Hyped as ‘next big thing’ and the ‘currency of the internet’, the math behind cryptocurrency is worth exploring.

Why can’t you create a “counterfeit bitcoin” and spend it?

Instead of a bank or government issuing out currency, bitcoin is ‘mined’ by computers performing certain actions. Miners both add transactions to the public ledger and confirm transactions that take place. So, firstly there’s not really

There would be no record of you having received that bitcoin, so it wouldn’t really exist.

The block chain

Every block contains a hash of its previous block verified using the SHA-2 algorithm. This authenticates the previous block because it

For a block to be accepted it must has to a value less than the current target.

Any change to a block will render the block hash completely different. For example if the known block is

Hello World!

This may hash to

1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

Then if you add a 1 to the end

Hello World!1

e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8

All miners are looking for an addition that is easy to check, ex, will have four zeros in the front of the hash.

So they keep adding to hello world until…

Hello, world!4250

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Look up the step by step for how the next btc is mined from the previous