Danny Diekroeger @dannydiekroeger

11 Jul 20 • 28 tweets • dannydiekroeger/status/1281981259946749955

~ The Anatomy of a Bitcoin Transaction ~

TXID, Outputs, Inputs, Transaction Fees, UTXOs - what do all these terms mean?

In this thread we will dissect a real bitcoin transaction and I'll explain its main components

To expand your background knowledge, read on 👇

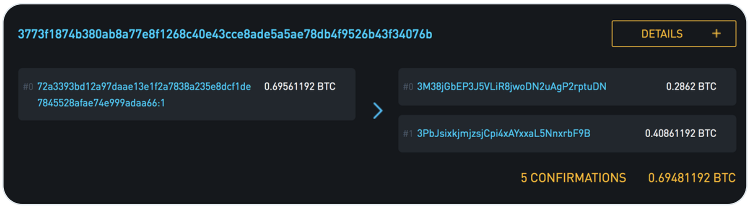
Let's take a look at random bitcoin transaction I picked from a recent block.

Bitcoin Explorer - Blockstream.info

Blockstream Explorer is an open source block explorer providing detailed blockchain data across Bitcoin, Testnet, and Liquid. Supports Tor and tracking-free.

https://blockstream.info/tx/3773f1874b380ab8a77e8f1268c40e43cce8ade5a5ae78db4…

The top of the page has a bunch of data about the Block it was mined in, the fees paid, and some other stuff, but let's focus on the bottom part of the page, as shown in this screenshot:



3773f1874b380ab8a77e8f1268c40e43cce8ade5a5ae78db4f9526b43f34076b

#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

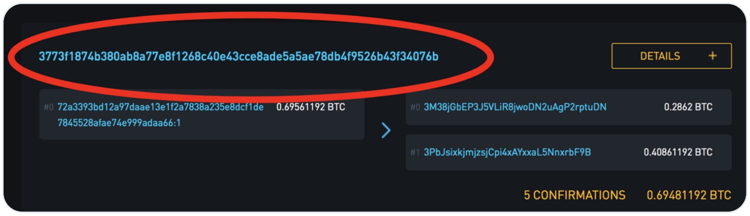
#0 3M38jGbEP3J5VLiR8jwoDN2uAgP2rptuDN 0.2862 BTC

#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.40861192 BTC

5 CONFIRMATIONS 0.69481192 BTC

The first part you should know about is the Transaction ID, also known as the TXID (circled in red).

This is used to uniquely identify a transaction, and it comes from taking the SHA-256 Hash of the transaction data twice.



3773f1874b380ab8a77e8f1268c40e43cce8ade5a5ae78db4f9526b43f34076b

#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

#0 3M38jGbEP3J5VLiR8jwoDN2uAgP2rptuDN 0.2862 BTC

#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.40861192 BTC

5 CONFIRMATIONS 0.69481192 BTC

(Side note, for a primer on what a SHA-256 Hash is, check out my thread on Hash functions)

Danny Diekroeger
@dannydiekroeger

Hash Functions are a key concept in computer science, cryptography, and yes #bitcoin.

It's impossible to explain how bitcoin works without first understanding what a Hash is.

If you'd like to expand your background knowledge, read on 👇

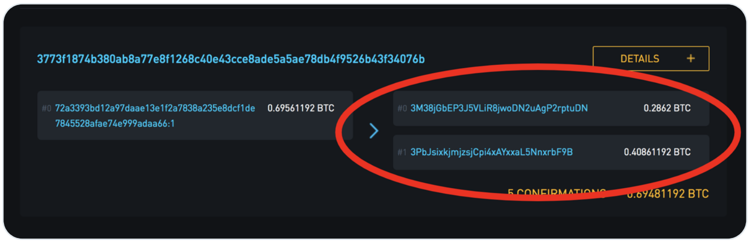
5:40 AM · Jul 9, 2020

♡ 1.6K 568 people are Tweeting about this

Next lets look at those two entries on the right. These are the Outputs (recipients) of the transaction

The recipients are identified by those jumble of numbers and letters that start with a 3.

These are bitcoin addresses, and you can think of them kinda like email addresses



3773f1874b380ab8a77e8f1268c40e43cce8ade5a5ae78db4f9526b43f34076b

#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

#0 3M38jGbEP3J5VLiR8jwoDN2uAgP2rptuDN 0.2862 BTC

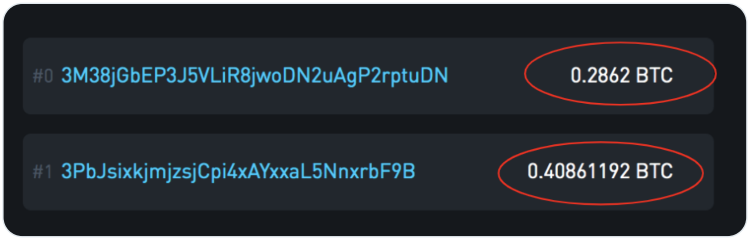
#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.40861192 BTC

5 CONFIRMATIONS 0.69481192 BTC

We can see there are two addresses that received bitcoin here...

#0 received 0.2862 BTC

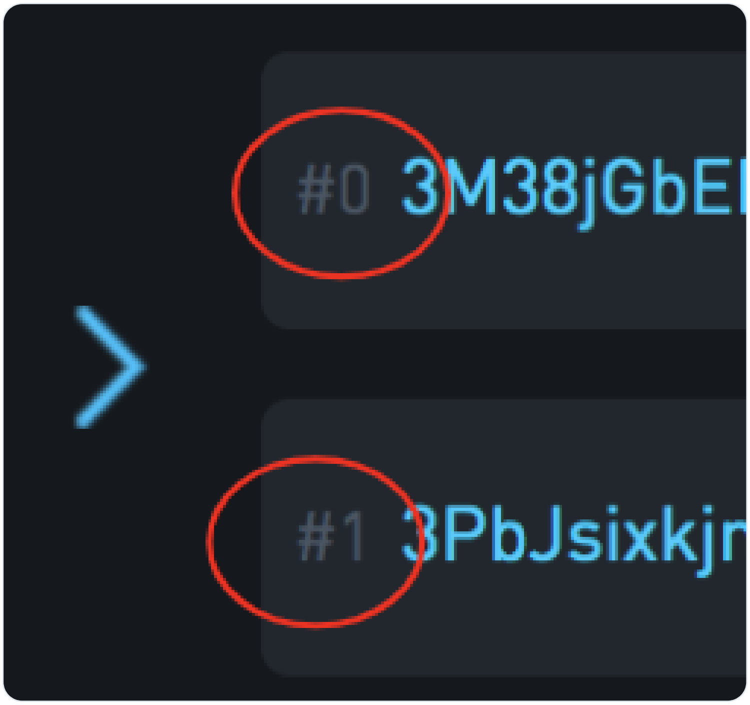
#1 received 0.40861192 BTC



#0 3M38jGbEP3J5VLiR8jwoDN2uAgP2rptuDN 0.2862 BTC

#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.40861192 BTC

In software, it's common to count starting from 0, which is why the first Output is labeled as #0, and the second is labeled as #1

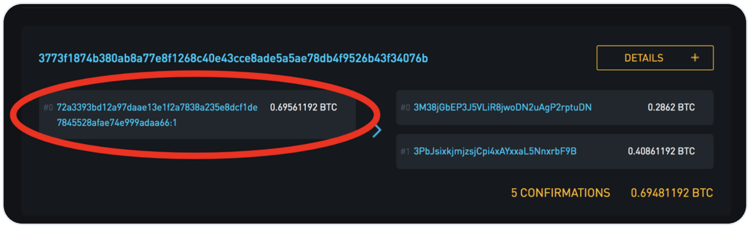


#0 3M38jGbE

#1 3PbJsixkj

Ok so we've identified the TXID and the Outputs, now lets take a look at the Input to this transaction, which is on the left.

Transactions can have multiple inputs, but this transaction has just one single Input, worth 0.69561192 BTC.



3773f1874b380ab8a77e8f1268c40e43cce8ade5a5ae78db4f9526b43f34076b

#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

#0 3M38jGbEP3J5VLiR8jwoDN2uAgP2rptuDN 0.2862 BTC

#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.40861192 BTC

5 CONFIRMATIONS 0.69481192 BTC

Now that we've inspected the TXID, the Outputs, and the Input, let's take a step back a summarize what's happening in this transaction.

Somebody spent 0.69561192 BTC

One address received 0.2862 BTC
Another address received 0.40861192 BTC

If you're quick at Math, you might realize that the amount Spent is slightly larger than the total amount Received...

0.69561192 - (0.2862 + 0.40861192) = 0.0008

Hmm.. what happened here, was it a mistake?

This missing amount is actually not a mistake at all

This leftover amount is what's known as the Transaction Fee, and it's a bribe paid to the miners to convince them to mine (finalize) the transaction

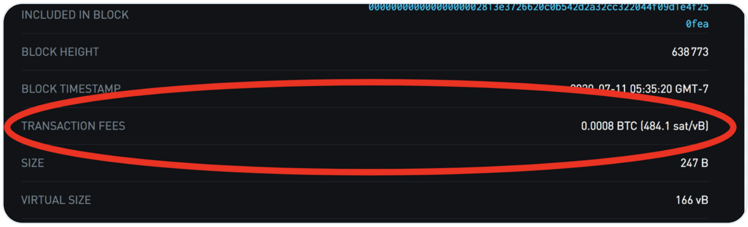
Higher fee rate = higher incentive for a miner to finalize your transaction

The fee is never explicitly written into the transaction

It's just calculated by subtracting the outputs from the inputs

The miner who mines a block with this transaction gets to claim these fees as their own

The website has calculated this fee for us and shows it at the top



INCLUDED IN BLOCK	00000000000000000002813e3726620c0b542d2a32cc322044f09d1e4f25 0fea
BLOCK HEIGHT	638 773
BLOCK TIMESTAMP	2020-07-11 05:35:20 GMT-7
TRANSACTION FEES	0.0008 BTC (484.1 sat/vB)
SIZE	247 B
VIRTUAL SIZE	166 vB

Ok so we've covered the TXID, Outputs, Inputs, and Transaction Fees.

But let's dive a little further and explain where that Input came from.

You see, when an Output is created, it becomes what we call a UTXO (or Unspent Transaction Output)

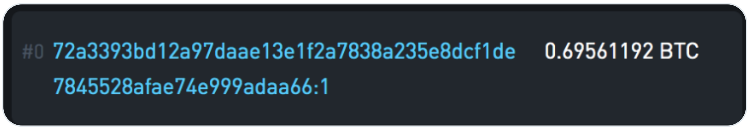
You can think of UTXOs like the dollar bills and coins in your physical wallet

These are the funds you have available to Spend at any given moment

To spend a UTXO, you put it as an Input to a transaction.

Let's see if we can figure out where our Input came from.

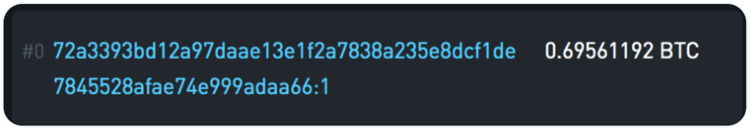
If we take another look, we'll see the Input has an identifier on it that looks like a TXID with ":1" added to the end



#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

This identifier (txid + :number) has a few different names, some call it a "UTXO-key", or an "outpoint".

In our situation it tells us our Input comes from Output #1 of 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66



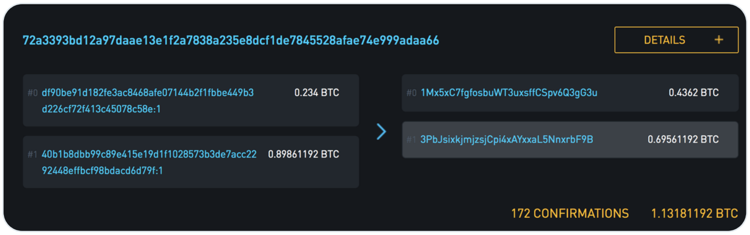
#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

So let's click on that link and see where it takes us!

It takes us to a previous transaction...

Now take a look at the second Output (Output #1) of this previous transaction...

Do you notice anything?



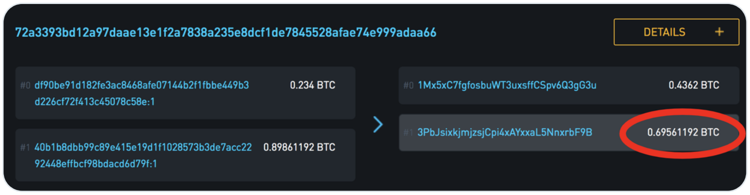
72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66

#0 df90be91d182fe3ac8468afe07144b2f1fbbe449b3d226cf72f413c45078c58e:1 0.234 BTC
#1 40b1b8dbb99c89e415e19d1f1028573b3de7acc2292448effbcf98bdacd6d79f:1 0.89861192 BTC

#0 1Mx5xC7fgfosbuWT3uxsffCSpv6Q3gG3u 0.4362 BTC
#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.69561192 BTC

172 CONFIRMATIONS 1.13181192 BTC

Look at the amount, it is 0.69561192 BTC, which is exactly the same amount as the Input to our original transaction!



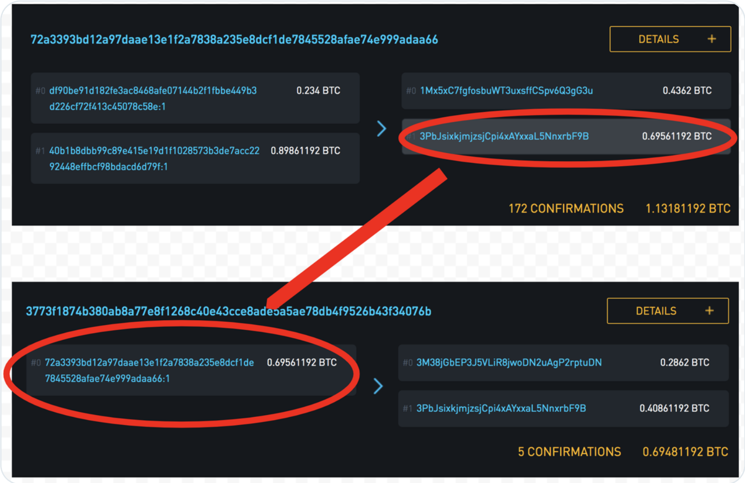
72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66

#0 df90be91d182fe3ac8468afe07144b2f1fbbe449b3d226cf72f413c45078c58e:1 0.234 BTC
#1 40b1b8dbb99c89e415e19d1f1028573b3de7acc2292448effbcf98bdacd6d79f:1 0.89861192 BTC

#0 1Mx5xC7fgfosbuWT3uxsffCSpv6Q3gG3u 0.4362 BTC
#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.69561192 BTC

You've just done what every bitcoin node does for every transaction before accepting it - you've validated that it is spending the correct amount from a previous output. Nice!

Here's a graphic showing the two transactions - the older one on top, and the newer one on the bottom



72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66

#0 df90be91d182fe3ac8468afe07144b2f1fbbe449b3d226cf72f413c45078c58e:1 0.234 BTC
#1 40b1b8dbb99c89e415e19d1f1028573b3de7acc2292448effbcf98bdacd6d79f:1 0.89861192 BTC

#0 1Mx5xC7fgfosbuWT3uxsffCSpv6Q3gG3u 0.4362 BTC
#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.69561192 BTC

172 CONFIRMATIONS 1.13181192 BTC

3773f1874b380ab8a77e8f1268c40e43cce8ade5a5ae78db4f9526b43f34076b

#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

#0 3M38jGbEP3J5VLiR8jwoDN2uAgP2rptuDN 0.2862 BTC
#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.40861192 BTC

5 CONFIRMATIONS 0.69481192 BTC

This linking of outputs to inputs is how the network monitors the history of all transactions, and ensures that no unexpected new coins are created.

Each output can only be spent once!

Make sense? Awesome!

But here's a question for you...

Say I only own a single UTXO, worth 0.69561192 BTC, but I want to send my friend @SahilBloom 0.2862 BTC?

Well let's go back to the dollar bill analogy and ask the same question.

Imagine I have a single 10 dollar bill in my wallet, but I want to buy a 5 dollar coffee?

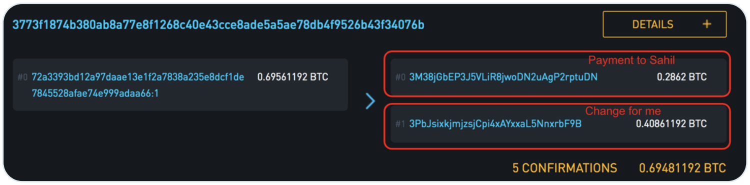
Easy, I give the cashier my 10 dollar bill, and they give me back a 5 dollar bill as Change.

Bitcoin uses a similar concept of Change.

For me to pay @SahilBloom 0.2862 using my 0.69561192 UTXO, I'll create a transaction with two Outputs:

One for 0.2862 to Sahil

And one that gives the remaining 0.40861192 change back to me



3773f1874b380ab8a77e8f1268c40e43cce8ade5a5ae78db4f9526b43f34076b

#0 72a3393bd12a97daae13e1f2a7838a235e8dcf1de7845528afae74e999adaa66:1 0.69561192 BTC

Payment to Sahil
#0 3M38jGbEP3J5VLiR8jwoDN2uAgP2rptuDN 0.2862 BTC

Change for me
#1 3PbJsixkjmjzsjCpi4xAYxxaL5NnxrbF9B 0.40861192 BTC

5 CONFIRMATIONS 0.69481192 BTC

Looks like that's exactly what might have happened in this transaction we dissected!

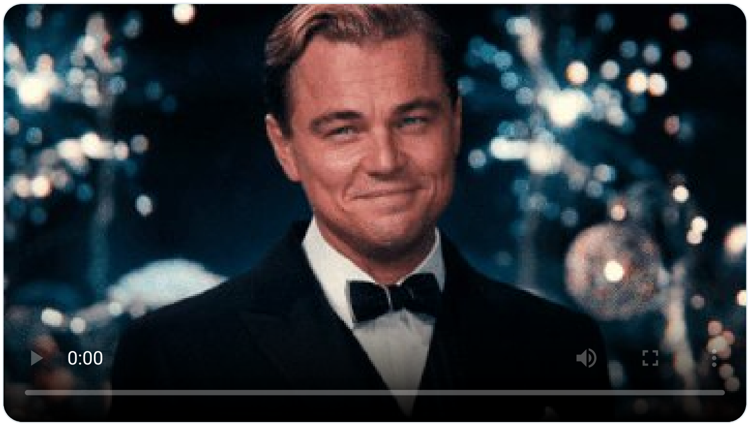
Although this wasn't actually my transaction - so I can't say for sure which output was the payment and which was the change, but you get the idea.

So let's recap:

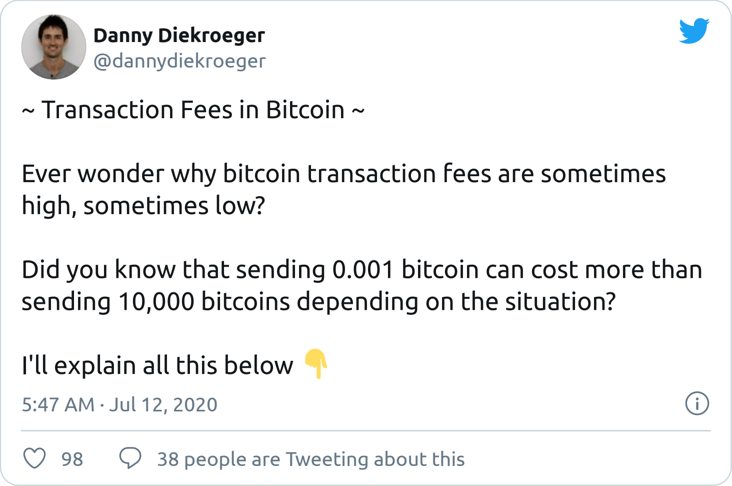
We learned about TXIDs, Outputs, Inputs, Fees, UTXOs, Change, and the basic concept of how transactions are linked (Outputs are UTXOs until they become Inputs).

There's a lot more we can discuss regarding Transactions, but I'll end the thread here.

I hope this was a helpful summary of the basics. Let me know in the comments if you have any questions!



Just posted a new one on Transaction Fees



Danny Diekroeger
@dannydiekroeger

~ Transaction Fees in Bitcoin ~

Ever wonder why bitcoin transaction fees are sometimes high, sometimes low?

Did you know that sending 0.001 bitcoin can cost more than sending 10,000 bitcoins depending on the situation?

I'll explain all this below 👇

5:47 AM · Jul 12, 2020

♡ 98 38 people are Tweeting about this

• • •