The following are a series of emails from Satoshi Nakamoto to Hal Finney, written in January 2009 as the two were working on early versions of the bitcoin software. Mr. Finney supplied these emails to The Wall Street Journal in the spring of 2014.

Since these emails were all coming from Nakamoto to Mr. Finney, they are Nakamoto's responses to Mr. Finney's emails, the body of which is marked by the > symbol. The exchange begins on Jan. 10, 2009, and ends on Jan. 24, 2009, and comprises the time they were working on versions 0.1.0 through 0.1.3 of the bitcoin software.

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sat, Jan 10, 2009 at 11:52 AM
Subject: RE:Crash in bitcoin 0.1.0
To: hal.finney@gmail.com

Normally I would keep the symbols in, but they increased the size of the EXE from 6.5MB to 50MB so I just couldn't justify not stripping them. I guess I made the wrong decision, at least for this early version. I'm kind of surprised there was a crash, I've tested heavily and haven't had an outright exception for a while. Come to think of it, there isn't even an exception print at the end of debug.log. I've been testing on XP SP2, maybe SP3 is something.

I've attached bitcoin.exe with symbols. (gcc symbols for gdb, if you're using MSVC I can send you an MSVC build with symbols)

Thanks for your help!

>Hi Satoshi - I tried running bitcoin.exe from the 0.1.0 package, and
>it crashed. I am running on an up to date version of XP, SP3. The
>debug.log output is attached. There was also a file db.log but it was
>empty.
>
>The crash allowed me to start up a debugger, but there were no
>symbols. The exception was at address 00930AF7. The displayed call
>stack was 942316 called by 508936.
>
>When I have a chance, I'll try building it, although it looks like it

>would take me a while to acquire all the dependencies.
>
>Hal

From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sat, Jan 10, 2009 at 2:59 PM
Subject: Re: Crash in bitcoin 0.1.0
To: hal.finney@gmail.com

I was temporarily able to reproduce the bug and narrowed it down to the "mapAddresses.count" in the following code. It was absolutely the last piece of code to go in and mainly only got tested with the MSVC build. It's not essential and I'm inclined to turn off optimization and delete the section of code until I figure out what's going on.

I'm attaching a dbg exe you can try that deletes the line of code and turns off optimization. I'm not able to reproduce it anymore at the moment.

irc.cpp:

```
if (pszName[0] == 'u')
{
   CAddress addr;
   if (DecodeAddress(pszName, addr))
   {
      CAddrDB addrdb;
      if (AddAddress(addrdb, addr))
         printf("new  ");
      else
      {
         // make it try connecting sooner
         CRITICAL_BLOCK(cs_mapAddresses)
            if (mapAddresses.count(addr.GetKey()))
               mapAddresses[addr.GetKey()].nLastFailed = 0;
      }
      addr.print();
   }
   else
   {
      printf("decode failed\n");
```

```
    }
}
```

>Yes, actually the version with MSVC symbols would be better, that is
>the one I am using.
>
>I found that if I launched this one from a cygwin shell, it does not
>crash. But if I launch it from Windows, double-clicking on the file,
>it does crash similarly to the previous version. However, I am pretty
>sure that the previous version did crash even when I launched it from
>cygwin.
>
>I have to go out but I'll leave this version running for a while.
>
>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sat, Jan 10, 2009 at 6:55 PM
Subject: Re: Crash in bitcoin 0.1.0
To: hal.finney@gmail.com

I isolated the problem. If I spawn a thread and do
mapAddresses.count, even as the very first thing in the program,
it segfaults. The workaround is to needlessly call
mapAddresses.count in the main thread once and it's fine from then
on. I hate to blame the compiler, and I've never had a GCC
compiler bug before, but this feels like one. Maybe some bit of
init code it tries to optimize out if it's not called at least once
in the same thread, or some STL optimization that's not thread
friendly. I'm really dismayed to have this botch up the release
after all that stress testing.

The attached file: bitcoin-0.1.1.rar (filesize 2,132,686) is the
version where I deleted the mapAddresses.count line, and that

should be the safest version. (that was the only use of
mapAddresses.count) If you could try this version and confirm
that the crash is fixed, I'd appreciate it.

Thanks,
Satoshi

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sat, Jan 10, 2009 at 7:11 PM
Subject: Re: Crash in bitcoin 0.1.0
To: hal.finney@gmail.com

OK, thanks. The one in bitcoin-0.1.1-exe-dbg.rar is the same build as in bitcoin-0.1.1.rar.

I forgot, when you build debug on MSVC, it uses the debug versions of the runtime DLLs, which aren't included with Windows distributions. Actually, MSVC 6.0's runtime (MSVC60.DLL) is the last version that shipped preinstalled on Windows, which is why the continued interest in that ancient version of the compiler. Later Visual C versions can't create a standalone EXE that doesn't require additional runtime packages installed.

I can't use MSVC 6.0 for the release because its optimization of the SHA-256 routines is too slow.

I've attached a copy of the debug runtime DLLs. (They're redistributable)

>Hi Satoshi - The version with the .pdb file did not run for me, I got
>an error about MSVCP60D.DLL not being found. I imagine this is due to
>the version incompatibility you were worried about.
>
>The next version, that deleted the questionable line of code and
>turned off optimization, seems to run fine for me. So the problem may
>be related to that bit.
>

>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sun, Jan 11, 2009 at 4:36 PM
Subject: How's v0.1.2 going?
To: hal.finney@gmail.com

Well this doesn't look good. After you upgraded to 0.1.2, your node responded to one or two messages and then stopped replying to messages. It's still accepting connections and seems to be alive on IRC. That could happen if ThreadSocketHandler or ThreadMessageHandler is hung or crashed or blocked. Usually when there's an exception or other problem, it only stops the affected thread and everything else keeps running.

I'm attaching the msvc debug version in case you need it.

Satoshi

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sun, Jan 11, 2009 at 4:49 PM
Subject: v0.1.2 gcc debug build attached
To: hal.finney@gmail.com

Could you send me your debug.log?

The gcc debug version is attached.

gdb is easier to use than you'd think. gdb.exe is the only file. You run
gdb bitcoin.exe
then type "run"
then if it crashes, type "backtrace" for a stack dump, or it may do it automatically. (The stack trace doesn't always go far enough back unfortunately)

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sun, Jan 11, 2009 at 5:25 PM
Subject: Re: v0.1.2 debug.log
To: hal.finney@gmail.com

OK, so no crash or exception window or anything. debug.log is all I need then.

It looks like there's a "select failed: 10038" error (the sockets select function failed) and then network communication goes quiet after that (except for IRC which is still working). I've never had select fail before. It looks like sockets is somehow partially hosed. At least now I know what's wrong now.

You should restart it. It's not doing anything right now. I don't know if it'll just get the "select failed" error again, or be fine for a while.

If I can't think of anything else, I can always shut down and restart sockets if it gets hosed like that. I'm sure everyone who's written an internet app like a browser or p2p app had to slog through all the ways the Internet can trash you. The Internet is a brutal, rough and tumble place.

The issue of bitcoin.exe still running after you close it is a known issue. It does a careful shutdown of everything to be extra safe, in case some important transaction is in progress, but it's completely fine and totally safe to just kill it if it doesn't exit on its own. I'll have to work on figuring out what's getting hung up. I may just have it kill itself after a timeout.

Thanks!

>Hi Satoshi - debug.log attached. When I started 0.1.2 this afternoon,
>I first quit the previous version which was running. However, 0.1.2
>would not start up. Looking at the debug log, it said "Existing
>instance found". I ran task manager, and found two processes called
>bitcoin.exe running. I killed them both and started up the new one,
>and it seemed to run OK. It says at the bottom "3 connections". I
>haven't tried the debug version, I'm not sure what I would look for.
>
>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sun, Jan 11, 2009 at 9:31 PM
Subject: select failed 10038 fix
To: hal.finney@gmail.com

I believe I've fixed the bug related to "select failed: 10038" (error WSAENOTSOCK). The select error is not a big deal, but it led the communications thread to get blocked on a socket that should have been in non-blocking mode but wasn't. It never came up until now because as long as select never failed, receive would never be called unless there was data.

Without this fix, your node's communication sometimes goes dead. Connections are still made, but no data is passed. Any generated blocks would probably not be accepted since you can't broadcast them and other nodes will leave your branch behind. That's why Generate doesn't run when you're not connected.

This could also have caused bitcoin.exe to fail to exit. There's no reason for shutdown to wait for the com thread, so I made it only wait for the message processing thread. I'll do a more thorough forced shutdown later.

Looks like your node's com thread just now got blocked on this bug again. It went for a few hours this time before it did.

Version 0.1.3 exe attached.

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Mon, Jan 12, 2009 at 8:41 AM
Subject: Re: select failed 10038 fix
To: hal.finney@gmail.com

It definitely looks like 0.1.3 solved it. It was getting so there were so many zombie nodes, I was having a hard time getting a reply to any of my messages. Now, four inventory messages go out, four getdata messages come back.

Did you get any "not accepted" blocks? The connectivity bug could have caused a generated block not to be accepted if the node wasn't able to broadcast at the time. Once the status is above 5 or so it's safely accepted.

Unfortunately, I can't receive incoming connections from where I am, which has made things more difficult. Your node receiving incoming connections was the main thing keeping the network going the first day or two.

You can send to my Bitcoin address if you want to, but you won't get to see the full transfer sequence:
1NSwywA5Dvuyw89sfs3oLPvLiDNGf48cPD

You could always findstr /c:"version message" debug.log and send a test to some random person you're connected to near the end of the list. The ones ending in port 8333 can receive connections.

I just thought of something. Eventually there'll be some interest in brute force scanning bitcoin addresses to find one with the first few characters customized to your name, kind of like getting a phone number that spells out something. Just by chance I have my initials.

Satoshi

>Thanks, Satoshi, this new version seems to be running much better.
>I've got 8 connections, and watching debug.log there seems to be quite
>a bit of activity. I see you sent me a payment, thanks! Let me know
>your address and I will try sending one to you. I managed to generate
>a block yesterday and the coins are about to mature, if I understand
>it correctly.
>
>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Mon, Jan 12, 2009 at 10:50 AM
Subject: Re: select failed 10038 fix
To: hal.finney@gmail.com

Could you send me the debug.log from the 0.1.3 crash?
I can usually get a lot just from that.

I'll send you the debug builds shortly.

>Looks like 0.1.3 crashed during the night, unfortunately. Next time I
>will try running the debug version. Today I am working and will need
>to take this computer up and down quite a bit, so I won't be able to
>run it for most of the day. Tonight I will try to look at it a little
>bit.
>
>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Mon, Jan 12, 2009 at 11:26 AM
Subject: Re: v0.1.3 msvc debug build
To: hal.finney@gmail.com

Here's the 0.1.3 MSVC debug build

>Looks like 0.1.3 crashed during the night, unfortunately. Next time I
>will try running the debug version. Today I am working and will need
>to take this computer up and down quite a bit, so I won't be able to
>run it for most of the day. Tonight I will try to look at it a little
>bit.

>
>Hal
>
>On Mon, Jan 12, 2009 at 8:41 AM, Satoshi Nakamoto <satoshi@vistomail.com> wrote:
>> It definitely looks like 0.1.3 solved it. It was getting so there
>> were so many zombie nodes, I was having a hard time getting a
>> reply to any of my messages. Now, four inventory messages go out,
>> four getdata messages come back.
>>
>> Did you get any "not accepted" blocks? The connectivity bug could
>> have caused a generated block not to be accepted if the node
>> wasn't able to broadcast at the time. Once the status is above 5
>> or so it's safely accepted.
>>
>> Unfortunately, I can't receive incoming connections from where I
>> am, which has made things more difficult. Your node receiving
>> incoming connections was the main thing keeping the network going
>> the first day or two.
>>
>> You can send to my Bitcoin address if you want to, but you won't
>> get to see the full transfer sequence:
>> 1NSwywA5Dvuyw89sfs3oLPvLiDNGf48cPD
>>
>> You could always findstr /c:"version message" debug.log and send a
>> test to some random person you're connected to near the end of the
>> list. The ones ending in port 8333 can receive connections.
>>
>> I just thought of something. Eventually there'll be some interest
>> in brute force scanning bitcoin addresses to find one with the
>> first few characters customized to your name, kind of like getting
>> a phone number that spells out something. Just by chance I have
>> my initials.
>>
>> Satoshi
>>
>>>Thanks, Satoshi, this new version seems to be running much better.
>>>I've got 8 connections, and watching debug.log there seems to be quite
>>>a bit of activity. I see you sent me a payment, thanks! Let me know
>>>your address and I will try sending one to you. I managed to generate
>>>a block yesterday and the coins are about to mature, if I understand
>>>it correctly.
>>>

>>>Hal
>>>
>>>On Sun, Jan 11, 2009 at 9:31 PM, Satoshi Nakamoto <satoshi@vistomail.com> wrote:
>>>> I believe I've fixed the bug related to "select failed: 10038"
>>>> (error WSAENOTSOCK). The select error is not a big deal, but it
>>>> led the communications thread to get blocked on a socket that
>>>> should have been in non-blocking mode but wasn't. It never came
>>>> up until now because as long as select never failed, receive would
>>>> never be called unless there was data.
>>>>
>>>> Without this fix, your node's communication sometimes goes dead.
>>>> Connections are still made, but no data is passed. Any generated
>>>> blocks would probably not be accepted since you can't broadcast
>>>> them and other nodes will leave your branch behind. That's why
>>>> Generate doesn't run when you're not connected.
>>>>
>>>> This could also have caused bitcoin.exe to fail to exit. There's
>>>> no reason for shutdown to wait for the com thread, so I made it
>>>> only wait for the message processing thread. I'll do a more
>>>> thorough forced shutdown later.
>>>>
>>>> Looks like your node's com thread just now got blocked on this
>>>> bug again. It went for a few hours this time before it did.
>>>>
>>>> Version 0.1.3 exe attached.

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Mon, Jan 12, 2009 at 11:39 AM
Subject: Re: v0.1.3 gcc debug build
To: hal.finney@gmail.com

and the gcc debug build w/gdb.exe

>Looks like 0.1.3 crashed during the night, unfortunately. Next time I
>will try running the debug version. Today I am working and will need
>to take this computer up and down quite a bit, so I won't be able to

>run it for most of the day. Tonight I will try to look at it a little
>bit.
>
>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Mon, Jan 12, 2009 at 11:59 PM
Subject: Re: select failed 10038 fix
To: hal.finney@gmail.com

Definitely the disk full. I completely put off disk full
handling until a later version. Probably about time I did it now.

Well, that's a relief.

Satoshi

>Hi Satoshi - Sorry I have not been able to do more today, this looks
>like a busy week for me. I started 0.1.3 again under the MSVC debugger
>this time so if it crashes tonight I may be able to get some more
>information.
>
>I remember now that last night, my disk filled up. I had downloaded a
>bunch of the dependencies (boost, etc) with an eye towards trying to
>build it myself, and my disk was already pretty full. I'm pretty sure
>this is what caused 0.1.3 to crash. I've attached the debug.log, which
>also includes some other runs. The error is about 1/3 of the way down
>and says,
>
>EXCEPTION: NSt8ios_base7failureE
>CAutoFile::read : end of file
>
>Normally this should be a rare occurrence with the large disk sizes
>people have today.

>
>Hal
>
>On 1/12/09, Satoshi Nakamoto <satoshi@vistomail.com> wrote:
>> Could you send me the debug.log from the 0.1.3 crash?
>> I can usually get a lot just from that.
>>
>> I'll send you the debug builds shortly.
>>
>>
>>>Looks like 0.1.3 crashed during the night, unfortunately. Next time I
>>>will try running the debug version. Today I am working and will need
>>>to take this computer up and down quite a bit, so I won't be able to
>>>run it for most of the day. Tonight I will try to look at it a little
>>>bit.
>>>
>>>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Tue, Jan 13, 2009 at 2:42 PM
Subject: Re: disk full
To: hal.finney@gmail.com

If you build the dependencies, let me know how that goes. Everything is always harder to build on Windows than Linux. I've always hated projects with a lot of big dependencies, but there's no avoiding it, each one is essential.

I still haven't figured out how you managed to get a read exception rather than a write exception when your disk filled up. It's unlikely but maybe possible that the incident could have messed up your block data file. In that case, it might manifest as a similar exception again, or if your block count in the status bar stopped going up, that would also indicate a problem. As of this moment it's at 375 blocks.

If there is a problem, it could easily be solved by deleting your block files, as follows:

```
(exit Bitcoin and make sure it's stopped)
cd /d "%appdata%\bitcoin"
(backup this directory first)
del blk0001.dat
del blkindex.dat
```

It'll then re-download the block chain. Your transactions and
generated blocks show as 0/unconfirmed until it's done downloading.

The crucial file to backup is wallet.dat. If bitcoin is running
then you have to backup the whole %appdata%\bitcoin directory
including the database subdirectory, but even if it's not running
it certainly feels safer to always backup the whole directory.

The database unfortunately names its files "log.0000000001". To
the rest of the world, "log" means delete-at-will, but to database
people it means delete-and-lose-everything-in-your-other-files. I
tried to put them out of harm's way by putting them in the
database subdirectory. Later I'll write code to flush the logs
after every wallet change so wallet.dat will be standalone safe
almost all the time.

Satoshi

>Hi Satoshi - Sorry I have not been able to do more today, this looks
>like a busy week for me. I started 0.1.3 again under the MSVC debugger
>this time so if it crashes tonight I may be able to get some more
>information.
>
>I remember now that last night, my disk filled up. I had downloaded a
>bunch of the dependencies (boost, etc) with an eye towards trying to
>build it myself, and my disk was already pretty full. I'm pretty sure
>this is what caused 0.1.3 to crash. I've attached the debug.log, which
>also includes some other runs. The error is about 1/3 of the way down
>and says,
>
>EXCEPTION: NSt8ios_base7failureE
>CAutoFile::read : end of file
>
>Normally this should be a rare occurrence with the large disk sizes

>people have today.
>
>Hal

---------- Forwarded message ----------
From: **Satoshi Nakamoto** <satoshi@vistomail.com>
Date: Sat, Jan 24, 2009 at 4:47 PM
Subject: Re: disk full
To: hal.finney@gmail.com

I hate duplicating code, but the compiler forces us. Copy the body of the function above it, like this:

```
   void insert(iterator it, const_iterator first, const_iterator last)
   {
      if (it == vch.begin() + nReadPos && last - first <= nReadPos)
      {
         // special case for inserting at the front when there's room
         nReadPos -= (last - first);
         memcpy(&vch[nReadPos], &first[0], last - first);
      }
      else
         vch.insert(it, first, last);
   }

#if !defined(_MSC_VER) || _MSC_VER >= 1300
   void insert(iterator it, const char* first, const char* last)
   {
      if (it == vch.begin() + nReadPos && last - first <= nReadPos)
      {
         // special case for inserting at the front when there's room
         nReadPos -= (last - first);
         memcpy(&vch[nReadPos], &first[0], last - first);
      }
      else
         vch.insert(it, first, last);
   }
#endif
```

The modified version of serialize.h is attached.

BTW, in my tests, VC8 produced an EXE that would only run on
systems that had VC8 installed on them. The error it gives
is extremely vague. I think they expect you to install a
package during setup, but bitcoin doesn't have a setup.

My testing has been with MSVC 6.0 SP6 and GCC 3.4.5.
GCC is the release build. There's nothing wrong with the
MSVC 6.0 build other than its optimization of the SHA routines
for generating blocks is slow.

Satoshi