TRENDING
10 Bitcoin Resolutions for 2015

BITCOIN PRICE INDEX (24H)

USD 0.31% ▲
$314.91
EUR €262.24

CNY 0.42% ▲
¥1,946.67
GBP £205.20

HOME NEWS GUIDES PRICE DATA EVENTS JOBS

Search

How Bitcoin Mining Works

Tweet 96 Share 132 g+1 18 Share 18 0 points

Last updated: 22nd December 2014

In traditional fiat money systems, governments simply print more money when they need to. But in bitcoin, money isn't printed at all – it is discovered. Computers around the world 'mine' for coins by competing with each other.

How does mining take place?

People are sending bitcoins to each other over the bitcoin network all the time, but unless someone keeps a record of all these transactions, no-one would be able to keep track of who had paid what. The bitcoin network deals with this by collecting all of the transactions made during a set period into a list, called a block. It's the miners' job to confirm those transactions, and write them into a general ledger.

Making a hash of it

This general ledger is a long list of blocks, known as the 'blockchain'. It can be used to explore any transaction made between any bitcoin addresses, at any point on the network. Whenever a new block of transactions is created, it is added to the blockchain, creating an increasingly lengthy list of all the transactions that ever took place on the bitcoin network. A constantly updated copy of the block is given to everyone who participates, so that they know what is going on.

But a general ledger has to be trusted, and all of this is held digitally. How can we be sure that the blockchain stays intact, and is never tampered with? This is where the miners come in.

When a block of transactions is created, miners put it through a process. They take the information in the block, and apply a mathematical formula to it, turning it into something else. That something else is a far shorter, seemingly random sequence of letters and numbers known as a hash. This hash is stored along with the block, at the end of the blockchain at that point in time.

Hashes have some interesting properties. It's easy to produce a hash from a collection of data like a bitcoin block, but it's practically impossible to work out what the data was

DAILY BITCOIN NEWS

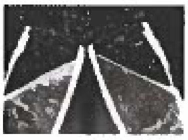
Don't miss a single story - subscribe now!

Email Address SUBSCRIBE

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

just by looking at the hash. And while it is very easy to produce a hash from a large amount of data, each hash is unique. If you change just one character in a bitcoin block, its hash will change completely.

Miners don't just use the transactions in a block to generate a hash. Some other pieces of data are used too. One of these pieces of data is the hash of the last block stored in the blockchain.

Because each block's hash is produced using the hash of the block before it, it becomes a digital version of a wax seal. It confirms that this block – and every block after it – is legitimate, because if you tampered with it, everyone would know.

If you tried to fake a transaction by changing a block that had already been stored in the blockchain, that block's hash would change. If someone checked the block's authenticity by running the hashing function on it, they'd find that the hash was different from the one already stored along with that block in the blockchain. The block would be instantly spotted as a fake.

Because each block's hash is used to help produce the hash of the next block in the chain, tampering with a block would also make the subsequent block's hash wrong too. That would continue all the way down the chain, throwing everything out of whack.

Competing for coins

So, that's how miners 'seal off' a block. They all compete with each other to do this, using software written specifically to mine blocks. Every time someone successfully creates a hash, they get a reward of 25 bitcoins, the blockchain is updated, and everyone on the network hears about it. That's the incentive to keep mining, and keep the transactions working.

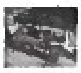
The problem is that it's very easy to produce a hash from a collection of data. Computers are really good at this. The bitcoin network has to make it more difficult, otherwise everyone would be hashing hundreds of transaction blocks each second, and all of the bitcoins would be mined in minutes. The bitcoin protocol deliberately makes it more difficult, by introducing something called 'proof of work'.

The bitcoin protocol won't just accept any old hash. It demands that a block's hash has to look a certain way; it must have a certain number of zeroes at the start. There's no way of telling what a hash is going to look like before you produce it, and as soon as you include a new piece of data in the mix, the hash will be totally different.

Miners aren't supposed to meddle with the transaction data in a block, but they must change the data they're using to create a different hash. They do this using another, random piece of data called a 'nonce'. This is used with the transaction data to create a hash. If the hash doesn't fit the required format, the nonce is changed, and the whole thing is hashed again. It can take many attempts to find a nonce that works, and all the miners in the network are trying to do it at the same time. That's how miners earn their bitcoins.

Tweet 98 Share 132 g+1 18 Share 18 0 points

NEXT: HOW TO SET UP A BITCOIN MINER



Decide on your hardware, calculate your profitability, and download the software.

INDEX: A BEGINNERS GUIDE TO BITCOIN

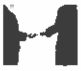
MUST READ MOST POPULAR

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?

> *"Cost reduction was only one of the drivers for accepting bitcoin. The other was grounded in ideology."*

Patrick Byrne, CEO of Overstock.com

Follow @coindesk