

# Theory of Blockchain

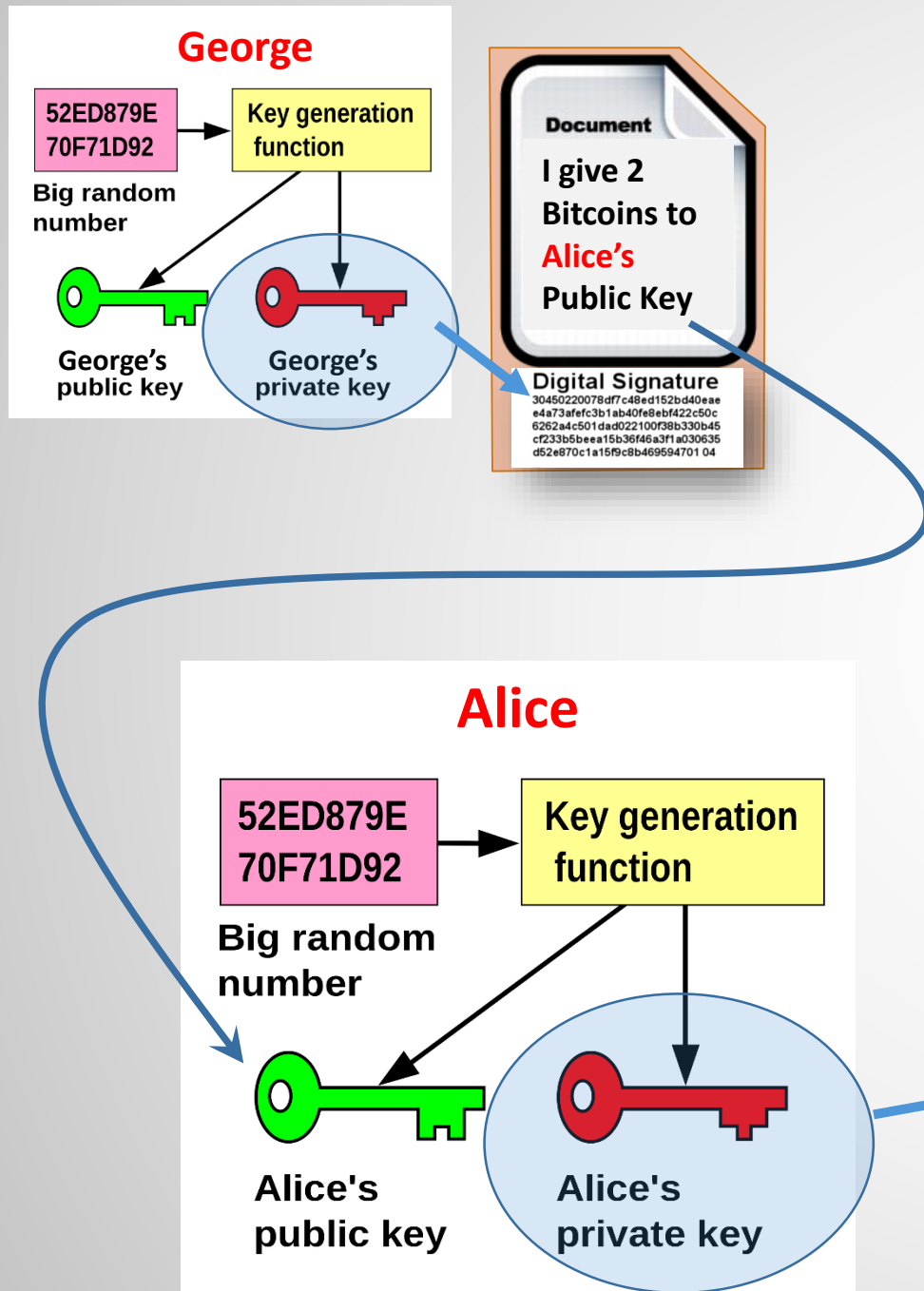


## Session 7:

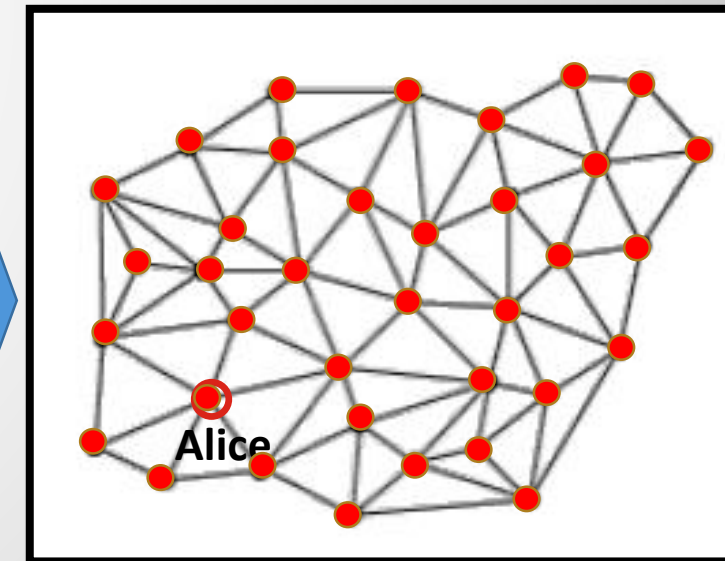
### Bitcoin – Part 2

#### Module 1 – Transaction Details & Anonymity in Bitcoin

# How the Transactions are Protected by Key Pairs and Digital Signature

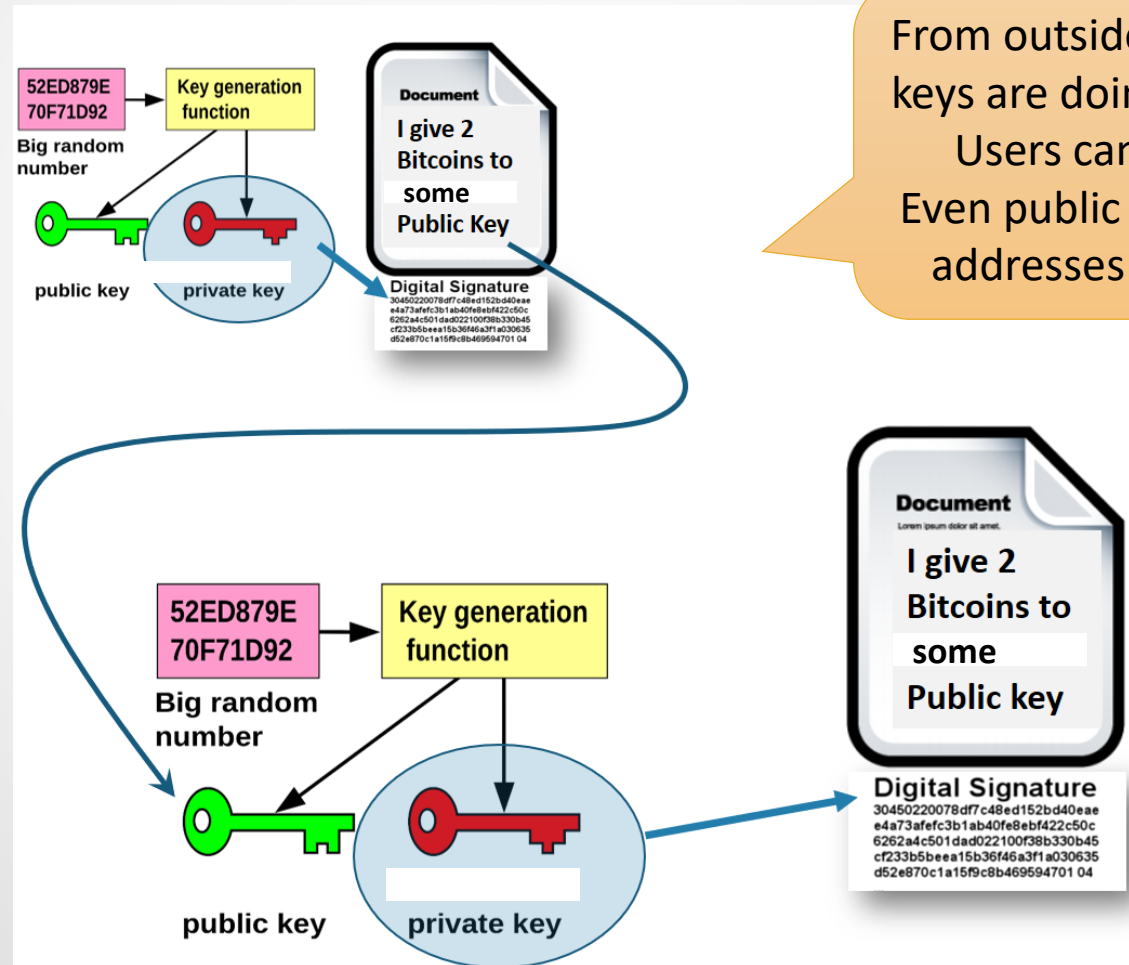


Everyone will know about this transaction then



# Anonymity

Anonymity, in theory, is achieved by not binding the key pairs to their owners' true identity.



From outside, it is as if a bunch of public keys are doing business with each other. Users can have multiple key pairs. Even public keys are turned into Bitcoin addresses by hashing as we will see.



# A Real Bitcoin Transaction

Blockchain.com

Search Blockchain, Transactions, Addresses and Blocks

USD 1,846.54 ▲1.47%    Arbitrum/USD 1.16 ▲3.56%    OKB/USD 46.03 ▲0.37%    Solana/USD 19.94 ▲1.06%    Dogecoin/USD 0.07 ▼0.74%    Polygon/USD 0.88 ▲1.14%    Aptos/USD 8.35 ▲2.40%

Sponsored: Win up to 5 BTC Everyday! Live casino + 20k slots [Play Now](#)

**Bitcoin BTC**  
\$27,139.13 +0.37% 100.44

“We should have a gentleman's agreement to postpone the GPU arms race as long as we can for the good of the network. It's much easier to get new users ...” [\(Read More\)](#)

Satoshi Nakamoto  
Bitcoin Talk • Dec 2009

520,366 Transactions • 6.02 TPs    \$2,583,993,008 Sent Today

791,079 Blocks • Last 43m53s    374.40 EH/s Network Hashrate

482.00 GB Blockchain Size    559,902 Unique Addresses 24 Hr

**Latest Blocks**  
Bitcoin

- 791,078  
23 May 2023 • 09:16:23 GMT+3:30  
2,953 Txs • 1.90 Mb
- 791,077  
23 May 2023 • 09:12:34 GMT+3:30  
3,104 Txs • 1.67 Mb
- 791,076  
23 May 2023 • 08:52:18 GMT+3:30  
2,620 Txs • 1.56 Mb
- 791,075 • Antpool  
23 May 2023 • 08:46:53 GMT+3:30  
3,309 Txs • 1.76 Mb
- 791,074  
23 May 2023 • 08:38:11 GMT+3:30  
3,363 Txs • 1.48 Mb

**Prices**  
Market Cap

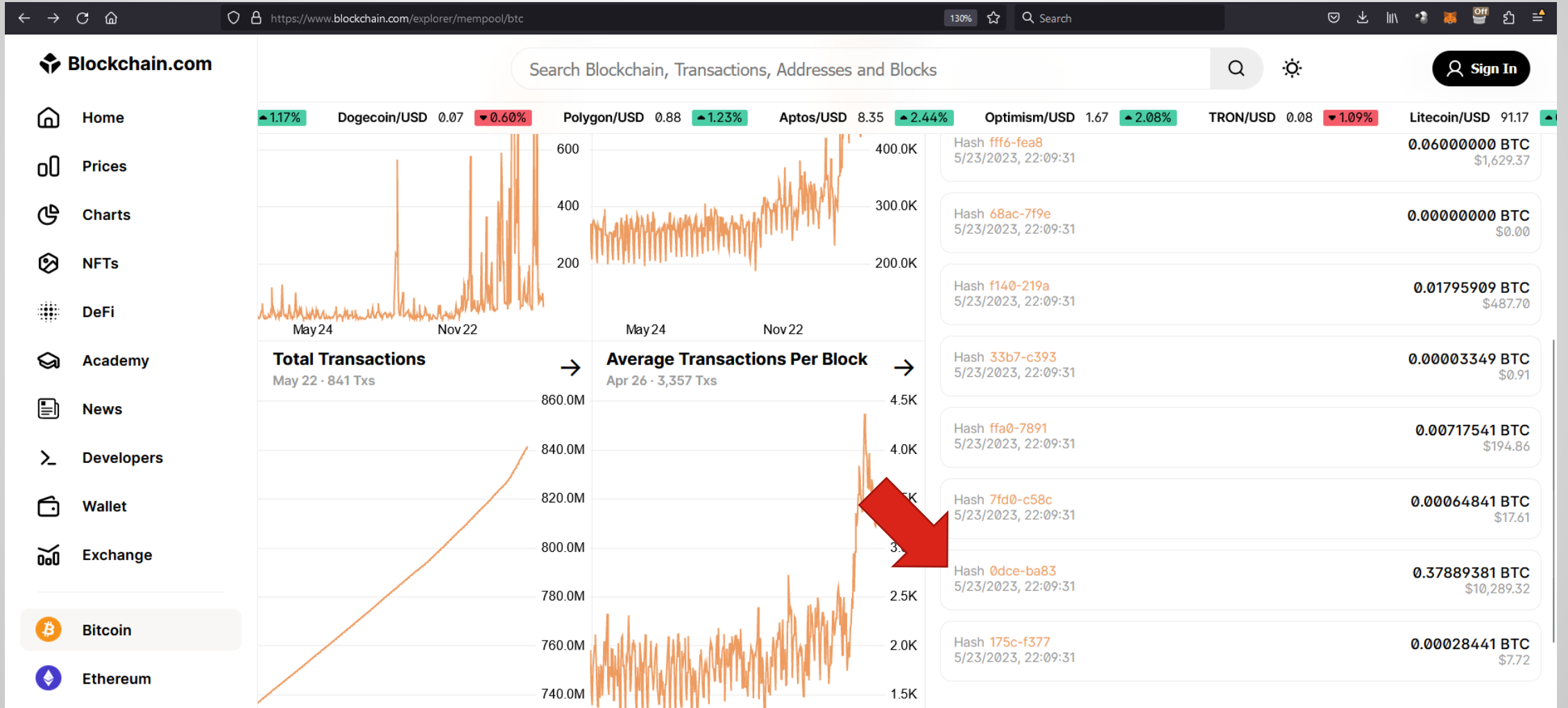
Bitcoin BTC \$27,152.52 +1.00% [Trade](#)

**Latest Transactions**  
Bitcoin

5c557-222ff 22:00:06 0.00 BTC \$0.00

**Bitcoin Cash BCH**  
\$115.06 -1.19% -1.39

# A Real Bitcoin Transaction



# A Real Bitcoin Transaction

Blockchain.com

Home

Prices

Charts

NFTs

DeFi

Academy

News

Developers

Wallet

Exchange

Bitcoin

Ethereum

Bitcoin Cash

BTC Testnet

Search Blockchain, Transactions, Addresses and Blocks

Search

Sign In

Tether/USD 1.00 ▲ 0.00%

Binance Coin/USD 309.64 ▼ 0.46%

XRP/USD 0.47 ▲ 0.82%

USD Coin/USD 1.00 ▼ 0.0100%

Cardano/USD 0.37 ▼ 1.47%

Staked Ether/USD

Sponsored: Win up to 10 BTC! VPN Friendly & NO KYC Casino [Play Now](#)

Play Slots & Win!

Claim Free Lottery Ticket

TX

USD

## Bitcoin Transaction

Broadcasted on 23 May 2023 10:09:35 GMT+3:30

**Hash ID**  
0dce17094e1a7406815fc193ccfd3f47e2eb603d3b61151e4a1b538795aba83

Amount

0.37889381 BTC • \$0.00

Fee

6,464 SATS • \$0.00

From

bc1qh-kt224

To

2 Outputs

Pending

✓

This transaction is efficient, no issues detected.

Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	4m 11s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
Fee	0.00006464 BTC	Output Value	0.37889381 BTC
Fee/VB	\$0.00	Fee/B	29.117 sat/B
Weight	561	Size	222 Bytes
Coinbase	No	Weight Unit	11.522 sat/WU
RBF	No	Witness	Yes
Version	1	Locktime	0

Overview

JSON

# A Real Bitcoin Transaction

The screenshot shows a Bitcoin transaction on the Blockchain.com explorer. The transaction ID is `0dce17094e1a7406815fc193ccfd3f47e2eb603d3b61151e4a1b538795aba83`. The transaction is currently **Pending**. A calculator overlay shows the calculation  $0.37895845 - 0.0044424 - 0.37445141 = 0.00006464$ , with a red arrow pointing from the result to the 'Fee' field in the transaction details.

**Transaction Summary:**

- Amount:** 0.37889381 BTC • \$0.00
- Fee:** 6,464 SATS • \$0.00
- From:** bc1qh-kt224
- To:** 2 Outputs

**Advanced Details:**

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	25m 39s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
Fee	0.00006464 BTC	Output Value	0.37889381 BTC
Fee/VB	45.844 sat/vByte	Fee/B	29.117 sat/B
Weight	561	Size	222 Bytes
Coinbase	No	Weight Unit	11.522 sat/WU
RBF	No	Witness	Yes
Version	1	Locktime	0

**From:** 1 bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt... 0.37895845 BTC • \$0.00

**To:**

- 1 bc1qm4tlaq44hpwgkqrsd7hnfx7v6w0456vr8077r 0.00444240 BTC • \$0.00
- 2 bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224 0.37445141 BTC • \$0.00

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffdf3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```



# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccff3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Hash of this TX = TXID

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccff3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Size of this TX (bytes)

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Version of the protocol used  
(1.0 for now)

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccff3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Time/Block index after which the output can be spent. Zero means there is no time lock.



# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccff3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Transaction fee that goes to the miner who puts this TX in a block.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffdf3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpwgkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

This is not the first transaction in the block and is not meant to award the miner the block reward.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,

  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fh98aef030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],

  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],

  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Hash of the transaction (TX ID) whose output is providing the input funds for this transaction.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffdf3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,

  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],

  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],

  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Usually specifies the relative number of blocks or the time duration that must elapse before the input can be considered for spending. Also has use cases in combination with RBF.



# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuytksku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuytksku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

scriptPubKey, is the script that defines the spending conditions or locking script of the previous transaction output.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,

  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60f",
      "value": 37895845,
      "address": "bc1qh4s0h",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee590220",
        "1bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],

  "outputs": [
    {
      "address": "bc1qmk4ttag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],

  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

The amount to be taken from the input (in Satoshi, which is 1/100.000.000 of BTC). You must take all of it, but you may return the change to yourself.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,

  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkv",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],

  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],

  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Address/Hash of the public key (from the previous transaction) to which money had gone. It is now providing money to this transaction as the input.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffdf3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d2f1bb47e5dba55cba2280d17893c548ed67177f02119c966a2ee8459c385a1f28ee1e496",
        ""
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

Elliptic Curve Digital Signature of the owner of the money in the previous transaction. The money had actually gone to his public key. Now he proves the money is his by signing this transaction by his corresponding private key.



# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpwgkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuayts",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

This transaction has two outputs. 444240 Satoshis (0.0044240 BTC ) go to the first address, and 37445141 Satoshis go to the second address, which is actually the address of the sender himself. This is the change. The remaining is the transaction fee.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffdf3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,

  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],

  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],

  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

The "pkscript" field contains the hexadecimal representation of the locking script or public key script associated with a specific output. This script defines the conditions that must be met to spend the funds locked in that output.

An interpreted version could be:  
OP\_DUP OP\_HASH160[3...2ea] OP\_EQUALVERIFY OP\_CH...ECKSIG

Recipient's Address

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,

  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],

  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014dda1f67151e4a1b538795aba83",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],

  "block": {
    "mempool": 1684867175
  },
  "deleted": false,
  "time": 1684867175,
  "rbf": false,
  "weight": 561
}
```

This output has not been the input of any other transactions yet (not spent yet). This info comes from blockchain.com and not the transaction content.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccff3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175,
    "deleted": false,
    "time": 1684867175,
    "rbf": false,
    "weight": 561
  }
}
```

The "memory pool," is a temporary storage area in each Bitcoin node where valid but unconfirmed transactions are held. When a transaction is broadcasted to the Bitcoin network, it first enters the mempool of the participating nodes. This transaction is young and is not in a block.



# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffd3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175,
    "deleted": false,
    "time": 1684867175,
    "rbf": false,
    "weight": 561
  }
}
```

The "deleted" field is typically used by blockchain explorers or APIs to indicate whether a particular transaction has been deleted or invalidated. A value of "false" means that the transaction is still valid and exists on the blockchain

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

**Summary**

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details			
Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffdf3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,

  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],

  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],

  "block": {
    "mempool": 16,
    "deleted": false,
    "time": 1684867,
    "rbf": false,
    "weight": 561
  }
}
```

Replace-By-Fee (RBF) is a feature in Bitcoin that allows the sender of a transaction to replace it with a new version that includes a higher fee. A "false" value means that the transaction is not marked for potential replacement through RBF.

# A Real Bitcoin Transaction

Metadata

Input(s)

Output(s)

## Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

## Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

```
{
  "txid": "0dce17094e1a7406815fc193ccffdf3f47e2eb603d3b61151e4a1b538795aba83",
  "size": 222,
  "version": 1,
  "locktime": 0,
  "fee": 6464,
  "inputs": [
    {
      "coinbase": false,
      "txid": "9c4364e816d8f6d2c8e57c22f49b7d71a100fb98aefe030f94a9431856e3eb00",
      "output": 1,
      "sigscript": "",
      "sequence": 4294967295,
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37895845,
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "witness": [
        "3044022052a0ae499d680f9e83a92f17d28ad84b9e66c9258ca0707213dadf574f70ee5902201bb47e5dba55cba2280d17893c548ed6717721955757044ec254f304e615d80b01",
        "02119c966a2ee8459c385a1f28ee1e49667a574501741b6018bb9eb3933d02069d"
      ]
    }
  ],
  "outputs": [
    {
      "address": "bc1qmk4tlag44hpgwkqrsd7hnfx7v6w0456vr8077r",
      "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
      "value": 444240,
      "spent": false,
      "spender": null
    },
    {
      "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
      "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
      "value": 37445141,
      "spent": false,
      "spender": null
    }
  ],
  "block": {
    "mempool": 1684867175,
    "deleted": false,
    "time": 1684867175,
    "rbf": false,
    "weight": 561
  }
}
```

The concept of "weight" is specific to SegWit transactions and is used to determine the transaction's size in terms of block space consumption. It is different from the traditional measure of transaction size in bytes. The weight of a transaction is used to calculate the transaction fee based on the amount of block space it consumes

Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

Pending

```
....
"outputs": [
  {
    "address": "bc1qmk4ttag44hpwgkqrsd7hnfx7v6w0456vr8077r",
    "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
    "value": 444240,
    "spent": false,
    "spender": null
  },
  {
    "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
    "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
    "value": 37445141,
    "spent": false,
    "spender": null
  }
],
"block": {
  "mempool": 1684867175
},
"deleted": false,
"time": 1684867175,
"rbf": false,
"weight": 561
}
```

Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. The transaction currently has 131 confirmations on the network. The current value of this transaction is now \$0.00.

Advanced Details

Hash	0dce-ba83	Block ID	791,082
Position	2194	Time	23 May 2023 10:09:35
Age	1d 1h 52m 43s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

Confirmed

```
....
"outputs": [
  {
    "address": "bc1qmk4ttag44hpwgkqrsd7hnfx7v6w0456vr8077r",
    "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
    "value": 444240,
    "spent": true,
    "spender": {
      "txid": "a289b4aba552a3caf5c7ec64470f96c6c33ea6b24d6a6e82b11b1fd9c3c8fc0",
      "input": 0
    }
  },
  {
    "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
    "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
    "value": 37445141,
    "spent": true,
    "spender": {
      "txid": "3635d5d01c1e4d...",
      "input": 0
    }
  }
],
"block": {
  "height": 791082,
  "position": 2194
},
"deleted": false,
"time": 1684867171,
"rbf": false,
"weight": 561
}
```

Block height represents the position of a block within the blockchain. The first block, also known as the genesis block, has a block height of 0, and each subsequent block increases the height by 1.

Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

Pending

```
....
"outputs": [
  {
    "address": "bc1qmk4tlag44hpwgkqrsd7hnfx7v6w0456vr8077r",
    "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
    "value": 444240,
    "spent": false,
    "spender": null
  },
  {
    "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
    "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
    "value": 37445141,
    "spent": false,
    "spender": null
  }
],
"block": {
  "mempool": 1684867175
},
"deleted": false,
"time": 1684867175,
"rbf": false,
"weight": 561
}
```

Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. The transaction currently has 131 confirmations on the network. The current value of this transaction is now \$0.00.

Advanced Details

Hash	0dce-ba83	Block ID	791,082
Position	2194	Time	23 May 2023 10:09:35
Age	1d 1h 52m 43s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

Confirmed

```
....
"outputs": [
  {
    "address": "bc1qmk4tlag44hpwgkqrsd7hnfx7v6w0456vr8077r",
    "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
    "value": 444240,
    "spent": true,
    "spender": {
      "txid": "a289b4aba552a3caf5c7ec64470f96c6c33ea6b24d6a6e82b811b1fd9c3c8fc0",
      "input": 0
    }
  },
  {
    "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
    "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
    "value": 37445141,
    "spent": true,
    "spender": {
      "txid": "3635d5d01c1e4dbf9f19493c56af128f76fb57a588d734943a1a7a02a5427380",
      "input": 0
    }
  }
],
"block": {
  "height": 791082,
  "position": 2194
},
"deleted": false,
"time": 1684867171,
"rbf": false,
"weight": 561
}
```

Position of the transaction in the block.

Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. This transaction is unconfirmed. The current value of this transaction is now \$0.00.

Advanced Details

Hash	0dce-ba83	Time	23 May 2023 10:09:35
Age	35m 19s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

Pending

```
....
"outputs": [
  {
    "address": "bc1qmk4tlag44hpwgkqrsd7hnfx7v6w0456vr8077r",
    "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
    "value": 444240,
    "spent": false,
    "spender": null
  },
  {
    "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
    "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
    "value": 37445141,
    "spent": false,
    "spender": null
  }
],
"block": {
  "mempool": 1684867175
},
"deleted": false,
"time": 1684867175,
"rbf": false,
"weight": 561
}
```

Summary

This transaction was first broadcasted on the Bitcoin network on May 23, 2023 at 10:05 AM GMT+3:30. The transaction currently has 131 confirmations on the network. The current value of this transaction is now \$0.00.

Advanced Details

Hash	0dce-ba83	Block ID	791,082
Position	2194	Time	23 May 2023 10:09:45
Age	1d 1h 52m 43s	Inputs	1
Input Value	0.37895845 BTC	Outputs	2
	\$0.00	Output Value	0.37889381 BTC
Fee	0.00006464 BTC		\$0.00
	\$0.00	Fee/B	29.117 sat/B
Fee/VB	45.844 sat/vByte	Size	222 Bytes
Weight	561	Weight Unit	11.522 sat/WU
Coinbase	No	Witness	Yes
RBF	No	Locktime	0
Version	1		

Overview

JSON

Confirmed

```
....
"outputs": [
  {
    "address": "bc1qmk4tlag44hpwgkqrsd7hnfx7v6w0456vr8077r",
    "pkscript": "0014ddaabff515adc2e45803837d79a4de669cfad34c",
    "value": 444240,
    "spent": true,
    "spender": {
      "txid": "a289b4aba552a3caf5c7ec64470f96c6c33ea6b24d6a6e82b11b1fd9c3c8fc0",
      "input": 0
    }
  },
  {
    "address": "bc1qh4s0hm6yls9plpgkvwxm9uuaytsku2ezekt224",
    "pkscript": "0014bd60fbef44fc0a1f8516638db2f39d22e16e2b22",
    "value": 37445141,
    "spent": true,
    "spender": {
      "txid": "3635d5d01c1e4dbf9f19493c56af128f76fb57a588d734943a1a7a02a5427380",
      "input": 0
    }
  }
],
"block": {
  "height": 791082,
  "position": 2194
},
"deleted": false,
"time": 1684867171,
"rbf": false,
"weight": 561
}
```



# Bitcoin Language

- Bitcoin has a language called “Script”.
  - It was inspired by the not-much-known Forth language.
  - It’s a stack-based language.
  - No loops are supported
    - It’s not a Turing-complete Language.
      - Do not expect complex functions to be implemented.
      - The good news is that there is no infinite or long loop problems and therefore, a workaround like Ethereum Gas is not necessary.
- It has 256 instructions (1 byte commands)
  - 15 are disabled, and 75 are reserved.
  - The rest are for cryptographic operations, IF THEN conditions, etc.
- If a transaction script is erroneous, the transaction will be deemed invalid.

# A Few Commonly-used Script Operations

Command	Description
<b>OP_DUP</b>	Copies/duplicates the top item on the stack.
<b>OP_HASH160</b>	Hashes the input two times; first with SHA-256, then with RIPEMD-160.
<b>OP_EQUALVERIFY</b>	Returns TRUE if the inputs are equal, and FALSE (and marks the transaction as invalid) if they are unequal.
<b>OP_CHECKSIG</b>	Checks that the input signature is a valid one using the input public key for the hash of the current transaction.
<b>OP_CHECKMULTISIG</b>	Checks that the k signatures mentioned in the transaction (out of the possible n signatures) are valid (based on the k specified public keys).

# How a Spending Transaction Works

- A spending transaction has a (script) signature in its input. It must be compatible with the output of the transaction it refers to in the input.
- For a payment to be successful, the input script of the spending transaction is put at the beginning of the output of the previous transaction, and it must execute flawlessly.

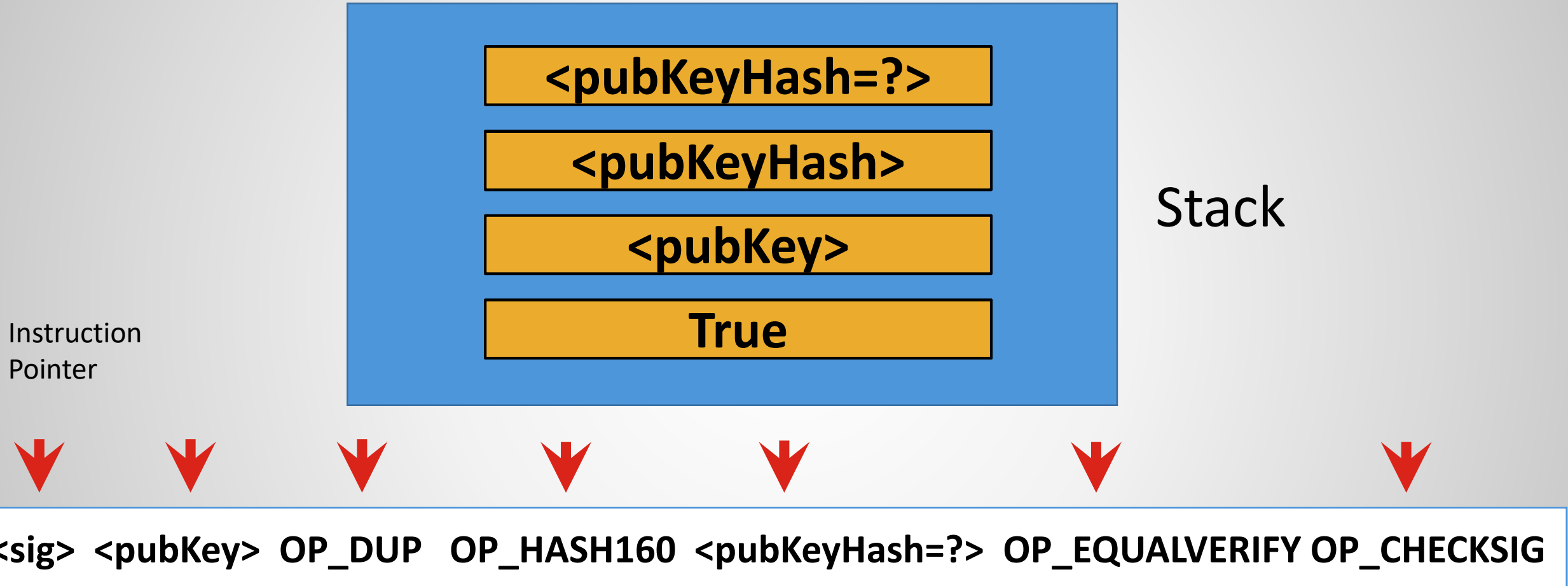
scriptSig

289a948e...  
8813e11b...

scriptPubKey

OP\_DUP  
OP\_HASH160  
392a305e2a...  
OP\_EQUALVERIFY OP\_CHECKSIG

# Bitcoin Language Stack in a Spending Transaction



# Multiple Signature Transaction

- It is possible to create a transaction whose output can be unlocked by the joint signatures of  $k$  out of  $n$  people.
- If  $n$  is the total people involved, and any  $k$  of them decide to unlock the transaction (in the input of another transaction), they issue a transactions with  $k$  signatures (in its input).
- The operation called is `OP_CHECKMULTISIG`.

# Statistics of Transaction Types

- 99.9% of transactions are simple signature checks (with one or more inputs)
- 0.01% are Multi-signature trans.
- 0.01% are Pay-to-Script-Hash
- The rest are erroneous trans., PoB, etc.

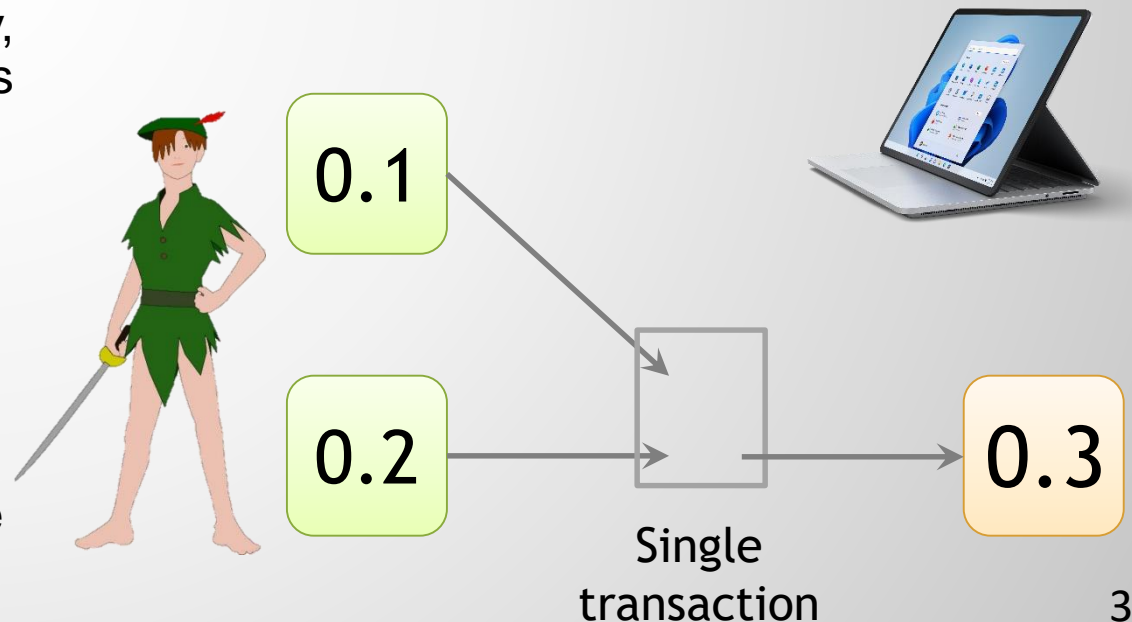


# Back to Anonymity

- A seller only gives the hash of his public key (Bitcoin address) to the buyer.
  - The buyer actually pays the money to the hash of a public key.
  - When the seller wants to spend the money, he/she reveals the public key in the spending transaction and proves owning the money by signing the transaction with the corresponding private key of his/hers.
- The hashing of public key and turning it into the address does not really hide the public key.
  - The first time the user tries to spend the money, the public key is disclosed in the input script of the spending transaction.

# Back to Anonymity

- The user has to spend all the input money in a transaction, but can send part of it back to his/her own address. After that everyone knows his/her public key.
- Creating a pair of public-private keys is very easy. So the user can make a new Bitcoin address and send the change to their new address.
- This might look a way of promoting anonymity, but almost everybody can understand that this new address belongs to the same person.
  - The identity of the person remains detached from the keys though.
- Some try to deanonymize the bitcoin transactions by relying on the fact that the addresses that are put in the input of a single transaction most probably belong to the same person.



# Back to Anonymity

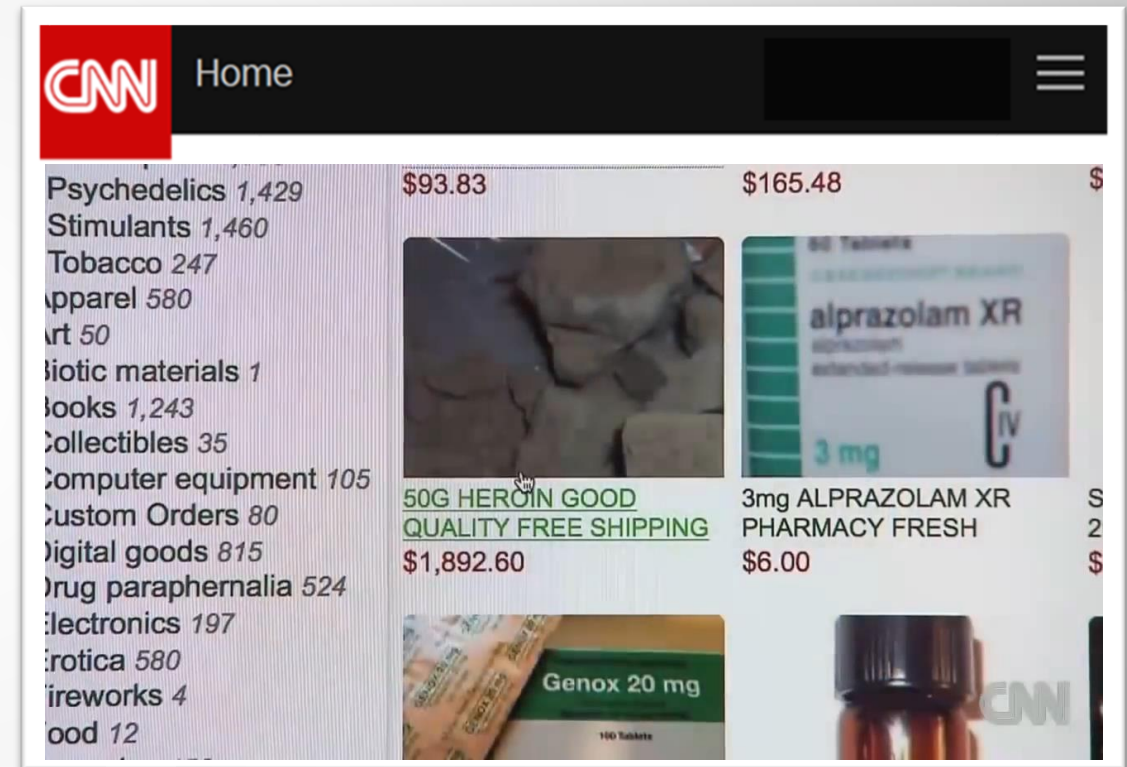
- Identity leakage could happen because source IP address of the packet submitting a new transaction to the network can potentially lead to identity of the user.
  - But if he/she hides behind e.g. TOR, nothing but the public key will be disclosed.



**TOR Anonymizing Network**  
(uses Diffie-Hellman key establishment)


# You Remember this? (Silk Road behind TOR)

- Silk Road was one of the first online black markets that used Bitcoin and TOR technologies for anonymity.
- Silk Road was shut down in 2013 and the admin (Ross Ulbricht) was arrested. He was sentenced to life in prison!
- Not all the credit for Bitcoin's fame goes to Silk Road. The 2017's price surge was also a big shot.





# Usage example: Anonymous p2p spending !

**Silk Road**  
anonymous market

messages 1 | orders 0 | account ₮0.00

Search

Go

Shop by Category

Drugs 2,399

- Cannabis 341
- Dissociatives 65
- Ecstasy 209
- Opioids 156
- Other 144
- Precursors 12
- Prescription 526
- Psychedelics 427
- Stimulants 273

Apparel 114

Art 7

Books 743

Collectibles 12

Computer equipment 19

Custom Orders 26

Digital goods 310

Drug paraphernalia 89

Electronics 20

Erotica 319

Fireworks 2

Food 3

Forgeries 58

Hardware 2


Home & Garden 7

Jewelry 48


Lab Supplies 5

Lotteries & games 29


Medical 5



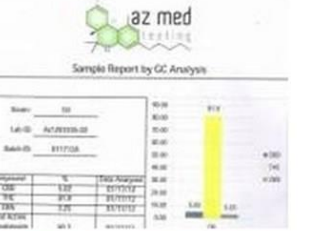
5x - 10mg Dexedrine (Pure Dextroamphetamine)  
₮4.94




2 x 0,25 mg Xanax (Alprazolam)  
₮1.50




Malana charas hand rubbed Indian hash 100g  
₮75.83




1 Gram OG KUSH OIL 81% THC 90% TOTAL  
₮4.13




14 grams (1/2 Ounce) of Nebula JWH-122  
₮2.63




3.5g Crystal Meth Ice Shards  
₮31.92




20 x 25mg Cialis  
₮2.57




!!!!...Psilocybe-Cubensis-Chocolate...!!!!  
₮18.15




100 x Orange Star Very high MDMA content 180mg



100x 200mg White XTC 'Speakers'



3g Methylone Crystals - \$50- Lab Grade



15mg Adderall Extended Release (1 Capsule)

# What Comes Next ...

- We saw how transactions are created and processed on Bitcoin network in detail.
- We learned to what extent anonymity is preserved in the Bitcoin network.
- In the next video, we explain P2SH and P2PKH payment types.



