

Forum:[Hack Forums](#)

Thread: [What's the point of confirmations?](#)

LastSession V - December 26, 2016, 11:59 am

What even is the point of confirmations, can you fake a confirmation or fake the sending of money, is it possible to get the BTC pulled back before the first confirmation?

Thanks

minimalist - December 26, 2016, 12:02 pm

The whole basis of cryptocurrencies is that the transactions are cryptographically proven to be "correct." When you wait for a confirmation, you are waiting for a miner to prove that your transaction is valid. When you do not wait for a confirmation, a miner is unable to prove that your transaction is legitimate and it may be overridden by another transaction (a consensus).

Punisher - December 26, 2016, 12:04 pm

Confirmations are basically how BTC operates.. miners match hashes until they find a matching hash for a block to confirm the transaction is real. This prevents double-spending (which basically answers your second question).

Cancelling unconfirmed transactions is easy. Just submit a higher fee double-spend transaction. For example: if you send a 0-fee transaction it could take a day before 1 block mines it. Then you send another transaction with the same inputs that just sends the money back to yourself.

<https://en.bitcoin.it/wiki/Double-spending>

LastSession V - December 26, 2016, 12:10 pm

(Dec 26, 2016 01:02 PM)Minimalist Wrote: [\[CITE\]](#) The whole basis of cryptocurrencies is that the transactions are cryptographically proven to be "correct." When you wait for a confirmation, you are waiting for a miner to prove that your transaction is valid. When you do not wait for a confirmation, a miner is unable to prove that your transaction is legitimate and it may be overridden by another transaction (a consensus).

(Dec 26, 2016 01:04 PM>Error Wrote: [\[CITE\]](#) Confirmations are basically how BTC operates.. miners match hashes until they find a matching hash for a block to confirm the transaction is real. This prevents double-spending (which basically answers your second question).

Cancelling unconfirmed transactions is easy. Just submit a higher fee double-spend transaction. For example: if you send a 0-fee transaction it could take a day before 1 block mines it. Then you send another transaction with the same inputs that just sends the money back to yourself.

<https://en.bitcoin.it/wiki/Double-spending>

So with Blockchain, how would I go about send \$200 BTC, and then taking it back. Is there any chance at all that the money could somehow send?

minimalist - December 26, 2016, 12:12 pm

(Dec 26, 2016 01:10 PM)LastSession V Wrote: [\[CITE\]](#) So with Blockchain, how would I go about send \$200 BTC, and then taking it back. Is there any chance at all that the money could somehow send?

There's no incentive for a miner to choose a no-fee transaction over a transaction with a non-zero fee, so probably not. However, if the network isn't loaded, the miner MAY select the no-fee transaction.

...but ideally, you shouldn't con others.

Nyxuo - December 26, 2016, 12:14 pm

This pretty much just makes me think with information like this being shared more people will consider 'double-spending'. I know it's out there already but I don't think we should encourage this information by sharing it here. It already sucks enough that people can even do this.

I'm also not suggesting that OP or anyone who has shared information on this would do it in no way. Just for the record.

Punisher - December 26, 2016, 12:15 pm

(Dec 26, 2016 01:10 PM)LastSession V Wrote: [\[CITE\]](#) So with Blockchain, how would I go about send \$200 BTC, and then taking it back. Is there any chance at all that the money could somehow send?

I don't really feel comfortable teaching people how to commit fraud.

Google is a great resource for this type of information though!

L A S S 3 - December 26, 2016, 12:18 pm

double spending is the most painful thing you can do with cryptocurrencies imo

Omniscient - December 26, 2016, 1:16 pm

Quote:What even is the point of confirmations, can you fake a confirmation or fake the sending of money, is it possible to get the BTC pulled back before the first confirmation?

Let me phrase that back at you.

The point of confirmations is that you can't fake sending money or pull back the funds once it's confirmed.

Before there is a first confirmation it is possible to spend it twice. That's called a double-spend and the blockchain miners will sort out which one to do first and the one they deem second won't be confirmed. This is why you should never consider Bitcoin payments from untrusted sources as PAID until at least one confirmation occurs. It's why many places require up to 6 confirmations before it's considered PAID. Some smaller cryptos want 10 or more confirmations. That's to avoid any possibility of a corrupt blockchain taking hold in order to steal the coins.

Quote:So with Blockchain, how would I go about send \$200 BTC, and then taking it back. Is there any chance at all that the money could somehow send?

You don't. Sent is sent even if it's not confirmed. Your only hope is to create a second transaction very quickly that will send it to another address. And be aware that while it is possible it is also difficult and doesn't have any guarantee it will work.