https://api.blockcypher.com/v1/btc/test3/txs/1a66ddebd10d0d5c102339cf12955934dc60983cf760a111653c8aba0e6dac3b?limit=50&includeHex=true


```
{
  "block_hash": "00000000000001130b6a930f2c2e8a73245a1b003d041d4dec1a5bf25829d3d5",
  "block_height": 1291743,
  "block_index": 28,
  "hash": "1a66ddebd10d0d5c102339cf12955934dc60983cf760a111653c8aba0e6dac3b",
  "hex":
"01000000000101f25dfc56936144da4a9945deedb1c7187af1154cc7ccb2ed46f2579d2920f32d0100000017
063eb1491e62f55aa557b375570895299b9913a65a62d87f30c0bd57c5815a1e20121033249de4fdc2136e03d
3bd6fb82c1661aa771736f66a6bd5cd2126b75e7fb1bcb00000000",
  "addresses": [
    "2N4LexNz2Zi9fd7zVso9K6FJDc9qp54QHDV",
    "2N7RG7xSagE2PJojH6zmZw75Jtb5Udjr5mY",
    "mfhfG8BiHjMzmJoyeXavTUmSUxRAdpQ7Ce"
  ],
  "total": 3299974077,
  "fees": 100000,
  "size": 140,
  "preference": "high",
  "relayed_by": "35.195.234.115:18333",
  "confirmed": "2018-04-06T17:28:40Z",
  "received": "2018-04-06T17:03:32.156Z",
  "ver": 1,
  "double_spend": false,
  "vin_sz": 1,
  "vout_sz": 2,
  "confirmations": 81,
  "confidence": 1,
  "inputs": [
    {
      "prev_hash": "2df320299d57f246edb2ccc74c15f17a18c7b1edde45994ada44619356fc5df2",
      "output_index": 1,
      "script": "160014d89caca364d629e48bad455043ec66ad69a78356",
      "output_value": 3300074077,
      "sequence": 4294967295,
      "addresses": [
        "2N4LexNz2Zi9fd7zVso9K6FJDc9qp54QHDV"
      ],
      "script_type": "pay-to-script-hash",
      "age": 1291713,
      "witness": [

"30440220669c2be6ad33b50ea76e7ded69cd6ad69cffdbef13c00ea124abb01a1645f9e8022063eb1491e62f
55aa557b375570895299b9913a65a62d87f30c0bd57c5815a1e201",
        "033249de4fdc2136e03d3bd6fb82c1661aa771736f66a6bd5cd2126b75e7fb1bcb"
      ]
    }
  ],
  "outputs": [
    {
      "value": 32500000,
      "script": "76a91402065b5f8beeb44df3f4c91804a2e012a5ae04ea88ac",
      "spent_by": "0e34e3bd9da5c89ba993682bbcb7eabc9381f41377ac6d1470874ff1c2b0b0d2",
      "addresses": [
        "mfhfG8BiHjMzmJoyeXavTUmSUxRAdpQ7Ce"
      ],
      "script_type": "pay-to-pubkey-hash"
    },
    {
      "value": 3267474077,
      "script": "a9149b77b3564f89161f685a2765410b20139700c36387",
      "spent_by": "52a6d4903cd534b1902fdbe3073b5c983a2f59a5d48dff6211b39fdf5b1bac02",
      "addresses": [
        "2N7RG7xSagE2PJojH6zmZw75Jtb5Udjr5mY"
      ],
      "script_type": "pay-to-script-hash"
    }
  ]
}
```

https://en.bitcoin.it/wiki/Transaction

Pay-to-PubkeyHash

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubKey>
```

Pay-to-Script-Hash

```
scriptPubKey: OP_HASH160 <scriptHash> OP_EQUAL
scriptSig: ..signatures... <serialized script>

m-of-n multi-signature transaction:
scriptSig: 0 <sig1> ... <script>
script: OP_m <pubKey1> ... OP_n OP_CHECKMULTISIG
```

Principle example of a Bitcoin transaction with 1 input and 1 output only

Data

```
Input:
Previous tx:
f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig:
304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b24150
1

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

Explanation

The input in this transaction imports 50 BTC from output #0 in transaction f5d8... Then the output sends 50 BTC to a Bitcoin address (expressed here in hexadecimal 4043... instead of the normal base58). When the recipient wants to spend this money, he will reference output #0 of this transaction in an input of his own transaction.

Address

- Has `scriptPubKey`
- Spender has to provide, `scriptSig`

`Encoding check websites`

https://en.bitcoin.it/wiki/Address

https://en.bitcoin.it/wiki/Base58Check_encoding

BIP

WIF

https://en.bitcoin.it/wiki/Wallet_import_format

`Private-key, Public-key`

https://en.bitcoin.it/wiki/Secp256k1

secp256k1 refers to the parameters of the ECDSA curve used in Bitcoin, and is defined in *Standards for Efficient Cryptography (SEC)*

https://pascalpares.gitbooks.io/implementation-of-the-bitcoin-system/1-blockchain.html

https://www.blockcypher.com/quickstart/

```
# get a couple transactions from a known address (supposedly Silk Road)

$ curl
https://api.blockcypher.com/v1/btc/main/addrs/1rundZJCMJhUiWQNFS5uT3BvisBuLx
kAp?limit=2

# get one of the two transactions (a big one)

$ curl
https://api.blockcypher.com/v1/btc/main/txs/a40c283de4c26b027a5734ff89ce78ad
e1220fc313befa107ec6c245c24bdec0

# retrieve the block it was included in by height

$ curl https://api.blockcypher.com/v1/btc/main/blocks/319957
```

testnet explorer

https://live.blockcypher.com/bcy/

https://live.blockcypher.com/btc-testnet/

https://testnet.manu.backend.hamburg/faucet

https://live.blockcypher.com/bcy/pushtx/

Sample to work and understand

```
bitcoin = require('bitcoinjs-lib');


function rng () { return Buffer.from('zzzttyyzzzzzzzzzzzzzzzzzzuuuzzz') }




var keyPair = bitcoin.ECPair.makeRandom({ network: bitcoin.networks.testnet,
rng: rng })


console.log(keyPair.toWIF());


var key = bitcoin.ECPair.fromWIF(

'cRgnQe1TQngWfnsLo9YUExBjx3iVKNHu2ZfiRcUivATuojDdzdus',

 bitcoin.networks.testnet);


console.log(key.getAddress());

console.log(key.getPublicKeyBuffer().toString('hex'));

var tx = new bitcoin.TransactionBuilder(bitcoin.networks.testnet);

tx.addInput("1a66ddebd10d0d5c102339cf12955934dc60983cf760a111653c8aba0e6dac3
b", 0);

tx.addOutput("mfhfG8BiHjMzmJoyeXavTUmSUxRAdpQ7Ce", 32489000);

tx.sign(0, key);

console.log(tx.build().toHex());
```

Wep app authentication

Explain concept

Working sample

Sample to use bitcoin-js lib 2.3

Testcase samples

https://github.com/bitcoinjs/bitcoinjs-lib/blob/master/test/integration/transactions.js#L115

Sigwit?

Errors

{"txid":"d18e7106e5492baf8f3929d2d573d27d89277f3825d3836aa86ea1d843b5158b","version":1,"locktime":0,"vin":

[{"txid":"5146ef36306b376497aa788ff744024ed831955d1a4ef1dc69971f2aecac581d","vout":1,"sequence":4294967295,"n":0,"scriptSig":
{"hex":"483045022100b580e429ec101453d7a8fb0ca12f778803561a09290112af3f3a9fb47c8449d0022041b7e14792c36d25d023f475df3b3bd50e4adb1ce92d5b9a05471e16db93cb9e012103836681a1e5beb2cd8864961b1de582952efc4a09325c11216b7d10734276637c","asm":"304502210 0b580e429ec101453d7a8fb0ca12f778803561a09290112af3f3a9fb47c8449d0022041b7e14792c 36d25d023f475df3b3bd50e4adb1ce92d5b9a05471e16db93cb9e[ALL] 03836681a1e5beb2cd8864961b1de582952efc4a09325c11216b7d10734276637c"},"addr":"1EvQUoukdKY5Fw3mqAx5AnaM4qogB5k6qZ","valueSat":6341355,"value":0.06341355,"doubleSpentTxID":null}],

"vout":[{"value":"0.06181355","n":0,"scriptPubKey":
{"hex":"76a914e424b522d5e5f8509e53bf17d254b63b25f1024388ac","asm":"OP_DUP OP_HASH160 e424b522d5e5f8509e53bf17d254b63b25f10243 OP_EQUALVERIFY OP_CHECKSIG",
"addresses":["1MoK3Dxtrk3QD96oraWTCjbzwXjtHHe9h1"],"type":"pubkeyhash"},
"spentTxId":"018cb1267d8dbec24a004b1d1d2601eac5d1b0b9ba8df783ad935f662469615d","spentIndex":0,"spentHeight":344729},
{"value":"0.00150000","n":1,"scriptPubKey":
{"hex":"76a914496dbfb76f2677792da9586f7cf407bf303b58a088ac","asm":"OP_DUP OP_HASH160 496dbfb76f2677792da9586f7cf407bf303b58a0 OP_EQUALVERIFY OP_CHECKSIG",
"addresses":
["17hFoVScNKVDfDTT6vVhjYwvCu6iDEiXC4"],"type":"pubkeyhash"},"spentTxId":"18f873da171be1d0c2518399eccbea889afbe1e5c4863a2dd1985d311bd6b288","spentIndex":0,"spentHeight":338044}],"blockhash":"000000000000000001961aebab0608488fb143ca38fd52e7b4a2237651dee2cf2","blockheight":338041,"confirmations":178939,"time":1420716305,"blocktime":1420716305,"valueOut":0.06331355,"size":226,"valueIn":0.06341355,"fees":0.0001}

https://medium.com/@orweinberger/how-to-create-a-raw-transaction-using-bitcoinjs-lib-1347a502a3a