HOW DO BITCOIN TRANSACTIONS WORK?

Last updated: 29th January 2018

Simple version:

If I want to send some of my bitcoin to you, I publish my intention and the nodes scan the entire bitcoin network to validate that I 1) have the bitcoin that I want to send, and 2) haven't already sent it to someone else. Once that information is confirmed, my transaction gets included in a "block" which gets attached to the previous block – hence the term "blockchain." Transactions can't be undone or tampered with, because it would mean re-doing all the blocks that came after.

Getting a bit more complicated:

My bitcoin wallet doesn't actually hold my bitcoin. What it does is hold my bitcoin address, which keeps a record of all of my transactions, and therefore of my balance. This address – a long string of 34 letters and numbers – is also known as my "public key." I don't mind that the whole world can see this sequence. Each address/public key has a corresponding "private key" of 64 letters and numbers. This is private, and it's crucial that I keep it secret and safe. The two keys are related, but there's no way that you can figure out my private key from my public key.

That's important, because any transaction I issue from my bitcoin address needs to be "signed" with my private key. To do that, I put both my private key and the transaction details (how many bitcoins I want to send, and to whom) into the bitcoin software on my computer or smartphone.

With this information, the program spits out a digital signature, which gets sent out to the network for validation.

This transaction can be validated – that is, it can be confirmed that I own the bitcoin that I am transferring to you, and that I haven't already sent it to someone else – by plugging the signature and my *public* key (which everyone knows) into the bitcoin program. This is one of the genius parts of bitcoin: if the signature was made with the private key that corresponds to that public key, the program will validate the transaction, without knowing what the private key is. Very clever.

The network then confirms that I haven't previously spent the bitcoin by running through my address history, which it can do because it knows my address (= my public key), and because all transactions are public on the bitcoin ledger.

Even more complicated:

Once my transaction has been validated, it gets included into a "block," along with a bunch of other transactions.

A brief detour to discuss what a "hash" is, because it's important for the next paragraph: a hash is produced by a "hash function," which is a complex math equation that reduces any amount of text or data to 64-character string. It's not random – every time you put in that particular data set through the hash function, you'll get the same 64-character string. But if you change so much as a comma, you'll get a completely different 64-character string. This whole article could be reduced to a hash, and unless I change, remove or add anything to the text, the same hash can be produced again and again. This is a very effective way to tell if something has been changed, and is how the blockchain can confirm that a transaction has not been tampered with.

Back to our blocks: each block includes, as part of its data, a hash of the previous block. That's what makes it part of a chain, hence the term "blockchain." So, if one small part of the previous block was tampered with, the current block's hash would have to change (remember that one tiny change in the input of the hash function changes the output). So if you want to change something in the previous block, you also have to change something (= the hash) in the current block, because the one that is currently included is no longer correct. That's very hard to do, especially since by the time you've reached half way, there's probably another block on top of the current one. You'd then *also* have to change that one. And so on.

This is what makes Bitcoin virtually tamper-proof. I say virtually because it's not impossible, just very very, very, very, very difficult and therefore unlikely.

Fun

And if you want to indulge in some mindless fascination, you can sit at your desk and watch bitcoin transactions float by. Blockchain.info is good for this, but if you want a hypnotically fun version, try BitBonkers.