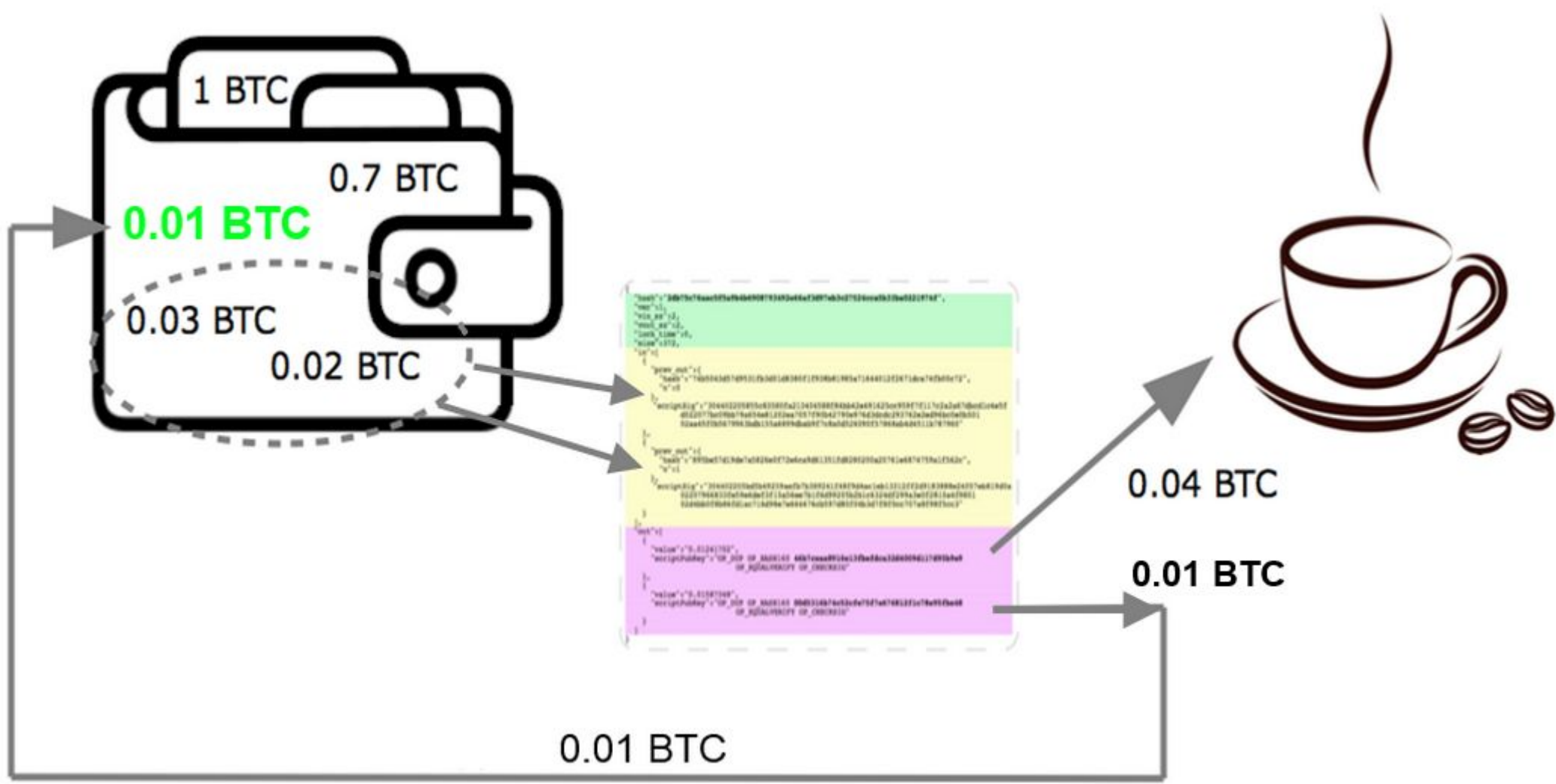
$$\text{fee} = (100) - (40+50)$$



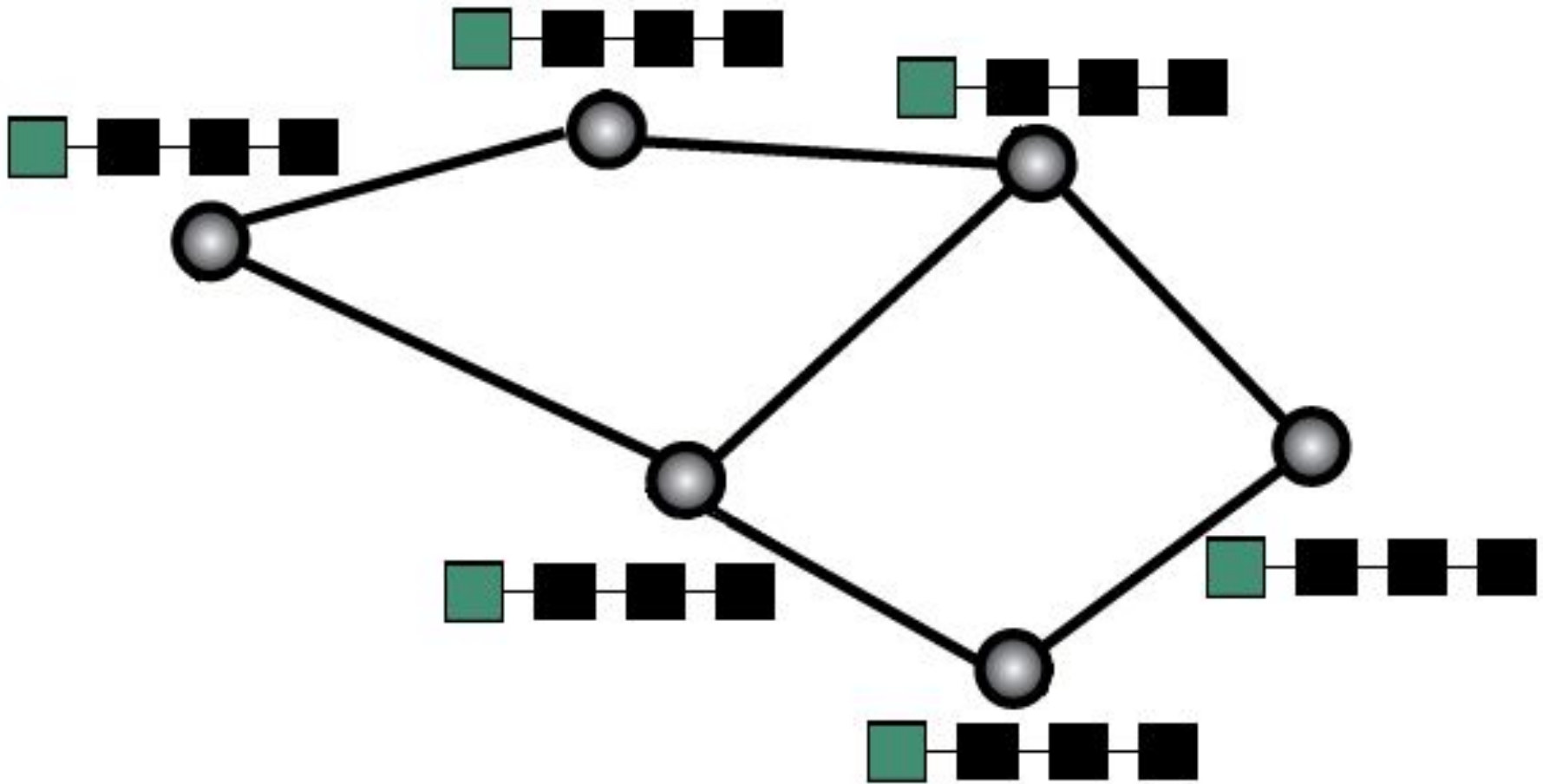
Цепочка транзакций



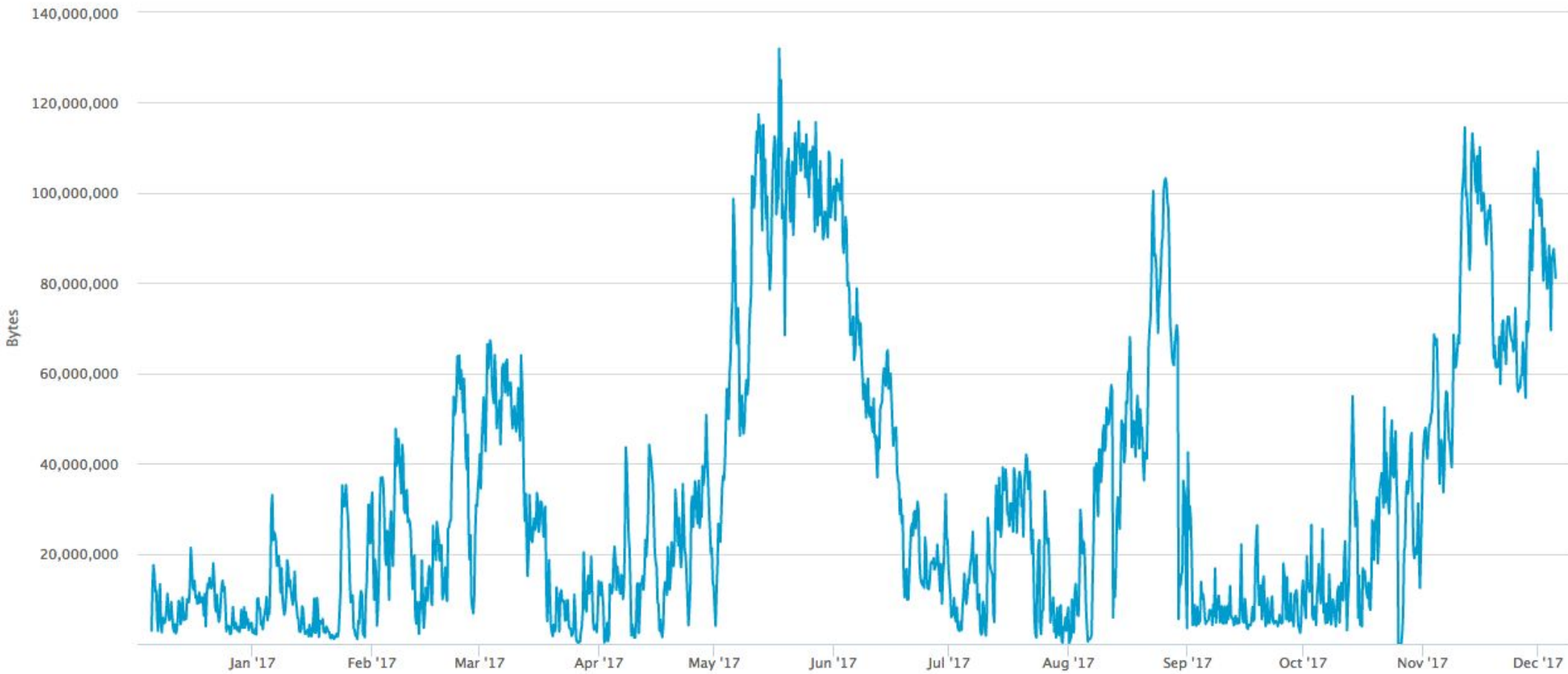
Как работает wallet



Как работает узел сети?



Размер тетроол за последний год



**Как защитить монеты от кражи?
от потери?**



Bitcoin Improvement Proposal

BIP0001

Questions?



skriabinb@gmail.com



bogdan.user



Bohdan Skriabin

