



We've seen transactions stored on the blockchain by their Transaction Hash.

BLOCKCYPHER

BTC ▾Address, transaction or block

 ▾

Bitcoin Transaction

b138360800cdc72248c3ca8dfd06de85913d1aac7f41b4fa54eb1f5a4a379081

AMOUNT TRANSACTED

0.02564198 BTC

FEES

0.0001 BTC

RECEIVED

🕒 3 years ago

CONFIRMATIONS ⓘ

🔒 6+

Advanced Details ▾

Details

1 Input Consumed

0.02574198 BTC from
1PZF16YWmuT37Hv5y7zSxdRSwisrwdKpak (output)

...

2 Outputs Created

0.015 BTC to
1EoxGLjv4ZADtRBJTVeXY35czVyDdp7rU4 (spent)

0.01064198 BTC to
1PZF16YWmuT37Hv5y7zSxdRSwisrwdKpak (unspent)

Estimated Value Sent : 0.015 BTC (more)

Transactions in the bitcoin blockchain are stored in a double-hashed form.

This means the raw transaction was put through SHA256 twice to get the Transaction hash we see on the blockchain.

Bitcoin Transaction Hash

SHA256(SHA256(Raw Transaction)) =
Transaction Hash

For example, a transaction with this

*hash:*b138360800cdc72248c3ca8dfd06de85913d1aac7f41b4fa54eb1f5a4a379081

Transaction in the bitcoin blockchain are stored in a double-hashed form: SHA256(SHA256(01000...)) =
b138360800cdc72248c3ca8dfd06de85913d1aac7f41b4fa54eb1f5a4a379081

Bitcoin Transaction Hash

SHA256(SHA256(Raw Transaction)) =

b138360800cdc72248c3ca8dfd06de85913d1a
ac7f41b4fa54eb1f5a4a379081

Given the raw transaction, we were able to see more details about the Transaction Data model.

Transaction Data Model

- Version
- Input Count
- Input Info
- Output Count
- Output Info
- Locktime

```
0100000001f3f6a909f8521adb57d898d29858
34e632374e770fd9e2b98656f1bf1fd42701
0000006b48304502203a776322ebf8eb8b58cc
6ced4f2574f4c73aa664edce0b0022690f2f6f
47c521022100b82353305988cb0ebd443089a1
73ceec93fe4dbfe98d74419ecc84a6a698e31d
012103c5c1bc61f60ce3d6223a63cedbece03b
12ef9f0068f2f3c4a7e7f06c523c3664ffffff
ff0260e31600000000001976a914977ae6e323
49b99b72196cb62b5ef37329ed81b488ac063d
1000000000001976a914f76bc4190f3d8e2315
e5c11c59cfc8be9df747e388ac00000000
```

We discussed that inside the Input Information section and Output Information section there's data about an Unlocking Script and Locking Script, respectively.

What we didn't mention is that there's a little bit more than that inside each of these sections. Let's see what else is contained here.

Transaction Data Model

- Input Info
 - Unlocking Script



- Output Info
 - Locking Script



```
0100000001f3f6a909f8521adb57d898d29858
34e632374e770fd9e2b98656f1bf1fd42701
0000006b48304502203a776322ebf8eb8b58cc
6ced4f2574f4c73aa664edce0b0022690f2f6f
47c521022100b82353305988cb0ebd443089a1
73ceec93fe4dbfe98d74419ecc84a6a698e31d
012103c5c1bc61f60ce3d6223a63cedbece03b
12ef9f0068f2f3c4a7e7f06c523c3664ffffff
ff0260e31600000000001976a914977ae6e323
49b99b72196cb62b5ef37329ed81b488ac063d
1000000000001976a914f76bc4190f3d8e2315
e5c11c59cfc8be9df747e388ac00000000
```

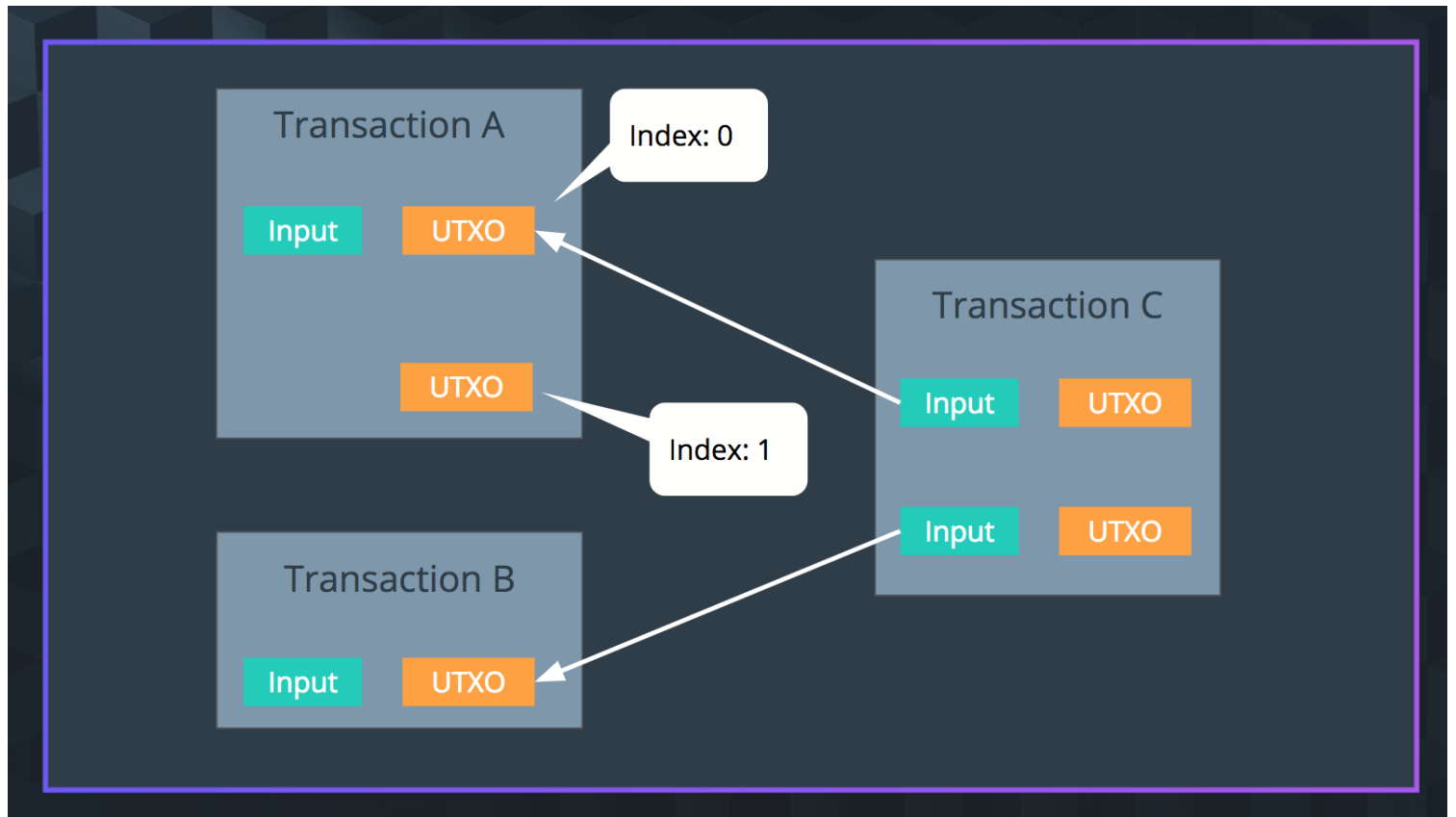
The input information section contains these pieces of data:

- **Previous output hash** - All inputs reference back to an output (UTXO). This points back to the transaction containing the UTXO that will be spent in this input. The hash value of this UTXO is saved in reverse order here.
- **Previous output index** - A transaction may have more than one UTXO which are referenced by their index number. The first index is 0.
- **Unlocking Script Size** - This is the size of the Unlocking Script in bytes.
- **Unlocking Script** - This is the hash of the Unlocking Script that fulfills the conditions of the UTXO Locking Script.
- **Sequence Number** - This is a deprecated feature of bitcoin Currently set to ffffffff by default.

Transaction Data Model

- **Input Info**
 - Transaction hash (reversed)
 - Previous output index
 - Unlocking Script Size (bytes)
 - Unlocking Script
 - Sequence Number

```
0100000001f3f6a909f8521adb57d898d29858
34e632374e770fd9e2b98656f1bf1fd42701
0000006b48304502203a776322ebf8eb8b58cc
6ced4f2574f4c73aa664edce0b0022690f2f6f
47c521022100b82353305988cb0ebd443089a1
73ceec93fe4dbfe98d74419ecc84a6a698e31d
012103c5c1bc61f60ce3d6223a63cedbece03b
12ef9f0068f2f3c4a7e7f06c523c3664ffffff
ff0260e31600000000001976a914977ae6e323
49b99b72196cb62b5ef37329ed81b488ac063d
1000000000001976a914f76bc4190f3d8e2315
e5c11c59cfc8be9df747e388ac00000000
```



Similarly, here's the data stored in the Transaction Output Information:

- **Amount** - The amount of Bitcoin outputted in Satoshis (the smallest bitcoin unit). 10^8 Satoshis = 1 Bitcoin.
- **Locking Script Size** - This is the size of the Locking Script in bytes.
- **Locking Script** - This is the hash of the Locking Script that specifies the conditions that must be met to spend this output.

Transaction Data Model

- **Output Info**
 - Amount
 - Locking Script Size
 - Locking Script

```
0100000001f3f6a909f8521adb57d898d29858
34e632374e770fd9e2b98656f1bf1fd42701
0000006b48304502203a776322ebf8eb8b58cc
6ced4f2574f4c73aa664edce0b0022690f2f6f
47c521022100b82353305988cb0ebd443089a1
73ceec93fe4dbfe98d74419ecc84a6a698e31d
012103c5c1bc61f60ce3d6223a63cedbece03b
12ef9f0068f2f3c4a7e7f06c523c3664ffffff
ff0260e31600000000001976a914977ae6e323
49b99b72196cb62b5ef37329ed81b488ac063d
1000000000001976a914f76bc4190f3d8e2315
e5c11c59cfc8be9df747e388ac00000000
```

Here is the full breakdown of the raw transaction:

Version		01000000
Input Count		01
Input Info	Previous output hash (reversed)	f3f6a909f8521adb57d898d2985834e632374e770fd9e2b98656f1bf1fdfd42701
	Previous output index	000000
	Script Size (bytes)	6b
	scriptSig	48304502203a776322ebf8eb8b58cc6ced4f2574f4c73aa664edce0b0022690f2f6f47c521022100b82353305988cb0ebd443089a173ceec93fe4dbfe98d74419ecc84a6a698e31d012103c5c1bc61f60ce3d6223a63cedbece03b12ef9f0068f2f3c4a7e7f06c523c3664
	sequence	ffffffff
Output Count		02
Output Info	Value	60e3160000000000
	Script Size (bytes)	19
	scriptPubKey	76a914977ae6e32349b99b72196cb62b5ef37329ed81b488ac063d100000000001976a914f76bc4190f3d8e2315e5c11c59cfc8be9df747e388ac
Lock time		00000000

Raw transaction breakdown

Version - All transactions include information about the Bitcoin Version number so we know which rules this transaction follows.

Input Count - Which is how many inputs were used for this transaction

Data stored in Input information:

- **Previous output hash** - All inputs reference back to an output (UTXO). This points back to the transaction containing the UTXO that will be spend in this input. The hash value of this UTXO is saved in a reverse ordered here.
- **Previous output index** - The transaction may have more than one UTXO which are referenced by their index number. The first index is 0.
- **Unlocking Script Size** - This is the size of the Unlocking Script in bytes.
- **Unlocking Script** - This is the hash of the Unlocking Script that fulfills the conditions of the UTXO Locking Script.
- **Sequence Number** - This s a deprecated feature of bitcoin Currently set to ffffffff by default.

Output Count - which tells us how many outputs were produced from this transaction.

Data stored in Output Information:

- **Amount** - The amount of Bitcoin outputted in Satoshis (the smallest bitcoin unit). 10^8 Satoshis = 1 Bitcoin.
- **Locking Script Size** - This is the size of the Locking Script in bytes.
- **Locking Script** - This is the hash of the Locking Script that specifies the conditions that must be met to spend this output.

Locktime - The locktime field indicates the earliest time or the earliest block a transaction can be added to the blockchain. If the locktime is non-zero and less than 500 million, it is interpreted as a block height and miners have to wait until that block height is reached before attempting to add it to a block. If the locktime is above 500 million, it is read as a unix timestamp which means the number of seconds since the date January 1st 1970. It is usually 0 which means confirm as soon as possible.