How do Bitcoin Transactions Work?

Last updated: 6th March 2014

Bitcoin transactions are sent from and to electronic bitcoin wallets, and are digitally signed for security. Everyone on the network knows about a transaction, and the history of a transaction can be traced back to the point where the bitcoins were produced.

Holding onto bitcoins is great if you're a speculator waiting for the price to go up, but the whole point of this currency is to spend it, right? So, when spending bitcoins, how do transactions work?

There are no bitcoins, only records of bitcoin transactions

Here's the funny thing about bitcoins: they don't exist anywhere, even on a hard drive. We talk about someone having bitcoins, but when you look at a particular bitcoin address, there are no digital bitcoins held in it, in the same way that you might hold pounds or dollars in a bank account. You cannot point to a physical object, or even a digital file, and say "this is a bitcoin".

Instead, there are only records of transactions between different addresses, with balances that increase and decrease. Every transaction that ever took place is stored in a vast public ledger called the block chain. If you want to work out the balance of any bitcoin address, the information isn't held at that address; you must reconstruct it by looking at the block chain.

What does a transaction look like?

If Alice sends some bitcoins to Bob, that transaction will have three pieces of information:

- An input. This is a record of which bitcoin address was used to send the bitcoins to Alice in the first place (she received them from her friend, Eve).
- An amount. This is the amount of bitcoins that Alice is sending to Bob.
- An output. This is Bob's bitcoin address.

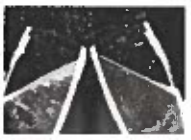
How is it sent?

To send bitcoins, you need two things: a bitcoin address and a private key. A bitcoin address isn't like a bank account; you don't need mountains of paperwork and ID to set one up. In fact, they are generated randomly, and are simply sequences of letters and numbers. The private key is another sequence of letters and numbers, but unlike your bitcoin address, this is kept secret.

FEATURES


Mike Hearn: How Bitcoin's Technology Advanced in 2014

How to Avoid Bitcoin Scams in 2015


10 Bitcoin Resolutions for 2015

The Giant Awakens: Asia's Top Bitcoin Stories in 2014

A Year in Headlines: CoinDesk's Top News Stories of 2014

Think of your bitcoin address as a safe deposit box with a glass front. Everyone knows what is in it, but only the private key can unlock it to take things out or put things in.

When Alice wants to send bitcoins to Bob, she uses her private key to sign a message with the input (the source transaction(s) of the coins), amount, and output (Bob's address).

She then sends them from her bitcoin wallet out to the wider bitcoin network. From there, bitcoin miners verify the transaction, putting it into a transaction block and eventually solving it.

Why must I sometimes wait for my transaction to clear?

Because your transaction must be verified by miners, you are sometimes forced to wait until they have finished mining. The bitcoin protocol is set so that each block takes roughly 10 minutes to mine. Some merchants may make you wait until this block has been confirmed, meaning that you may have to make a cup of coffee and come back again in a short while before you can download the digital goods or take advantage of the service that you paid for.

On the other hand, some merchants won't make you wait until the transaction has been confirmed. They effectively take a chance on you, assuming that you won't try and spend the same bitcoins somewhere else before the transaction confirms. This often happens for low value transactions, where the risk of fraud isn't as great.

What if the input and output amounts don't match?

Because bitcoins exist only as records of transactions, you can end up with many different transactions tied to a particular bitcoin address. Perhaps Jane sent Alice two bitcoins, Philip sent her three bitcoins, and Eve sent her a single bitcoin, all as separate transactions at separate times. These are not automatically combined in Alice's wallet to make one file containing six bitcoins. They simply sit there as different transaction records.

When Alice wants to send bitcoins to Bob, her wallet will try to use transaction records with different amounts that add up to the number of bitcoins that she wants to send Bob.

The chances are that when Alice wants to send bitcoins to Bob, she won't have exactly the right number of bitcoins from other transactions. Perhaps she only wants to send 1.5 bitcoins to Bob. None of the transactions that she has in her bitcoin address are for that amount, and none of them add up to that amount when combined. Alice can't just split a transaction into smaller amounts. You can only spend the whole output of a transaction, rather than breaking it up into smaller amounts.

Instead, she will have to send one of the incoming transactions, and then the rest of the bitcoins will be returned to her as change.

Alice sends the two bitcoins that she got from Jane to Bob. Jane is the input, and Bob is the output. But the amount is only 1.5 bitcoins, because that is all she wants to send. So, her wallet automatically creates two outputs for her transaction: 1.5 bitcoins to Bob, and 0.5 bitcoins to a new address, which it created for Alice to hold her change from Bob.

Are there any transaction fees?

Sometimes, but not all the time. Transaction fees are calculated using various factors. Some wallets let you set transaction fees manually. Any portion of a transaction that isn't picked up by the recipient or returned as change is considered a fee. This then goes to the miner lucky enough to solve the transaction block as an extra reward.

Right now, many miners process transactions for no fees. As the block reward for bitcoins decreases, this will be less likely.

One of the frustrating things about transaction fees in the past was that the calculation of those fees was complex and arcane. It has been the result of several updates to the protocol, and has developed organically. Updates to the core software handling bitcoin transactions will see it change the way that it handles transaction fees, instead estimating the lowest fee that will be accepted.

MUST READ MOST POPULAR


Missing Mt Gox Bitcoins Likely an Inside Job Say Japanese Police


BitMEX to Launch Bitcoin 'Fear' Index


India's Central Bank Could One Day Use Digital Currency, Chief Says


Bitcoin Donations Can Now Fund Mine-Detecting 'Super Rats'


OKCoin Now Offers P2P Lending to International Users


Russian Ministry Criticises Draft Bill Banning Bitcoin

Got a news tip or guest feature?

> "In Korea, people take to new technologies really quickly, so I think bitcoin usage is going to boom, like China."

Richard Yun, SilverBlue managing director

Follow @coindesk

Can I get a receipt?

Bitcoin wasn't really meant for receipts. Although there are changes coming in version 0.9 that will alter the way payments work, making them far more user-friendly and mature. Payment processors like BitPay also provide the advanced features that you wouldn't normally get with a native bitcoin transaction, such as receipts and order confirmation web pages.

What if I only want to send part of a bitcoin?

Bitcoin transactions are divisible. A satoshi is one hundred millionth of a bitcoin, and it is possible to send a transaction as small as 5430 satoshis on the bitcoin network.

NEXT: IS BITCOIN LEGAL?

The legality of your bitcoin activities will depend on who you are and what you are doing with it.

INDEX: A BEGINNERS GUIDE TO BITCOIN

What is Bitcoin?	It's a decentralized digital currency
Why Use Bitcoin?	It's fast, cheap to use, and secure
How Can I Buy Bitcoins?	From an exchange or an individual
How to Buy Bitcoin in the UK	Buying bitcoin in the UK
How to Store Your Bitcoins	Use a digital or paper wallet
What Can You Buy with Bitcoin?	Spend your bitcoins
How to Sell Bitcoin	A guide on how to sell your bitcoins
How to Accept Bitcoin Payments for Your Store	Learn about bitcoin POS systems
How do Bitcoin Transactions Work?	Bitcoin addresses and private keys
Is Bitcoin Legal?	The current regulation around bitcoin
Who is Satoshi Nakamoto?	The founder of bitcoin
How Bitcoin Mining Works	By confirming transactions
How to Set Up a Bitcoin Miner	Generate bitcoins yourself
What are Bitcoin Mining Pools?	What are pools how and how to join them?
How Does Cloud Mining Bitcoin Work?	Alternative bitcoin mining solutions
How to Calculate Mining Profitability	Can you make a ROI?
How to Make a Paper Bitcoin Wallet	Creating an unhackable bitcoin wallet