
vinteum

Casa21

Casa21@12345

Running Bitcoin:
Run Your own Bitcoin Node

Unicamp

vinteum

Edil Medeiros

Universidade de Brasília

prof@edil.com.br

@edil_medeiros

/@edilmedeiros

edil@nostrplebs.com

Jão Noctus

ZBD

jaonoctus@protonmail.com

PGP 0x782C165A293D6E18

jaonoctus.dev

halfin
@halfin

Running bitcoin

9:33 PM · 1/10/09 · Twitter Web Client

Agenda

1. Iniciar um nó Bitcoin
2. Criar uma carteira
3. Conectar-se com outros nós
4. Criar um pagamento
5. Confirmar os pagamentos
6. Entender as transações
7. Entender blocos e a blockchain

https://edil.com.br/workshop

Atenção

Ao copiar e colar comandos dos slides, ajustar as aspas.

1. Iniciar um nó Bitcoin

Explicar o que é um nó de Bitcoin

```
# Clonar o repositório
$ git clone https://github.com/vinteum-bdl/infra-signet-docker

# “Compilar" a imagem do container
$ docker compose build --no-cache

# Subir o container
$ docker compose up bitcoin-node -d

# Logar no container
$ docker compose exec --user student -it bitcoin-node bash

# No shell do container
# bitcoind
```

$ bitcoin-cli **getblockchaininfo**


```
{
  "chain": "signet",
  "blocks": 0,
  "headers": 0,
  "bestblockhash": "00000008819873e925422c1ff0f99f7cc9bbb232af63a077a480a3633bee1ef6",
  "difficulty": 0.00112651529069818 6,
  "time": 1598918400,
  "mediantime": 1598918400,
  "verificationprogress": 1,
  "initialblockdownload": true,
  "chainwork": "0000000000000000000000000000000000000000000000000000049d414",
  "size_on_disk": 293,
  "pruned": false,
  "warnings": ""
}
```

```
$ bitcoin-cli help
$ bitcoin-cli help getblockchaininfo

getblockchaininfo

Returns an object containing various state info regarding blockchain processing.

Result:
{                                         (json object)
  "chain" : "str",                        (string) current network name (main, test, signet,
regtest)
  "blocks" : n,                           (numeric) the height of the most-work fully-validated
chain. The genesis block has height 0
…
}

Examples:
> bitcoin-cli getblockchaininfo
> curl --user myusername --data-binary '{"jsonrpc": "1.0", "id": "curltest", "method":
"getblockchaininfo", "params": []}' -H 'content-type: text/plain;' http://127.0.0.1:8332/
```

2. Criar uma carteira

Explicar o que é uma carteira

```
$ bitcoin-cli createwallet "<name>"


{
  "name": "wallet_edil"
}
```

```
$ bitcoin-cli getbalance

0.00000000
```

```
$ bitcoin-cli importdescriptors ‘[{“desc”: “<descriptor>”, “timestamp”: 0}]’


[
  {
    "success": true,
    "warnings": [
      "Range not given, using default keypool range"
    ]
  }
]
```

Qual é o saldo da sua carteira?

3. Conectar-se com outros nós

```
$ bitcoin-cli getpeerinfo


[
]
```

Em duplas, decidam quem será o nó A e quem será o nó B.

A. Conecte-se ao seu colega

```
$ bitcoin-cli addnode “<node IP>:38333” “onetry"
```

A+B. Verifique seus peers

Qual é o saldo da sua carteira?

Que tal conectar o seu node ao de outros 3 colegas?

Quantos blocos tem a sua blockchain?

Conecte-se ao minerador!

10.21.21.88

E agora, quantos blocos tem a sua blockchain?

Qual é o saldo da sua carteira?

4. Criar um pagamento

Em duplas, decidam quem será o nó A e quem será o nó B.

A. Crie um endereço para receber bitcoins do seu colega.

```
$ bitcoin-cli getnewaddress

tb1q3hn57lswjdmv5vnr4nff5uhwxuee0erugvy8g6
```

B. Crie um pagamento de para o seu colega. Anote o txid para investigarmos a transação posteriormente.

```
$ bitcoin-cli -named sendtoaddress address="<address>" amount=<amount> fee_rate=1
```

```
4c42e0d3bf7ca1ac65107e12207ae6ed0d38428a4dbc1c7665aa767fb2dd953a
```

Qual é o balanço da sua carteira após o pagamento?

```
$ bitcoin-cli getbalances
```


```
{
  "mine": {
    "trusted": 7.46290747,
    "untrusted_pending": 1.00000000,
    "immature": 0.00000000
  },
  "lastprocessedblock": {
    "hash":
"0000011b6b8e072729f5e4500946c96530f2a296305b687ba18a20d3db7fef1e",
    "height": 303
  }
}
```

O que é o saldo pendente?

$ bitcoin-cli **getrawtransaction** “<txid>” 1


```
{
  "txid": "4c42e0d3bf7ca1ac65107e12207ae6ed0d38428a4dbc1c7665aa767fb2dd953a",
  "hash": "6fe60b8bceda707bbe681b35e029a04494ab2b63681e79a2612982df68089fb9",
  "version": 2,
  "size": 518,
  "vsize": 276,
  "weight": 1103,
  "locktime": 216,
  "vin": [
    {
      "txid": "35bbf26d0e2eeef9d30e501ff5a7e0980643ac27c0c8849d043b3783be6f6ea5",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402200ca30fcf9b0897b4938de8a1e149a0856ee56b7ef45e7d1a9b02701aa5064e20022027f0721ee2214af24cf8f693aae605e0c4728dbd3c6cd0e3551a081d489f142301",
        "036128c701f1769889945de8ddd59e8e0c6d33553b56d6a7ef9c46aed39c49d793"
      ],
      "sequence": 4294967293
    },
    {
      "txid": "12604a90d38827ebfc3381307751d77a587a12e5dae5a6cb26482b1fce592900",
      "vout": 1,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
```

Onde foi parar a transação?

```
$ bitcoin-cli getrawmempool


[
  "4c42e0d3bf7ca1ac65107e12207ae6ed0d38428a4dbc1c7665aa767fb2dd953a"
]
```

5. Confirmar os pagamentos

Qual é o saldo da sua carteira após a mineração de um novo bloco?

Diving deeper!

6. Entender blocos e a blockchain

Qual foi o último bloco minerado?

```
$ bitcoin-cli getblockhash <height>
```

```
000002898e5d67b653370beb37701af9fa207a1ce3ed5a5099368219b908a4bf
```

$ bitcoin-cli **getblockheader** "<block hash>”


```
{
  "hash": "000002898e5d67b653370beb37701af9fa207a1ce3ed5a5099368219b908a4bf",
  "confirmations": 6,
  "height": 304,
  "version": 536870912,
  "versionHex": "20000000",
  "merkleroot": "4922268ff84988cc31a88bb42809072dc15cc2dc19906c841eeb195b5a621733",
  "time": 1730203899,
  "mediantime": 1730200899,
  "nonce": 1641808,
  "bits": "1e0377ae",
  "difficulty": 0.0011265152906981 86,
  "chainwork": "00000000000000000000000000000000000000000000000000000057f5abd4",
  "nTx": 2,
  "previousblockhash": "0000011b6b8e072729f5e4500946c96530f2a296305b687ba18a20d3db7fef1e",
  "nextblockhash": "000002ae2176c9ed5728f7816b26c9887a1f83d2cd3c820d70016e89851e3af2"
}
```

```
$ bitcoin-cli getblockheader <block hash> false
```

```
000000201ca9d4c086746e68cfbb7a27d44734ff9cb35412f1ad94332a50ff2691010
000a5497a5c64266cee635fb1789d6e617ccb41addd538bec854971f843a6f24b8cdb
d31f67ae77031e2a963200
```

Qual versão do cabeçalho do bloco é efetivamente transmitido na rede?

Qual é a função da blockchain?

6. Entender as transações

```
$ bitcoin-cli getrawtransaction <txid> 1
```

Quais são os componentes da transação?

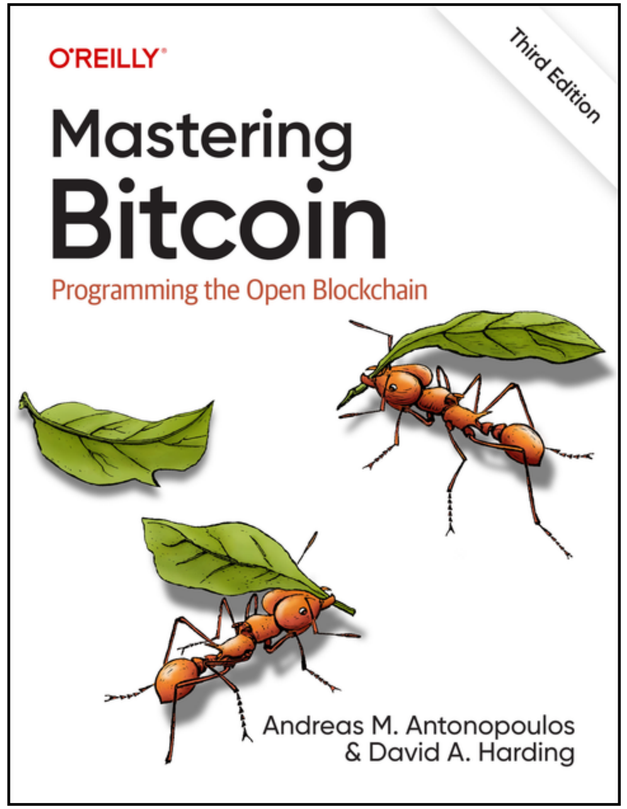
Quais as informações presentes em uma saída de uma transação?

Qual é a função do campo scriptPubKey?

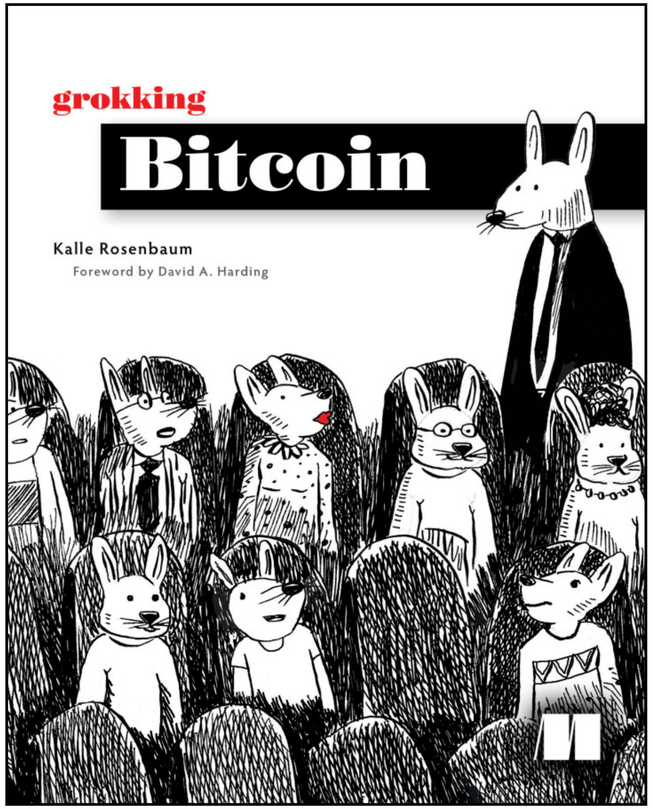
O que é um UTXO?

Quais as informações presentes em uma entrada de uma transação?

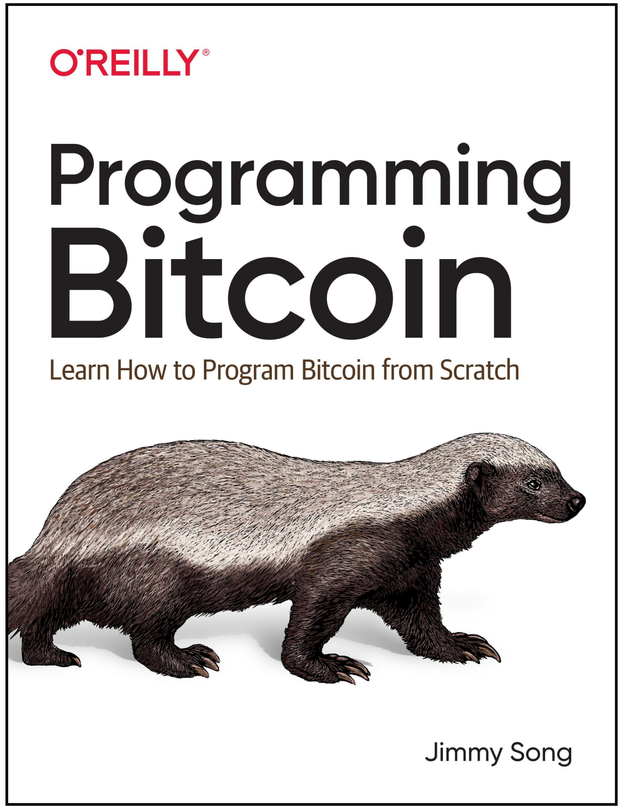
Qual informação não está presente nas transações?



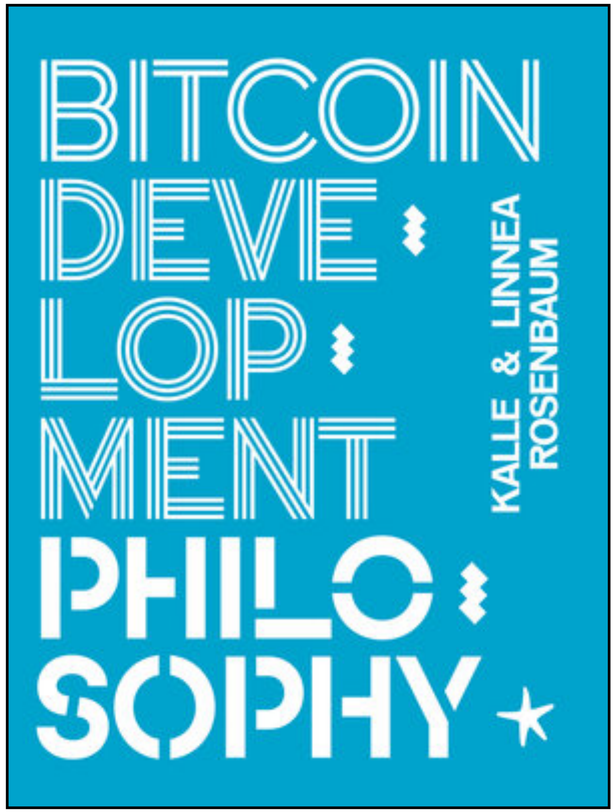
Most comprehensive



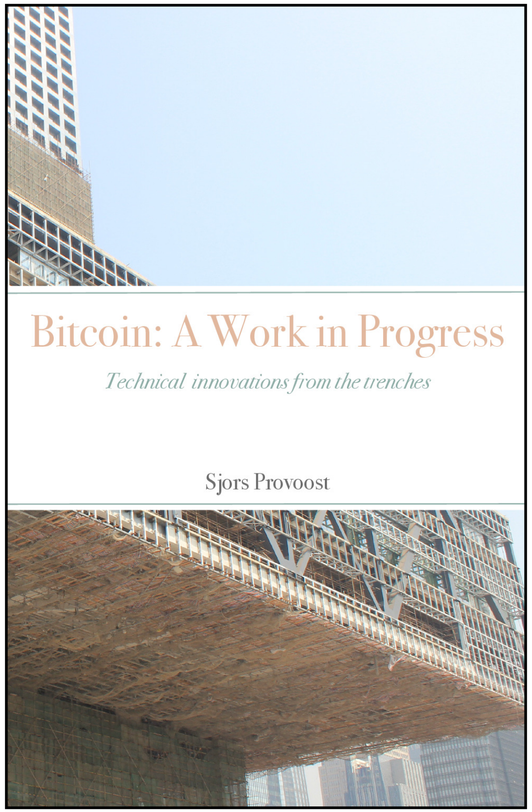
Best pedagogy



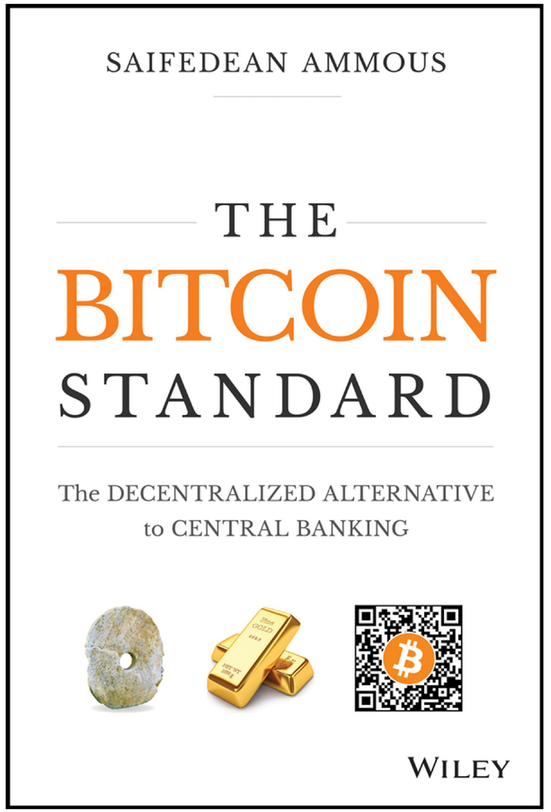
Most hands-on



Bitcoin development ethos



Bitcoin history



Bitcoin economics

Edil Medeiros

Universidade de Brasília

prof@edil.com.br

@edil_medeiros

/@edilmedeiros

edil@nostrplebs.com

Jão Noctus

ZBD

jaonoctus@protonmail.com

PGP 0x782C165A293D6E18

jaonoctus.dev