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

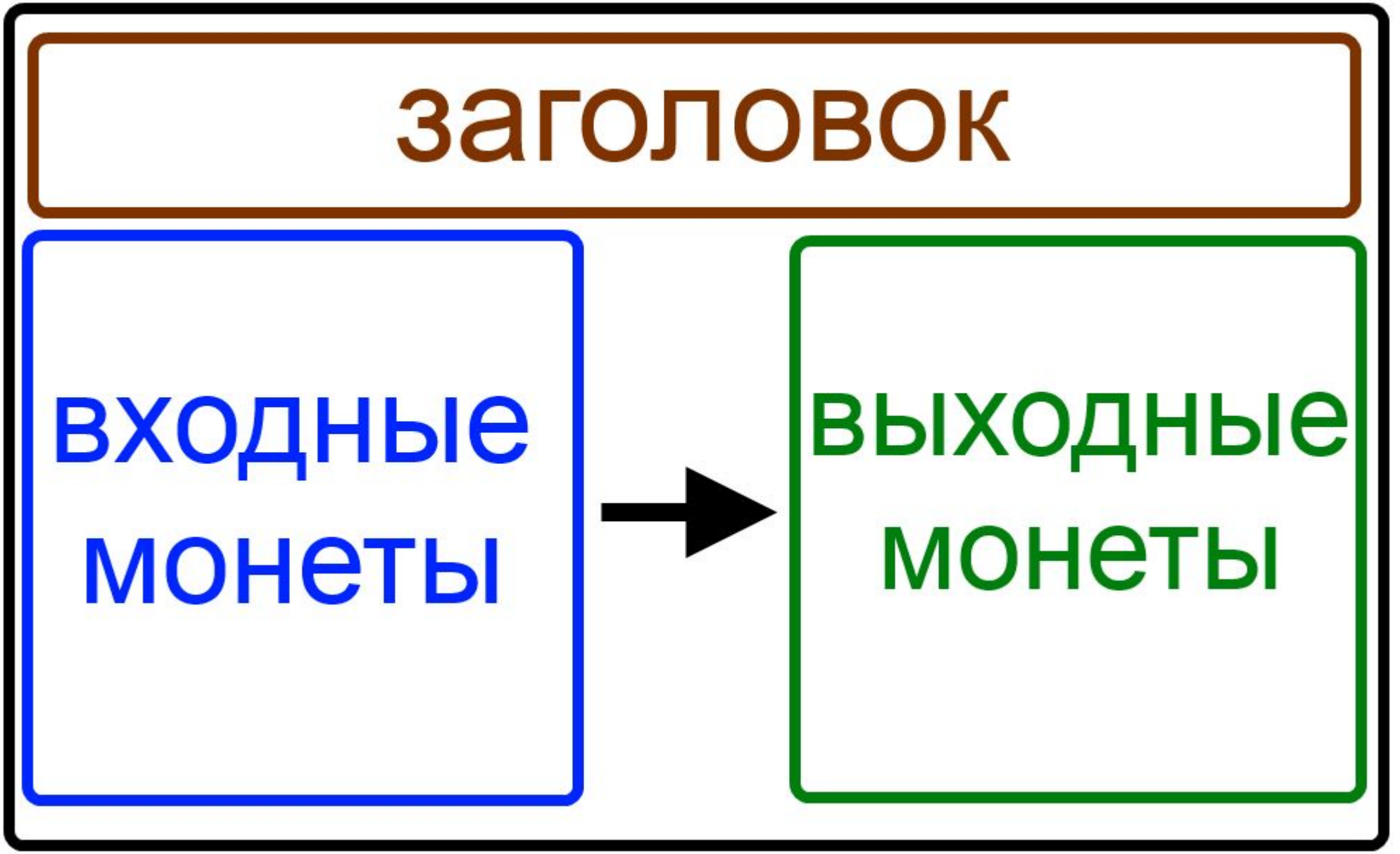
UTXO – Unspent Transaction Output (не потраченные выходы)

fee – комиссия

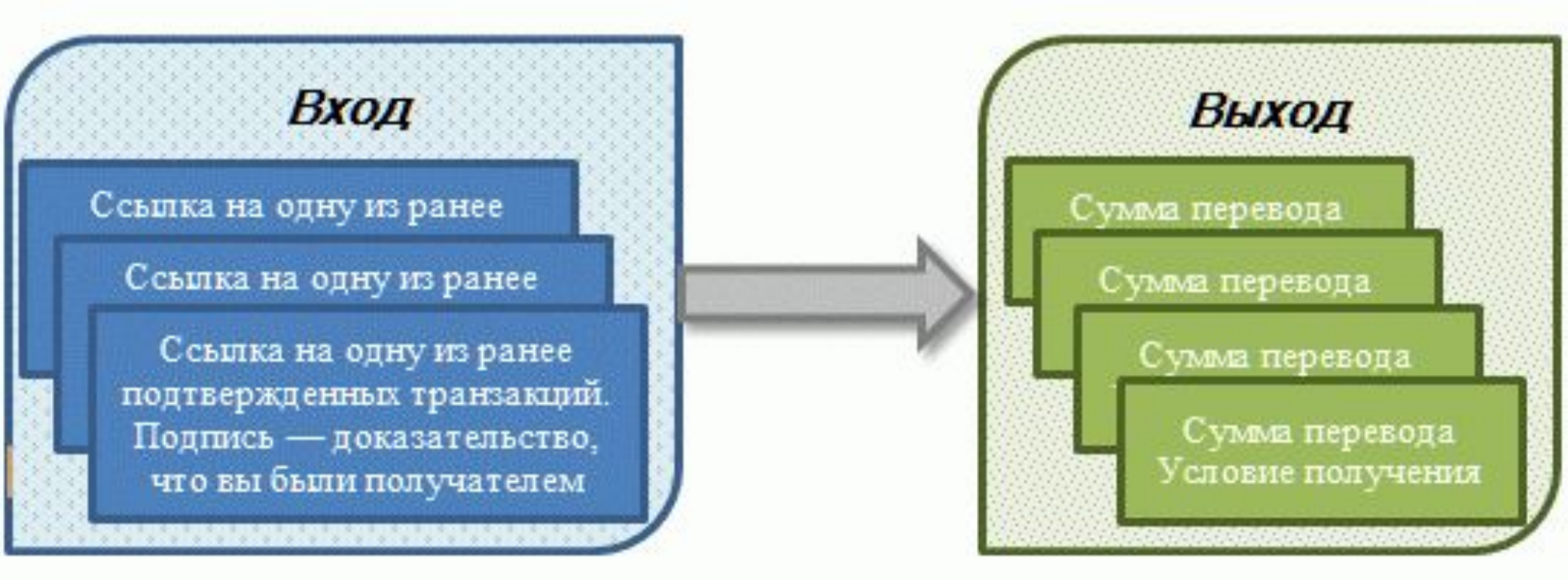
KeyPair – ключевая пара (открытый и личный)

Address – хеш открытого ключа

Wallet – программа кошелёк


заголовок
входные монеты
выходные монеты

Транзакция


Вход
Ссылка на одну из ранее
Ссылка на одну из ранее
Ссылка на одну из ранее подтвержденных транзакций. Подпись — доказательство, что вы были получателем
Выход
Сумма перевода
Сумма перевода
Сумма перевода
Сумма перевода
Условие получения

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

Input-0

Input-1

Outputs

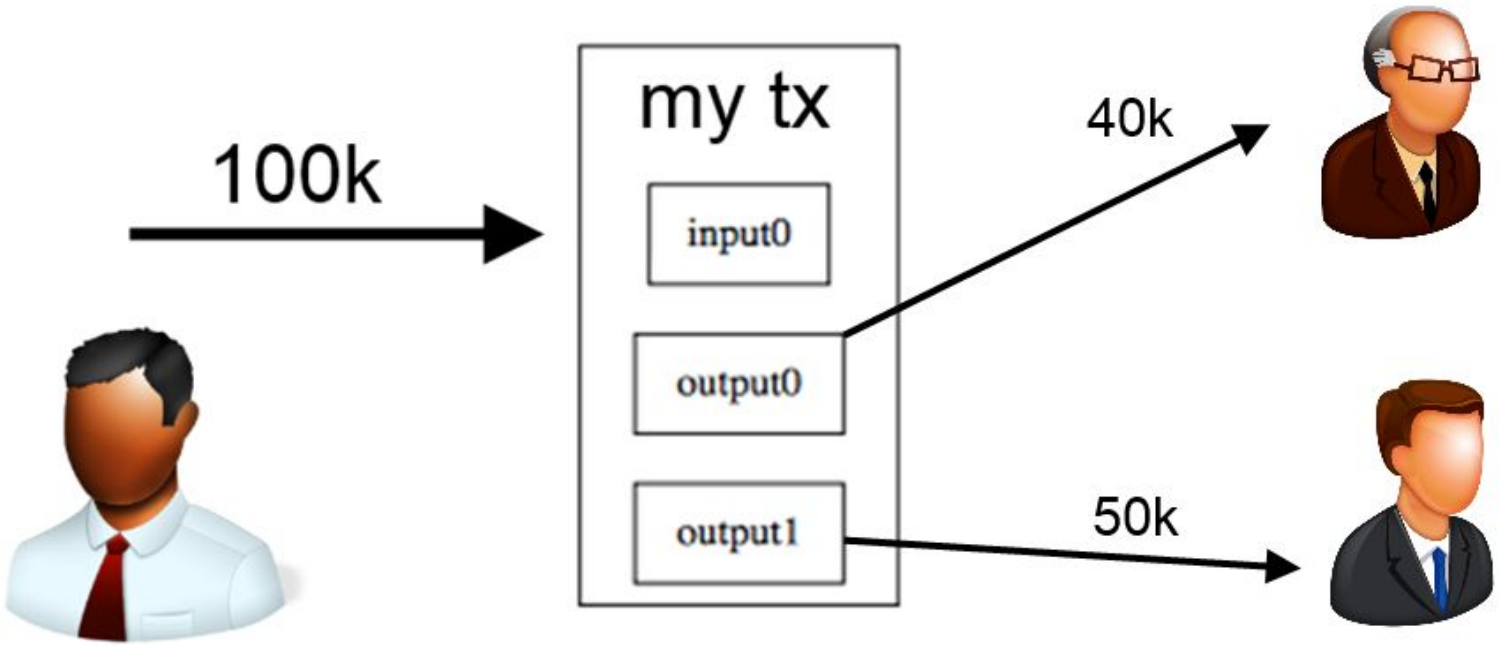
Output-0

Output-1

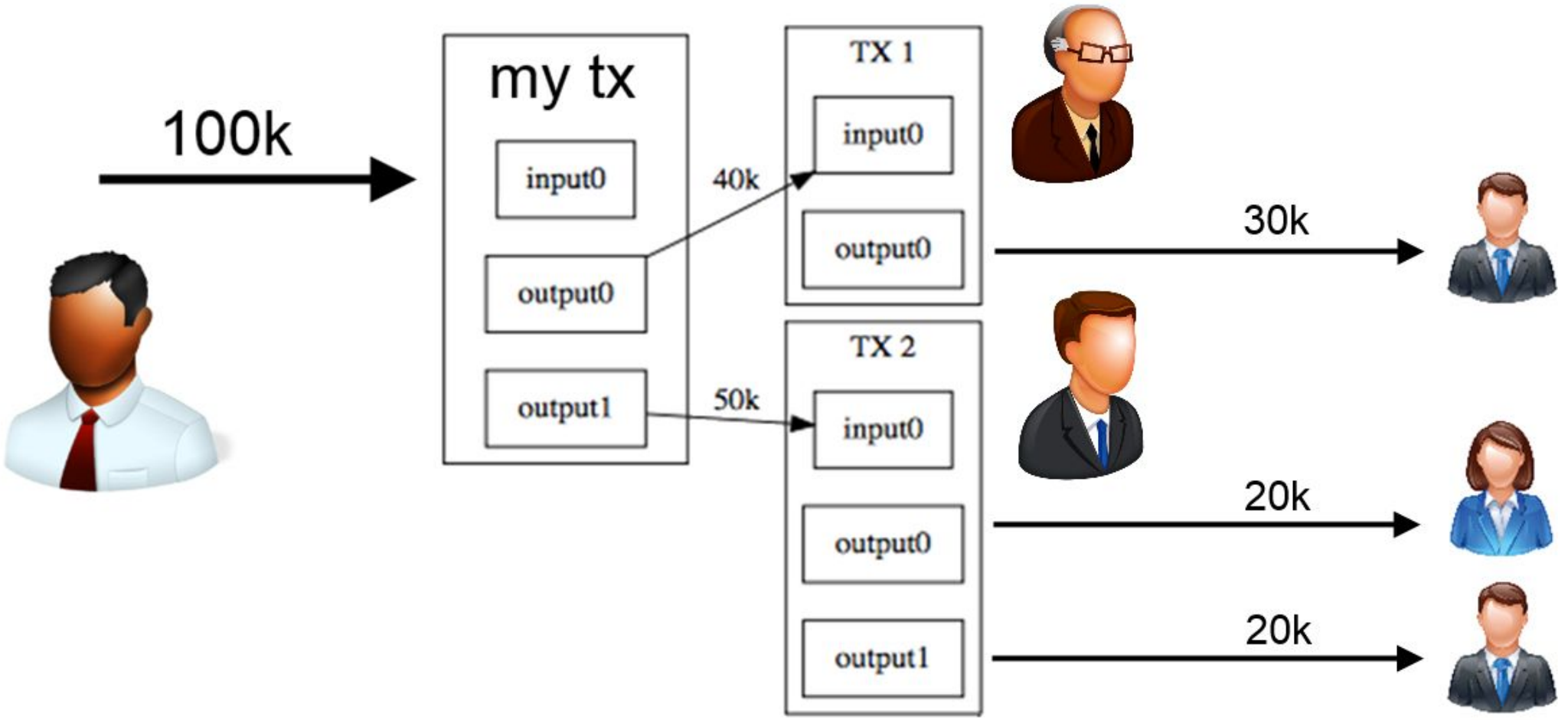

```
{
  "hash":"b8ddb8d91f18c9ad80727c2f05f96d1c0db0ba204f0233f3725ae39bcd074ffd",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":191,
  "in":[
    {
      "prev_out":{
        "hash":"09173d4cb8cc71e1cfcdb0446c9886b7cc1e0875290b1e1566be1fa1a4df0f4a",
        "n":14
      },
      "scriptSig":"304402202d42afd73aec0fb7d91db750b1be61ad2103378d9fe39cde24f8b12351b3
            08ad02200cad5e7c3a0e0fc98dbfe0bfb820c85ea317896e44c9b4a3a2d2bdfecdc2ecf201
            031eac46e3a4e001f2c1e937e0b2c5027fa3f2d405c59df5a2b2233fdc6b671c53"
    }
  ],
  "out":[
    {
      "value":"0.03400000",
      "scriptPubKey":"OP_DUP OP_HASH160 e936205ce69349818cd510ca982c2e76a03ec967
                      OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

Сдача

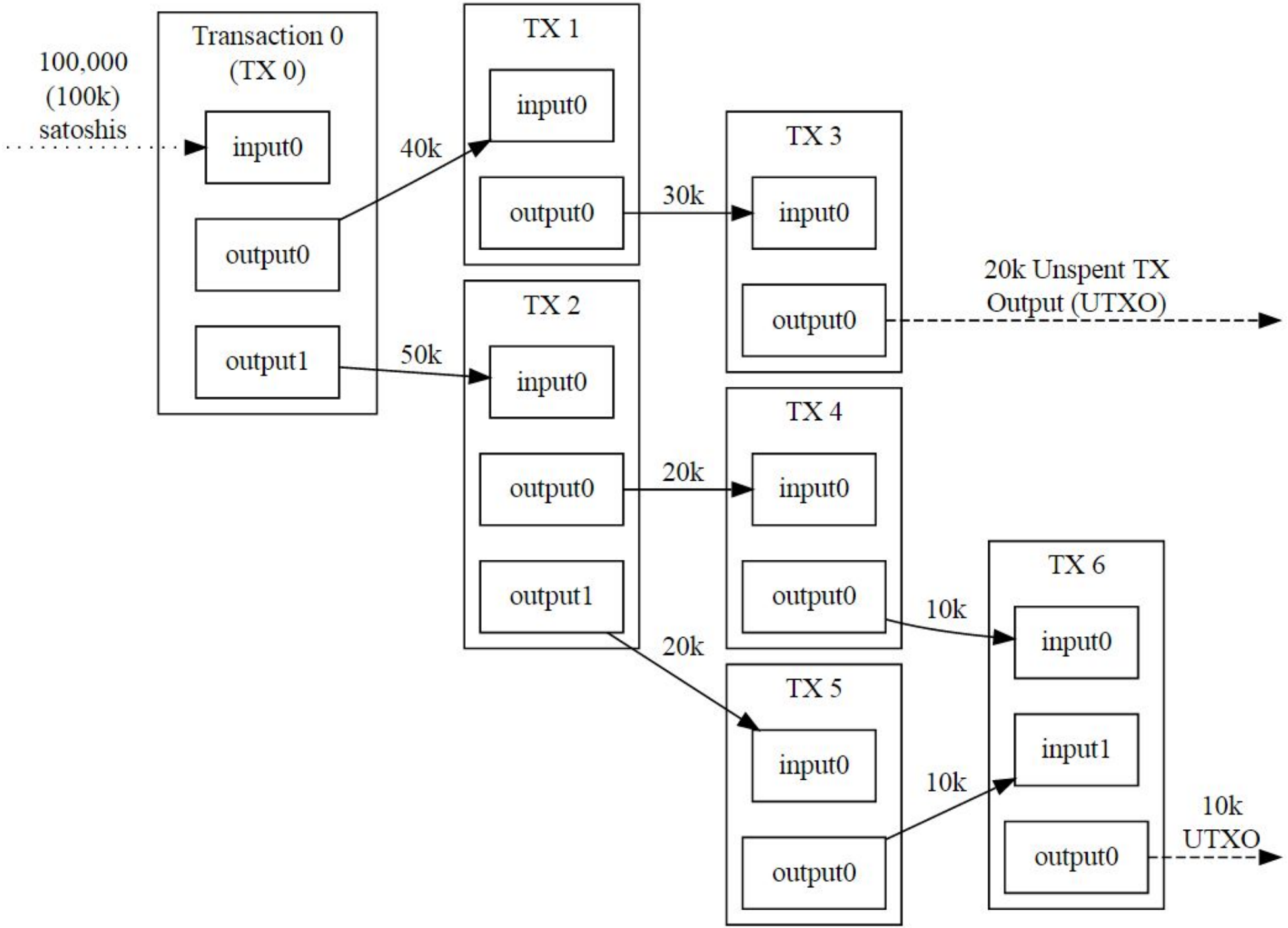
Комиссии



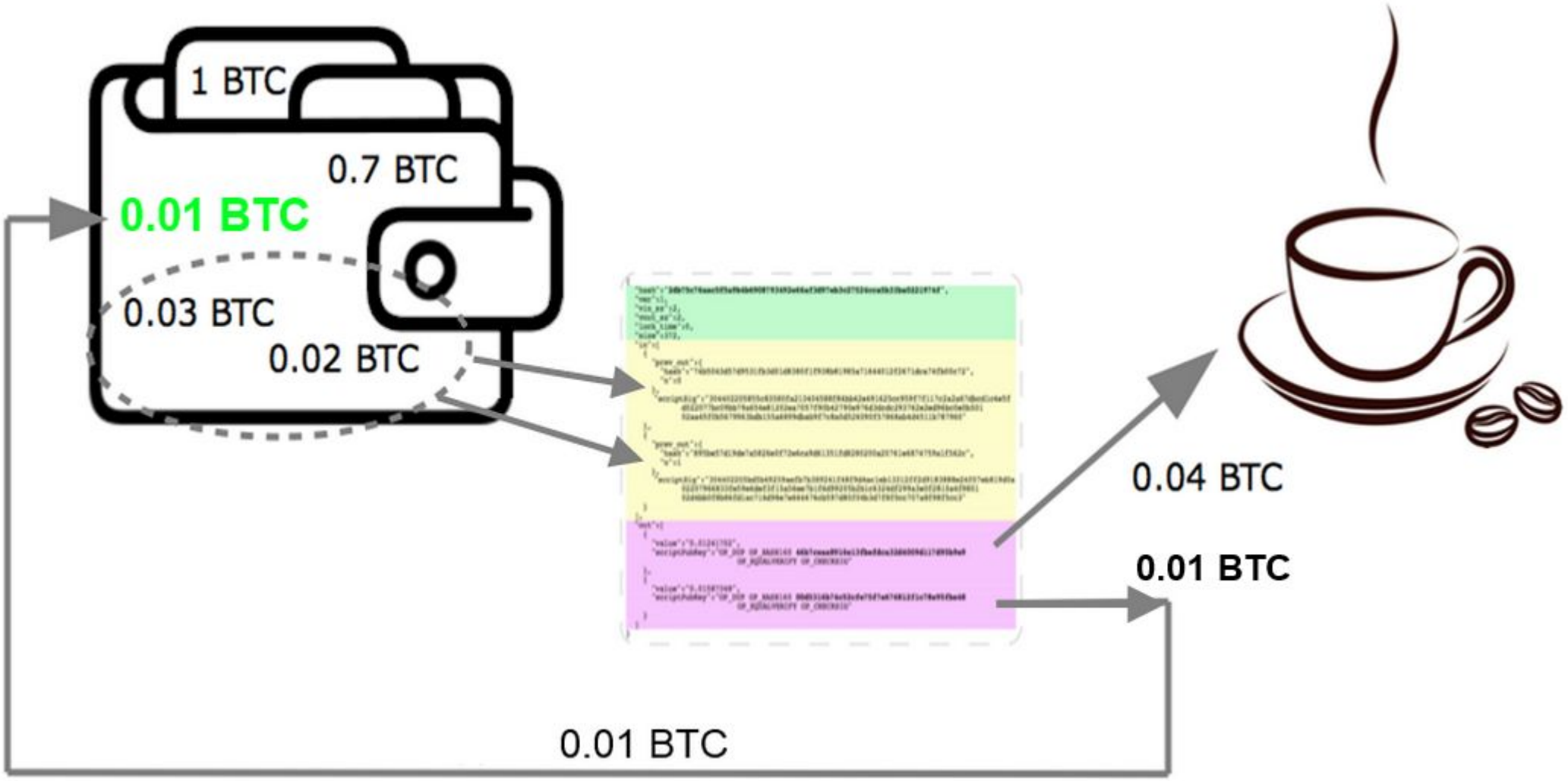
fee = (100) - (40+50)


100k
my tx
input0
output0
output1
40k
50k
TX 1
input0
output0
TX 2
input0
output0
output1
30k
20k
20k

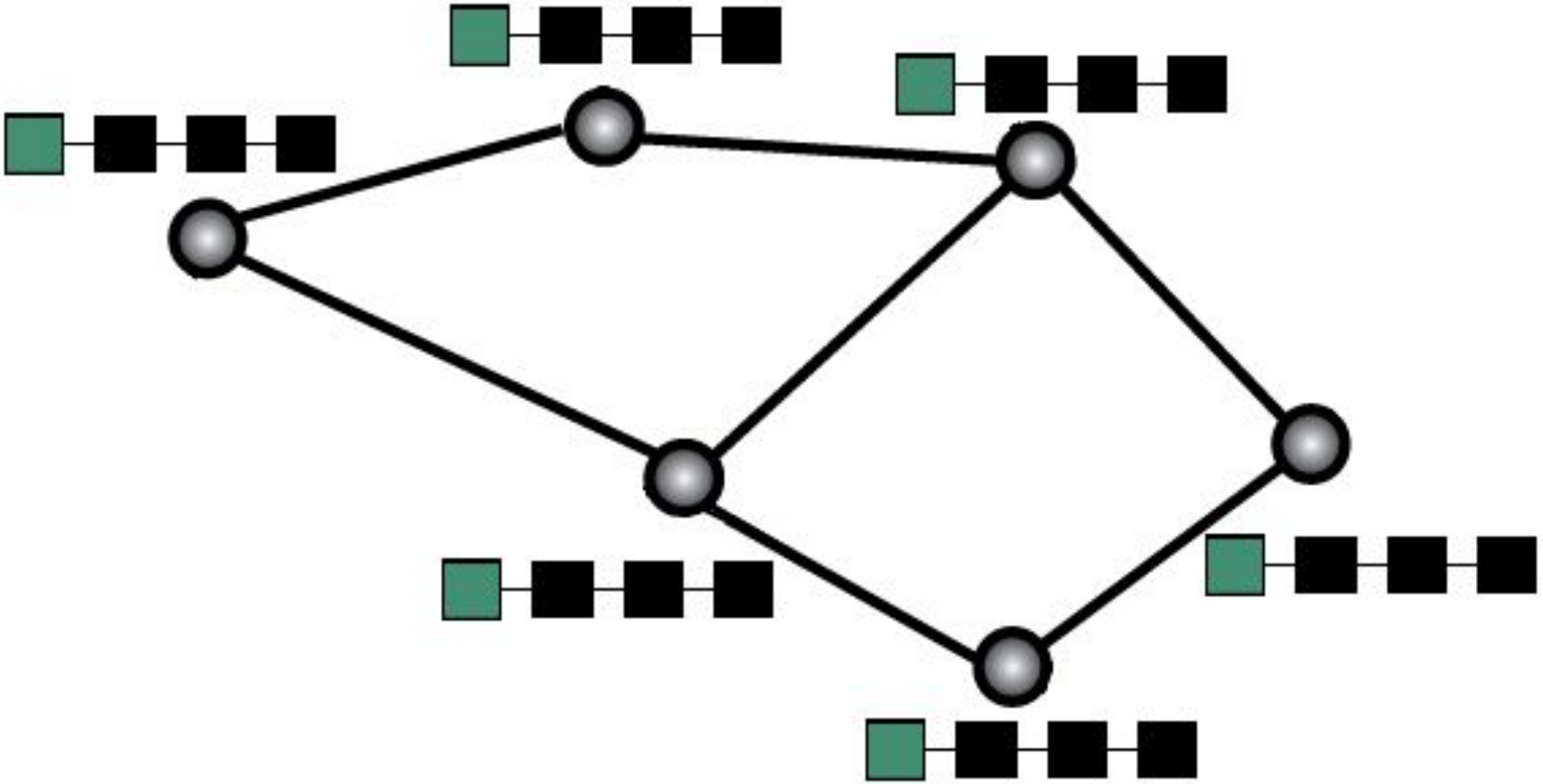
Цепочка транзакций



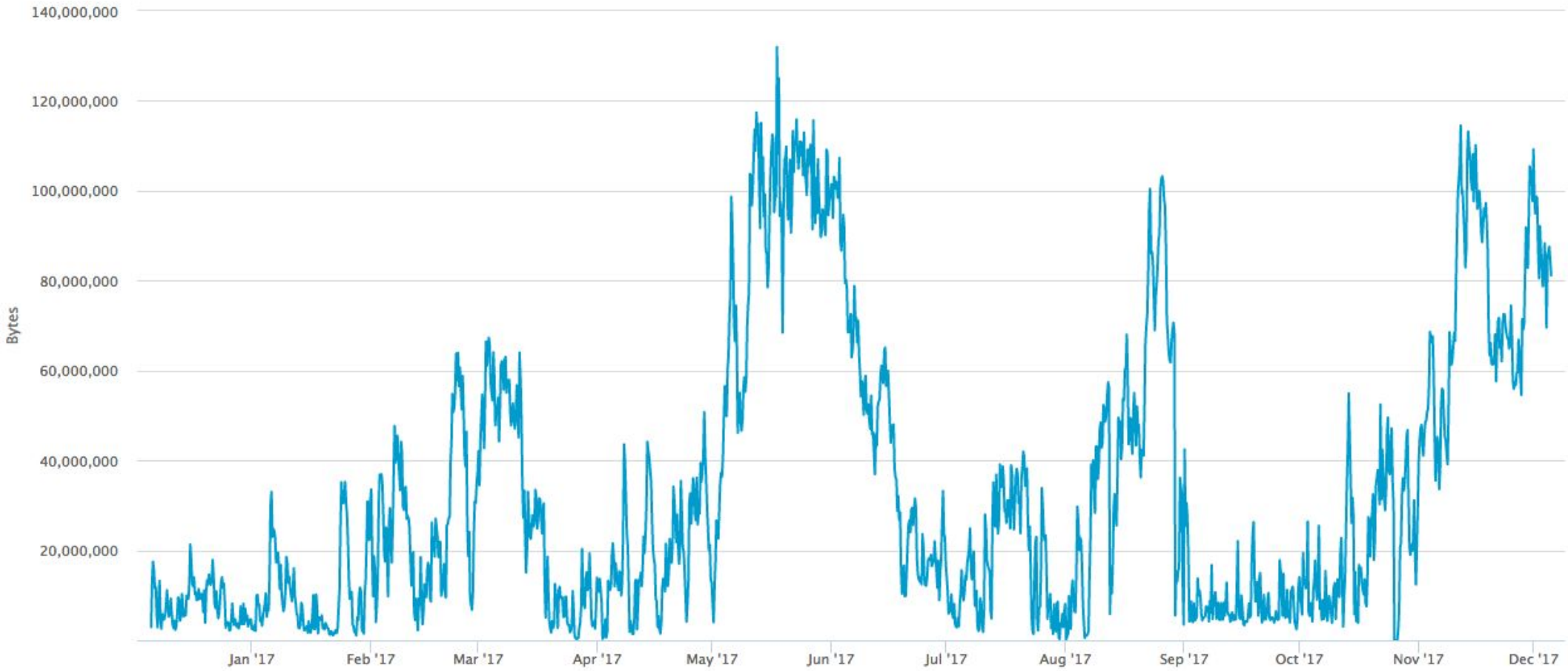
Как работает wallet



Как работает узел сети?

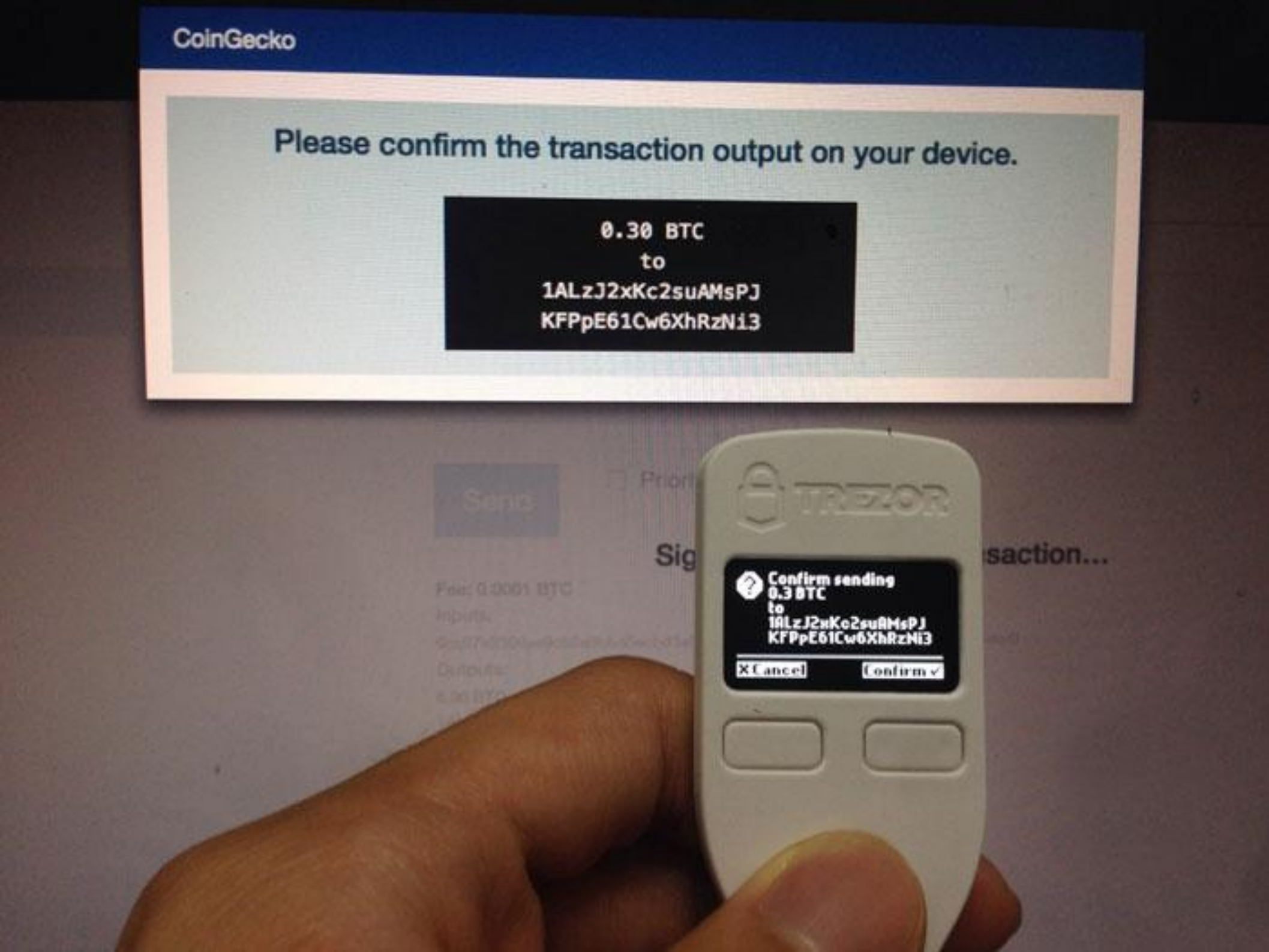


Размер mempool за последний год



Как защитить монеты от кражи? от потери?


tab
caps lock
shift
Ledger


CoinGecko
Please confirm the transaction output on your device.
0.30 BTC
to
1ALzJ2xKc2suAMsPJ
KFPpE61Cw6XhRzNi3
TREZOR
Confirm sending
0.3 BTC
to
1ALzJ2xKc2suAMsPJ
KFPpE61Cw6XhRzNi3
Cancel
Confirm

Bitcoin Improvement Proposal

BIP0001

Questions?

skriabinb@gmail.com

bogdan.user

Bohdan Skriabin