Latest News

Opinions: What Experts Think about a Possible Bitcoin ETF
BITCOIN OPINION

Secret Plots, Google Bans, and Augur Assassination Markets: This Week in Crypto
NEWS

Only 2% of U.S. Investors Own Bitcoin, Most View it as 'Very Risky': Wells Fargo Poll
BITCOIN & BLOCKCHAIN
INVESTMENTS

Opinion | How Blockchain Could Fix Facebook's Fake News Problem
BLOCKCHAIN NEWS

Interview: Joe Fanelli, Co-Founder of Top 21 Block Producer EOS Asia
ALTCOIN NEWS

Crypto Market Rebounds, Bithumb Drives Kimchi Premium Up 50%
ALTCOIN PRICES

Chinese Social Network Tianya is Launching a Native Cryptocurrency
BLOCKCHAIN NEWS

Crypto Exchange HitBTC Adds Support for Euro-Pegged Stablecoin 'EURS'
EXCHANGES

Romania Targets Cryptocurrencies With New Electronic Money Law
NEWS

Tezos Foundation Taps 'Big Four' Firm PwC for Independent Audit
ALTCOIN NEWS

BITCOIN TUTORIALS AUGUST 06, 2014 16:22

How a Bitcoin Transaction Works

This article explains what a Bitcoin transaction is, its purpose and outcome. The explanation made below is suitable for both novice and intermediate Bitcoin users.

As a cryptocurrency user you need to be familiar with transaction rudiments – for the sake of your own confidence with this evolving innovation, and as a foundation for understanding emerging *multi-signature* transactions and *contracts*, both of which will be explored later in the series. This is not a technical article and explanation will focus on what you need to know about **standard bitcoin transactions** – the spend transactions we commonly make – and we'll gloss over what you can safely ignore.

An infographic at the bottom of the article provides a comprehensive illustration of the entire Bitcoin transaction process from wallet to blockchain.

Note: Even the Core developers acknowledge that some of the language being used to describe transactions and their components can lead one to a mistaken concept of what is really happening. These misconceptions are avoided in the explanation below. So, while trying to keep things as simple as possible, and with the aid of a few diagrams, let's dive right in.

[divider]CCN[/divider]

Definition of Terms and Abbreviations

Bitcoin with a capital "B" refers to the protocol – the code, the nodes, the network and their peer-to-peer interaction.
bitcoin with a lowercase 'b' refers to the currency – the cryptocurrency we send and receive, via the Bitcoin network.
tx – wherever it is used in the text – is an abbreviation for 'Bitcoin transaction'
txid is an abbreviation for 'transaction id' – this is a hash that is used by both humans and the protocol to reference transactions.
Script is the name of the Bitcoin protocol's scripting system that processes and validates transactions. Script is a clever, stack-based instruction engine, and it makes all transactions from simple payments to complex oracle overseen contracts possible.
UTXO is an abbreviation for Unspent Transaction Output, also referred to as an "output".
satoshi – 1 BTC = 100,000,000 satoshi

What is a Bitcoin Transaction and Why?

Definition

A Bitcoin transaction is a signed piece of data that is broadcast to the network and, if valid, ends up in a block in the blockchain.

Purpose

ICO CALENDAR

RS Coin NEO $ 26.08.2018
FOAM Protocol ETHEREUM 6 31.07.2018
Metabase NATIVE $ 04.09.2018
ARAW ETHEREUM 7.5 01.08.2018

View all ICOs

The Bitcoin Podcast by CCN
THE CCN PODCAST
#4 This Week in Crypto: Bitco...
00:00:00

BITCOIN EVENTS CALENDAR

No Events found.

Trending

Crypto Exchange HitBTC Adds Support for Euro-Pegged Stablecoin 'EURS'

Opinions: What Experts Think about a Possible Bitcoin ETF

Romania Targets Cryptocurrencies With New Electronic Money Law

London Remittance Firm Launches Cryptocurrency Trading Service, Says Crypto's 'Here to Stay'
ACCEPTS BITCOIN

Bitcoin Ransomware Creators Avoid Jail Time for $11,000 Heist
BITCOIN CRIME

Circle Taps Fmr. Goldman Sachs Executive to Spearhead Regulatory Affairs
EXCHANGES

U.S. Congress Should Make Cryptocurrency a Key Focus: House Rep.
BITCOIN REGULATION

CME Won't Be Listing New Cryptocurrency Futures Anytime Soon: CEO
BITCOIN EXCHANGE

Kim Dotcom Creates Own Cryptocurrency Aimed at Content Creators
ALTCOIN NEWS

We're 'Thrilled' That Regulators Are Getting Involved in Crypto: Ripple Exec.
NEWS

AMD Expects GPU Sales

Purpose

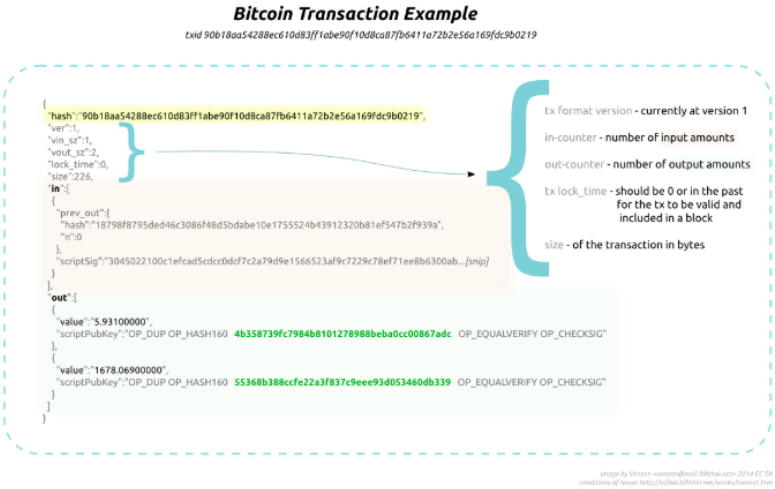
The purpose of a Bitcoin transaction is to *transfer ownership* of an amount of Bitcoin to a Bitcoin address.

Outcome

When you send Bitcoin, a single data structure, namely a Bitcoin transaction, is created by your wallet client and then broadcast to the network. Bitcoin nodes on the network will relay and rebroadcast the transaction, and if the transaction is valid, nodes will include it in the block they are mining. Usually, within 10-20mins, the transaction will be included, along with other transactions, in a block in the blockchain. At this point the receiver is able to see the transaction amount in their wallet.

Example

Here is an example transaction that was included in the blockchain earlier this year:



The main components of this standard transaction are color-coded:

- **Transaction ID** *(highlighted in yellow)*
- **Descriptors and meta-data** *(blue curly brace elaborated upon to the right)*
- **Inputs** *(pink area)*
- **Outputs** *(green area)*

Bitcoin Transaction Inputs and Outputs

Firstly, four axiomatic truths about transactions:

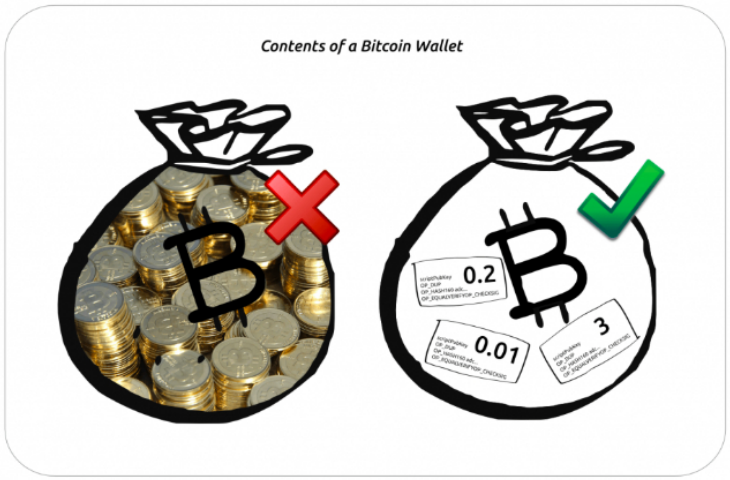
- *Any Bitcoin amount that we send is always sent to an address.*
- *Any Bitcoin amount we receive is locked to the receiving address – which is (usually) associated with our wallet.*
- *Any time we spend Bitcoin, the amount we spend will always come from funds previously received and currently present in our wallet.*
- *Addresses receive Bitcoin, but they do not send Bitcoin – Bitcoin is sent from a wallet.*

The amounts that go into our wallet are not jumbled like the coins in a physical wallet. The **received amounts don't mix** but remain separate and distinct as the exact amounts received by the wallet. Here's an illustration:

Example

You create a brand new wallet and, in time, it receives three amounts of 0.01, 0.2 and 3 BTC as follows: you send 3 BTC to an address associated with the wallet and two payments are made to another address by Alice.

The wallet reports a balance of 3.21 BTC, yet if you were to virtually peek inside the wallet, you would see – not 321,000,000 satoshi (321 mil satoshi) – but three distinct amounts still grouped together by their originating transactions: 0.01, 0.2 and 3 BTC.



The received bitcoin amounts don't mix but remain separated as the exact amounts sent to the wallet. The three amounts in the example above are called the **outputs** of their originating transactions.

Bitcoin wallets always keep outputs separate and distinct.

Definition

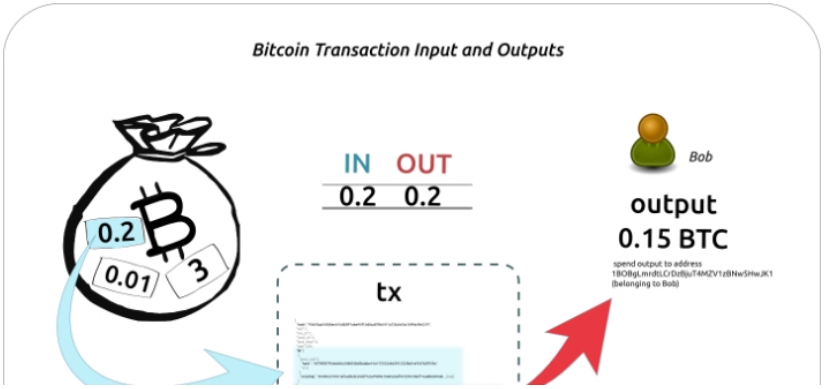
An **output** is an amount that was sent (via a standard transaction) to a Bitcoin address, along with a set of rules to unlock the output amount. In Bitcoin parlance an output is called an *"unspent transaction output"*, or **UTXO**.

A standard transaction output can be unlocked with the private key associated with the receiving address. Addresses and their associated public/private key pairs will be covered later in the series. For now, we are concerned with the output amount only.

Example

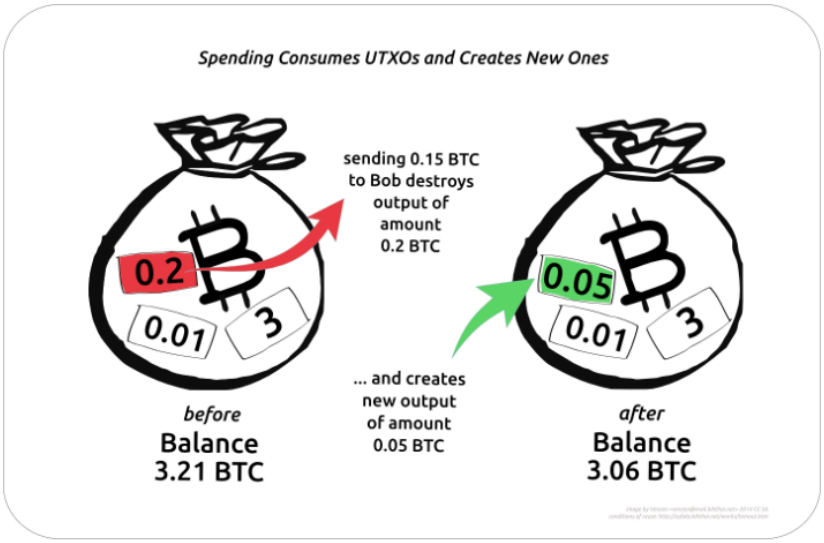
Let's consider an example by following the money in a scenario where you send 0.15 BTC to Bob.

As we have seen, your wallet does not select 15 mil satoshi (0.15 BTC) from an undifferentiated pool of 321 mil satoshi making up the wallet balance. Instead, the wallet selects a spend candidate from amongst the three existing "outputs" contained in the wallet. So, it chooses (for various reasons that are not important now) the 0.2 BTC output. The wallet will unlock the 0.2 BTC output and use the whole amount of 0.2 BTC as an **input** to your new 0.15 BTC transaction. The 0.2 BTC output is "spent" in the process. *–Read this paragraph a second time.*



The spend transaction your wallet creates will send 0.15 BTC to Bob's address – where it will reside in *his* wallet as an output – waiting eventually to be spent.

The 0.05 BTC difference (0.2 BTC input minus 0.15 BTC output) is called **"change"** and the transaction will send this back to your wallet via a newly created address. The 0.05 BTC change amount will reside in your wallet as a new output – waiting eventually to be spent. So, now, a virtual peek inside your wallet reveals the following:



Each of the three outputs that are "waiting to be spent", is locked to its receiving addresses until such time as one or more of them are selected as input(s) to a new spend transaction.

Behind the scenes, different wallet clients apply different logic rules when selecting UTXOs as inputs to new transactions. A sane wallet policy is to use older UTXOs first, wherever possible, but implementations differ. The manner in which UTXOs are selected is not of concern to us right now, since the objective has been emphasis of the point that amounts received to our wallets remain separate and distinct.

Summary of How a Bitcoin Transaction Works

Various received amounts don't mix as they do in a physical wallet. Instead, received amounts (UTXOs) are used individually (or in combination) at the moment we spend Bitcoin. When creating the spend transaction our wallet selects UTXOs (of sufficient value to satisfy the amount we want to send) and typically creates two new outputs: one for the receiver and one for the change we receive back to our wallet. The change becomes a brand new UTXO in our wallet, and the amount we send becomes a UTXO locked to the recipient address – which may or may not be associated with a wallet, e.g. cold storage. The original UTXO used as input to the spend transaction is "spent" and destroyed forever.

This has been an introduction to how outputs (UTXOs) are handled by wallet software. Once a UTXO is selected for expenditure, it requires the private key associated with the address that received it. This private key redeems the UTXO and allows it to become an input in a new spend transaction. The mechanism whereby previous transaction outputs are reused as the inputs to new transactions is central to the Bitcoin protocol's function – and exactly as per Satoshi's design.

CryptoCoinsNews

How Bitcoin Works

Images by Shutterstock.

POSTED IN: BITCOIN TUTORIALS, LEARN ABOUT BITCOIN, NEWS

AUTHOR
Venzen Khaosan

SHARE POST

Market analyst and Open source developer with a keen interest in blockchain technology, consensus mechanisms and the decentralizing effect. He has found a solution to the PKI mechanism. Email me to discuss.

BITCOIN POLITICS AUGUST 06, 2014 12:20

British Chancellor George Osborne Buys Into Bitcoin

Today, the U.K.'s Chancellor of the Exchequer, George Osborne,

bought bitcoins for the first time from Cointrader.net's Bitcoin ATM powered by Robocoin. Mr. Osborne declared that it was his intention to explore the potential for using digital currencies, such as Bitcoin, to better access finance for small businesses. He went on to explain how regulation of virtual and digital currencies, and the risks associated with them, were to be explored in a bid to boost the UK's Financial Technology (FinTech) sector.

[divider]CCN[/divider]

British Chancellor, George Osborne, was the VIP guest at today's launch of Innovate Finance, previously FinTech UK, an industry body designed to champion Britain's finance and technology industry. As the Cabinet Minister is directly responsible for all economic and financial matters, Osbourne has the most powerful position in Government alongside the Prime Minister. Osbourne's receptive attitude to Bitcoin is another positive sign as the popular digital currency gains widespread worldwide institutional acceptance.

British Chancellor of the Exchequer, George Osborne, Acknowledges Bitcoin

The UK government is preparing to publish a strategy document later this year setting out how the UK can become the World's *"global center of financial innovation"*.

Today's Huffington Post is reporting that Vince Cable, the UK Business Secretary, has said: *"Forcing banks to refer businesses to alternative lenders is something I've been determined to make happen."* He later went on to say : *"It's good that more SMEs are making use of alternative finance but the big banks still dominate and small businesses often give up if they're turned down for finance by their bank. The UK needs a diverse and competitive business finance market like Germany and the US if our SMEs are to thrive, and that is why the Business Bank is so important. Money is already reaching small businesses, but my ambition for the Business Bank is to radically alter the overall market landscape."*

George Osbourne is the Chancellor of the Exchequer in the UK Government, he is the Member of Parliment for the district of Tatton, in Cheshire. He was first elected in June 2001 becoming the youngest Conservative MP in the House of Commons. May 2010 General Election, George Osbourne has been re-elected at every election since and was, after the last election, appointed Chancellor of the Exchequer by the new Prime Minister, David Cameron. The *Financial Times* describes Osborne as *"metropolitan and socially liberal. He is hawkish on foreign policy with links to Washington neo-conservatives and ideologically committed to cutting the state. A pragmatic Eurosceptic."*

In March the UK exchequer outlined plans for taxation (VAT) on bitcoins but other than this has remained tight lipped on cryptocurrencies to date. A finance spokesman said: *"It's only by harnessing innovations in finance, alongside our existing world class knowledge and skills in financial services, that we'll ensure Britain's financial sector continues to meet the diverse needs of businesses and consumers, here and around the globe, and create the jobs and growth we all want to see in the future."*

The city of London has been long established as a center of financial management.

Featured image by Shutterstock.

POSTED IN: BITCOIN POLITICS, NEWS

TAGS: EXCHEQUER, GEORGE OSBORNE, UK BITCOIN

AUTHOR
PJ Delaney

SHARE POST

Masters in Public Administration, Bachelors in Mgt., I live in Ireland, I have a bit of a background in Economics and lots of opinions on everything else.

CME Won't Be Listing New Cryptocurrency Futures Anytime Soon: CEO
BITCOIN EXCHANGE

Kim Dotcom Creates Own Cryptocurrency Aimed at Content Creators
ALTCOIN NEWS

We're 'Thrilled' That Regulators Are Getting Involved in Crypto: Ripple Exec.
NEWS

AMD Expects GPU Sales to Cryptocurrency Miners to Keep Sliding
ALTCOIN MINING