

Welcome, **Guest**. Please login or register.

Input fields for username, password, session length (Forever), and a Login button.

Login with username, password and session length

News: Latest stable version of Bitcoin Core: [0.11.2](#) [Torrent]

Search bar with a magnifying glass icon and a Search button.

HOME HELP SEARCH DONATE LOGIN REGISTER

Bitcoin Forum > Bitcoin > Development & Technical Discussion (Moderator: gmaxwell) > **Need OP_BLOCKNUMBER to allow "time" limited transactions**

<< previous topic next topic >>

Pages: [1]

print

Author Topic: Need OP_BLOCKNUMBER to allow "time" limited transactions (Read 3194 times)

ByteCoin Sr. Member



Activity: 416



Ignore

Need OP_BLOCKNUMBER to allow "time" limited transactions

November 15, 2010, 01:17:03 AM

#1

At the moment, if you make a payment to someone but they've wiped their wallet then the coins are irretrievably lost.

Similarly, if the network is flooded with 0.01 fee transactions and you make an urgent payment but forget to include a higher fee then you can't reissue that payment backed by the same coins but with a fee.

If you could cause the current block number to be pushed on the stack and do some maths with it then you could implement a payment that must be spent by the recipient before a certain block number is reached or else the script would allow it to be spent again by the sender for example.

I suspect that this would be a very popular transaction mechanic.

ByteCoin

C O I N P L E I

L P E N B O R R O

B O R R O W N O W

Advertised sites are not endorsed by the Bitcoin Forum. They may be unsafe, untrustworthy, or illegal in your jurisdiction. Advertise here.

theymos Administrator Legendary



Activity: 2142



Ignore

Re: Need OP_BLOCKNUMBER to allow "time" limited transactions

November 15, 2010, 01:49:59 AM

#2

That would be useful, but it's probably best to keep scripts stateless. Since different nodes might have different ideas about what the current blockcount is, a situation could develop where half the network considers a transaction valid and half considers it invalid. This is not good for the network.

1NXYoJ5xU91Jp83XfVMHwwTUyZFK64BoAD

ByteCoin Sr. Member



Activity: 416



Ignore

Re: Need OP_BLOCKNUMBER to allow "time" limited transactions

November 15, 2010, 02:47:30 AM

#3

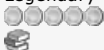
Quote from: theymos on November 15, 2010, 01:49:59 AM

That would be useful, but it's probably best to keep scripts stateless. Since different nodes might have different ideas about what the current blockcount is, a situation could develop where half the network considers a transaction valid and half considers it invalid. This is not good for the network.

Hmm.. If clients disagree about what the current block count is then they already disagree about whether certain transactions are valid or not and therefore the problem you mention exists already without my proposal. Please go into more detail about why this is not good for the network.

ByteCoin

theymos Administrator Legendary



Activity: 2142



Ignore

Re: Need OP_BLOCKNUMBER to allow "time" limited transactions

November 15, 2010, 03:53:09 AM

#4

Quote from: ByteCoin on November 15, 2010, 02:47:30 AM

Hmm.. If clients disagree about what the current block count is then they already disagree about whether certain transactions are valid or not and therefore the problem you mention exists already without my proposal. Please go into more detail about why this is not good for the network.

You may be right about this. Bitcoin's segmentation-fixing mechanisms would seem to keep everything in order.

A similar feature seems to already be planned. Every transaction has the currently-unused "nLockTime"

field, and this bit of code exists for the UI (the text would appear in the same place as "x confirmations"):


Code:

```
if (!wtx.IsFinal())
{
    if (wtx.nLockTime < 500000000)
        return sprintf(_("Open for %d blocks"), nBestHeight - wtx.nLockTime);
    else
        return sprintf(_("Open until %s"), DateTimeStr(wtx.nLockTime).c_str());
}
```

Sounds very much like what you're thinking of.

1NXYoJ5xU91Jp83XFVMHwwTUyZFK64BoAD

theymos
Administrator
Legendary

 **Re: Need OP_BLOCKNUMBER to allow "time" limited transactions**

#5

After investigating some more, I found that nLockTime requires in-memory transaction replacement to be re-activated for it to be useful.

Code:

```
if (mapNextTx.count(outpoint))
{
    // Disable replacement feature for now
    return false;


    // Allow replacing with a newer version of the same transaction
    if (i != 0)
        return false;
    ptxOld = mapNextTx[outpoint].ptx;
    if (!IsNewerThan(*ptxOld))
        return false;
    for (int i = 0; i < vin.size(); i++)
    {
        COutPoint outpoint = vin[i].prevout;
        if (!mapNextTx.count(outpoint) || mapNextTx[outpoint].ptx != ptxOld)
            return false;
    }
    break;
}
```

Activity: 2142



1NXYoJ5xU91Jp83XFVMHwwTUyZFK64BoAD

satoshi
Founder
Sr. Member

 **Re: Need OP_BLOCKNUMBER to allow "time" limited transactions**

#6

We can't safely do OP_BLOCKNUMBER. In the event of a block chain reorg after a segmentation, transactions need to be able to get into the chain in a later block. The OP_BLOCKNUMBER transaction and all its dependants would become invalid. This wouldn't be fair to later owners of the coins who weren't involved in the time limited transaction.

Activity: 364



Ignore

nTimeLock does the reverse. It's an open transaction that can be replaced with new versions until the deadline. It can't be recorded until it locks. The highest version when the deadline hits gets recorded. It could be used, for example, to write an escrow transaction that will automatically permanently lock and go through unless it is revoked before the deadline. The feature isn't enabled or used yet, but the support is there so it could be implemented later.

MoonShadow
Legendary

 **Re: Need OP_BLOCKNUMBER to allow "time" limited transactions**

#7

Quote from: satoshi on November 15, 2010, 06:37:44 PM

```
nTimeLock does the reverse. It's an open transaction that can be replaced with new versions until the deadline. It can't be recorded until it locks. The highest version when the deadline hits gets recorded. It could be used, for example, to write an escrow transaction that will automatically permanently lock and go through unless it is revoked before the deadline. The feature isn't enabled or used yet, but the support is there so it could be implemented later.
```

Activity: 1596


**Ron
2012
Paul**




Ignore

Does using nTimeLock also tie up some of the sender's coins until the lock expires? I imagine that it would have to, and that would solve the escrow problem immediately, allowing the sender to effectively write the Bitcoin version of a backdated check. Even better, seeing the locked transaction on the network would allow the merchant to know that the sender actually does have the funds to buy the product, and if the coins are tied up until the lock expires, that the sender will probably *still* have those same funds. The possibility of a fraudster sending a locked transaction to buy something online, and then revoking the transaction after the product has been shipped, still exists. But it can add confidence in a transaction without requiring a third party escrow. Would the revocation of transactions leave a record inside or outside the blockchain? If it did, a scan of the blockchain might be able to highlight increased risks of a revoked transaction if a fraudster had already done the scam once to someone else with the same set of coins. Doing this would temporarily 'taint' the coins used in the revoked transaction, until they were used in several valid transactions.

"The powers of financial capitalism had another far-reaching aim, nothing less than to create a world system of financial control in private hands able to dominate the political system of each country and the economy of the world as a whole. This system was to be controlled in a feudalist fashion by the central banks of the world acting in concert, by secret agreements arrived at in frequent

ByteCoin
Sr. Member


 **Re: Need OP_BLOCKNUMBER to allow "time" limited transactions**
November 18, 2010, 02:16:15 AM

#8

Quote from: satoshi on November 15, 2010, 06:37:44 PM

We can't safely do OP_BLOCKNUMBER. In the event of a block chain reorg after a segmentation, transactions need to be able to get into the chain in a later block. The OP_BLOCKNUMBER transaction and all its dependants would become invalid. This wouldn't be fair to later owners of the coins who weren't involved in the time limited transaction.

Activity: 416


Ignore


OP_BLOCKNUMBER does not introduce any new vulnerabilities compared to the existing system as segmentation can be exploited to defraud people at the moment. This is accomplished as follows:


An opportunistic attacker has clients running in multiple locations around the world. The attacker's clients have the same wallets and connect to different subsets of peers, probably preferring local ones and definitely keeping in touch with local mining peers. The clients communicate with each other at intervals to check whether the network has segmented and exchange the list of peers that they are talking to. If communication is lost to one or more of the attacker's clients (they go offline) then the remaining clients attempt to communicate with all the offline client's peers. If they all succeed then it's likely that that attacker's client has just crashed or lost its internet connection. If however that client goes offline and a number of the peers are uncontactable then it's possible that the network has segmented. The attacker's clients determine whether they are on the network portion with the majority of the mining power or the minority. They also guess whether the other inaccessible portion of the network has enough mining power to generate blocks over the time it is imagined to be isolated. If the conditions are favourable then the attack proceeds as follows:

The attacker's clients on the majority of the network send coins from the wallet to new addresses in plausible innocent looking transactions. The attacker's clients on the minority of the network use the same coins in the same wallet to buy whatever goods they can find for sale on the subnetwork. When the network joins up again, it's highly likely that the majority part of the network has generated more blocks and all the transactions in blocks on the minority part of the chain re-enter the transaction pool. The attacker's transactions on the shorter chain are discarded as the coins have already been spent on the longer chain. Fraud complete!

So you can see that OP_BLOCKNUMBER does not introduce any new risks and that the real prevention of segmentation-based fraud must rely on some sort of detection of the loss of mining power.

ByteCoin

theymos
Administrator
Legendary


 **Re: Need OP_BLOCKNUMBER to allow "time" limited transactions**
November 18, 2010, 02:22:26 AM

#9


Problems with OP_BLOCKNUMBER might happen accidentally, whereas exploiting segmentation for double-spending is very difficult and requires someone to be attacking you.

Activity: 2142



1NXy0J5xU91Jp83XFV MHwwTUyZFK64BoAD

ByteCoin
Sr. Member


 **Re: Need OP_BLOCKNUMBER to allow "time" limited transactions**
November 18, 2010, 03:01:45 AM

#10

Quote from: theymos on November 18, 2010, 02:22:26 AM

Problems with OP_BLOCKNUMBER might happen accidentally, whereas exploiting segmentation for double-spending is very difficult and requires someone to be attacking you.

Activity: 416



Ignore


OP_BLOCKNUMBER transactions are not understood by the current client and their use should come with the proviso that under certain rare conditions problems might occur without any malicious intent. Exactly how rare is made clear below.

At the moment, if you send BTC to an address and for some reason the owner has lost the private key then your coins are lost forever. Payees can lose private keys due to hacking activity, hardware theft, hard disc crashes etc.. OP_BLOCKNUMBER transactions would allow you to recover your money and the transaction could imply a reversion time of months or years in future. In order for a segmentation to accidentally cause problems then the coins would have to go unspent until the deadline was just about to expire at which point the network would have to segment at which point the payee would have to be in the minority portion and try to spend them at which point the network would have to stay segmented until the reversion time had expired. That's a long list of coincidences for it to happen by accident.

On the other hand, exploiting segmentation for double spending is not difficult. Please show me what is difficult about the method I posted. All that is required is one adequately prepared attacker waiting for the network to segment. Anyone on the minority network portion offering goods or services for sale is at risk.

ByteCoin

MoonShadow
Legendary


 **Re: Need OP_BLOCKNUMBER to allow "time" limited transactions**
November 18, 2010, 04:35:33 AM

#11

Quote from: ByteCoin on November 18, 2010, 03:01:45 AM

On the other hand, exploiting segmentation for double spending is not difficult. Please show me what is difficult about the method I posted. All that is required is one adequately prepared attacker waiting for the network to segment. Anyone on the minority network portion offering goods or services for sale is at risk.

Activity: 1596

Ron
2012

Yet a system wide segmentation is fairly easy to detect, the current client just doesn't do it. If code implementing my 'watchdog' idea were included, the client could be set to suspend automatic trading on websites or warn the user of a fault on interactive clients.

Ignore

"The powers of financial capitalism had another far-reaching aim, nothing less than to create a world system of financial control in private hands able to dominate the political system of each country and the economy of the world as a whole. This system was to be controlled in a feudalist fashion by the central banks of the world acting in concert, by secret agreements arrived at in frequent

RHorning
Full Member

Re: Need OP_BLOCKNUMBER to allow "time" limited transactions
November 18, 2010, 09:10:36 PM

#12

Activity: 210

Ignore

Quote from: ByteCoin on November 18, 2010, 03:01:45 AM

Quote from: theymos on November 18, 2010, 02:22:26 AM

Problems with OP_BLOCKNUMBER might happen accidentally, whereas exploiting segmentation for double-spending is very difficult and requires someone to be attacking you.

At the moment, if you send BTC to an address and for some reason the owner has lost the private key then your coins are lost forever. Payees can lose private keys due to hacking activity, hardware theft, hard disc crashes etc.. OP_BLOCKNUMBER transactions would allow you to recover your money and the transaction could imply a reversion time of months or years in future. In order for a segmentation to accidentally cause problems then the coins would have to go unspent until the deadline was just about to expire at which point the network would have to segment at which point the payee would have to be in the minority portion and try to spend them at which point the network would have to stay segmented until the reversion time had expired. That's a long list of coincidences for it to happen by accident.

On the other hand, exploiting segmentation for double spending is not difficult. Please show me what is difficult about the method I posted. All that is required is one adequately prepared attacker waiting for the network to segment. Anyone on the minority network portion offering goods or services for sale is at risk.

ByteCoin

If there is anything that I've discovered about computers and released software, that any sort of unlikely series of events, not matter how unlikely, are bound to happen in a sort of perverse Murphy's Law sort of situation. In other words, if it can happen, it will happen and happen in the most annoying way possible. One sure sign of an amateur software developer, or at least somebody green to the field, is one who dismisses rare or exceptional circumstances to ever happen.

I believe in coincidence and depend upon it to occur even if it is rare. Indeed a bulk of the computer software I ever write is to deal with those very seldom exceptions with code that is rarely if ever executed. When you are talking networked computers, the chance for exceptional situation to happen seems to increase even more substantially because there are many more variables involved. You even get quantum effect showing up where bits get flipped and other hardware "glitches" which cause all kind of other issues. Sometimes I'm amazed that software works at all half the time.

1FLK3uUT3Vup5JtkGJVXKHAoS3AZWPcKdv

Pages: [1]

print

« previous topic
next topic »

Bitcoin Forum > Bitcoin > Development & Technical Discussion (Moderator: gmaxwell) > **Need OP_BLOCKNUMBER to allow "time" limited transactions**

Jump to: => Development & Technical Discussion go

Sponsored by Private Internet Access, a Bitcoin-accepting VPN.



Powered by SMF 1.1.19 | SMF © 2006-2009, Simple Machines

