# Did Dustin Trammell run Bitcoin before Hal Finney?

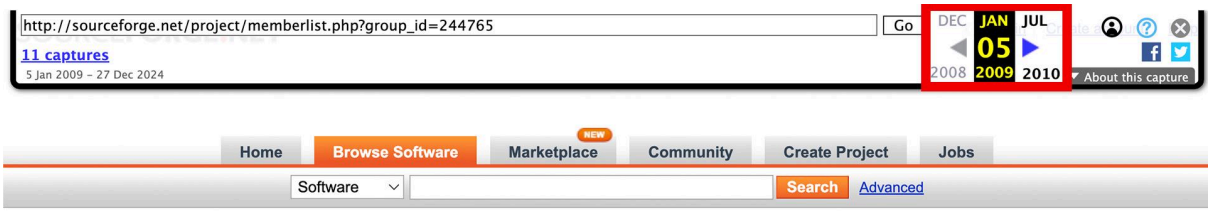
by Alex WALTZ

**NOTE FOR PUBLISHING**
All text in this format is to be deleted when the article is published.
This is used to identify the name and position of each picture on the article.

Most people know Hal Finney from the famous Running Bitcoin tweet (https://x.com/halfin/status/1110302988) he made at 3:33 AM Jan 11, 2009.

Considering that:

1. the tweet was made close to the launch of Bitcoin
2. it is kind of the only Bitcoin historical relic outside the Cryptography Mailing List at the time
3. Hal was a very well known and prolific cryptographer that worked on PGP and even made his own cryptocurrency RPOW
4. Hal had known known private conversations(which he later released) with Satoshi between the launch of the White Paper and the launch of Bitcoin
5. He mentioned in one Bitcointalk post, he **MAY** have been the 1st person to join the Bitcoin Network after satoshi
6. Hal was the 1st developer to be added to sourceforge by Satoshi





01 - Hal 1st Developer on Sourceforge

- https://web.archive.org/web/20090105145118/http://sourceforge.net/project/memberlist.php?group_id=244765

*On the 5th of January 2009, we can see Hal being the only other developer for the Bitcoin project on sourceforge along with Satoshi. Bitcoin was announced on the 8th.*

People automatically presumed **Hal was the 2nd person to join the Bitcoin Network**, right after Satoshi.
Today this is considered a well known fact, thousands of articles have been written about it, and Bitcoiners celebrate Hal's tweet every year.

While this is a very reasonable presumption, I wanted to see some concrete proof.
I could **not find anything** on the topic, so I decided to conduct my own investigation.

This led me to **discover the following never before known facts about the very seminal and fragile days of Bitcoin launch:**

- Hal missed Bitcoin's Launch
- Hal join Bitcoin around Block 49
- There were 2 nodes present when Hal joined
- Bitcoin halted for 24 hours and 8 hours in the first 30 blocks

But more importantly it allowed me to paint a **pretty vivid picture of how it must have been to participate in the launch of Bitcoin**, and how it must have felt to be one of the first people to try Bitcoin.

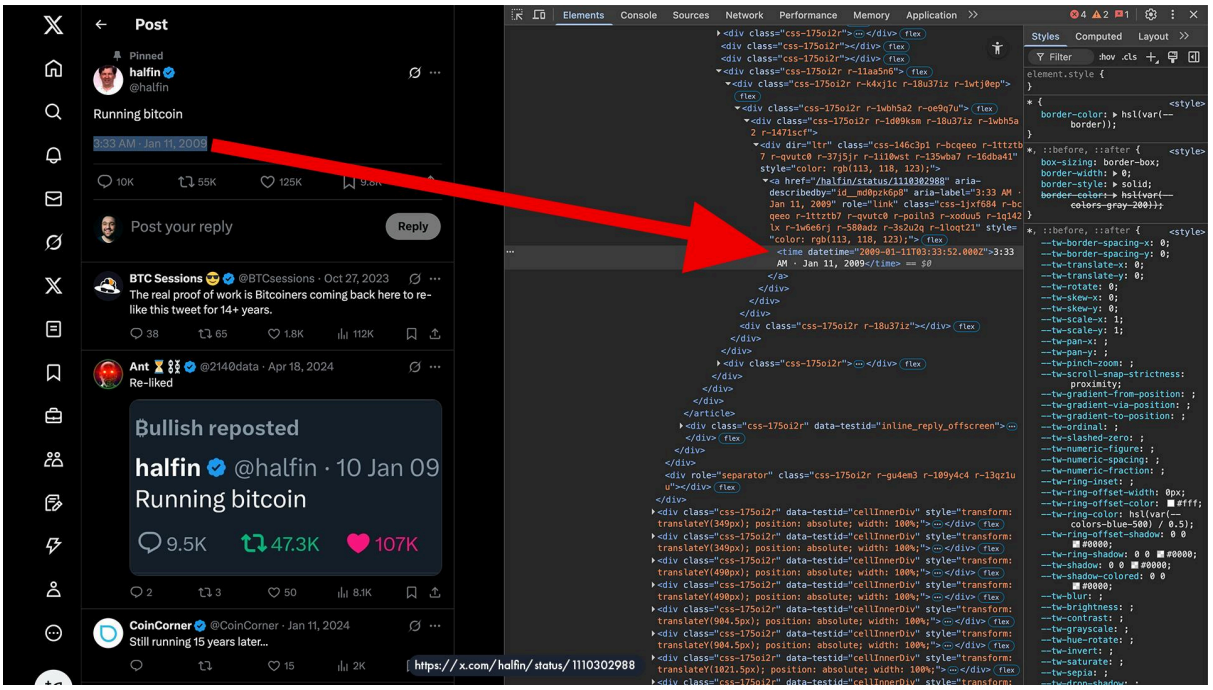
First I gathered all the events that lead to the Bitcoin Launch and Hal's tweet and converted them to the same timezone to make comparing them easier.
UTC is the best choice, since the Bitcoin Block Time is also saved in UTC.

For easier reading I will present screenshots of each relevant event and highlight with red squares and arrows the important information. This way you don't have to jump through tabs and have all the information present in this article.

Where necessary I will explain how certain information was extracted, or why we can trust the information as being accurate.
Under each screenshot I will also have the official source, so you can verify that I did not make up these facts, or if I made an error you can catch it.

**1st the "Running Bitcoin" tweet".**
We know the time zone in which X(Twitter) saves the time is UTC because if we inspect the source code of the website we can see 2009-01-11T03:33:52.000Z = Sunday, 11 January

2009 03:33:52, the Z stands for Zulu which is UTC+0000.




02 - Hal Tweet Inspect Element

- https://x.com/halfin/status/1110302988

Now let's go back in time a bit.

# Hal's private emails with Satoshi

Satoshi made himself publicly known to the world a few months before Hal's tweet, when he published the Bitcoin White Paper on the Cryptography Mailing List *Fri Oct 31 14:10:00 EDT 2008*

# Bitcoin P2P e-cash paper

**Satoshi Nakamoto** satoshi at vistomail.com
*Fri Oct 31 14:10:00 EDT 2008*

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ]

---

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
```

https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

03 - White Paper Post Crypto Mail List

- https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

*Before the White Paper announcement Satoshi exchanged a few private emails with Adam Back and Wei Dai since he added both of their previous work as references in the White Paper thus contacting them to check if he had the correct sources, so technically this is the first time the world heard of Satoshi Nakamoto, but that's not relevant to what we are looking at.*

Very few people took interest in Satoshi's White Paper, and Hal was one of them, replying to Satoshi's posts on the Cryptography Mail List.

The 1st reply was on Fri Nov 7 18:40:12 EST 2008

# Bitcoin P2P e-cash paper

**Hal Finney** hal at finney.org
*Fri Nov 7 18:40:12 EST 2008*

- Previous message: NIST Special Publication 800-108 Recommendation for Key Derivation Using Pseudorandom Functions
- Next message: This is a test. This is only a test...
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ]

---

```
Bitcoin seems to be a very promising idea. I like the idea of basing
security on the assumption that the CPU power of honest participants
outweighs that of the attacker. It is a very modern notion that exploits
the power of the long tail. When Wikipedia started I never thought it
would work, but it has proven to be a great success for some of the
same reasons.

I also do think that there is potential value in a form of unforgeable
token whose production rate is predictable and can't be influenced
by corrupt parties. This would be more analogous to gold than to fiat
currencies. Nick Szabo wrote many years ago about what he called "bit
```

https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html

- https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html

04 - Hal Response #1 Crypto List 7 Nov

And the 2nd on Thu Nov 13 11:24:18 EST 2008

# Bitcoin P2P e-cash paper

**Hal Finney** hal at finney.org
*Thu Nov 13 11:24:18 EST 2008*

- Previous message: Comment Period for FIPS 186-3: Digital Signature Standard
- Next message: Bitcoin P2P e-cash paper
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ]

---

```
James A. Donald writes:
> Satoshi Nakamoto wrote:
>  > When there are multiple double-spent versions of the
>  > same transaction, one and only one will become valid.
>
> That is not the question I am asking.
>
> It is not trust that worries me, it is how it is
> possible to have a  a globally shared view even if
> everyone is well behaved.
>
> The process for arriving at a globally shared view of
> who owns what bitgold coins is insufficiently specified.

I agree that the description is not completely clear on how these matters
are handled. Satoshi has suggested that releasing source code may be the
best way to clarify the design. As I have tried to work through details on
my own, it does appear that the rules become rather complicated and indeed
one needs at least a pseudo-code algorithm to specify the behavior. So
perhaps writing real code is not a bad way to go. I found that there is
a sourceforge project set up for bitgold, although it does not have any
code yet.
```

https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html

05 - Hal Response #2 Crypto List 13 Nov

- *https://www.metzdowd.com/pipermail/cryptography/2008-November/014848.html*

So from these two posts we know Hal was immediately interested in Bitcoin.

Not too long after Satoshi announced the Bitcoin White Paper, Hal, Satoshi and others started conversing in private, and we have access to these private conversations via this CoinDesk article that coincidentally also focuses on time stamps, but for different topic: https://web.archive.org/web/20220507011228/https://www.coindesk.com/markets/2020/11/26/previously-unpublished-emails-of-satoshi-nakamoto-present-a-new-puzzle/

The author of the article notes that Fran Finey (Hal's wife) confirmed the emails are authentic, according to the Editor's note in the article.

The first email in the CoinDesk article is dated 19 November 2008 (around White Paper launch), and does indeed confirm the start of the private conversations, but is of no interest to us.

So lets fast forward to Satoshi announcing Bitcoin v0.1 to the Cryptography Mailing List at
Thu Jan 8 14:27:40 EST 2009 = Thursday, 8 January 2009 19:27:40

# Bitcoin v0.1 released

**Satoshi Nakamoto** satoshi at vistomail.com
*Thu Jan 8 14:27:40 EST 2009*

- Previous message: [tmoore at seas.harvard.edu: [fc-announce] Financial Crypto February 23-26 in Barbados, Early Registration Deadline Approaching]
- Next message: MD5 considered harmful today, SHA-1 considered harmful tomorrow
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ]

---

```
Announcing the first release of Bitcoin, a new electronic cash
system that uses a peer-to-peer network to prevent double-spending.
It's completely decentralized with no server or central authority.

See bitcoin.org for screenshots.

Download link:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Windows only for now.  Open source C++ code is included.

- Unpack the files into a directory
- Run BITCOIN.EXE
- It automatically connects to other nodes
```

https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html

06 - Satoshi ANN Crypto List Bitcoin v0.1

- https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html

Shortly after the announcement on the Cryptography Mailing List, Satoshi writes an email to Hal, letting him know of the “official” launch.

As the email header (from CoinDesk article) shows, the email was received by Hal’s server at
Thu, 8 Jan 2009 20:54:55 -0800 (PST) = Friday, 9 January 2009 04:54:55 UTC

```
From satoshi@vistomail.com  Thu Jan  8 20:54:55 2009
Return-Path: <satoshi@vistomail.com>
X-Original-To: hal@finney.org
Delivered-To: hal@finney.org
Received: from mail.anonymousspeech.com (anonymousspeech.com [124.217.253.42])
        by finney.org (Postfix) with ESMTP id 467AA14F6E1
        for <hal@finney.org>; Thu,  8 Jan 2009 20:54:53 -0800 (PST)
Received: from server123 ([124.217.253.42]) by anonymousspeech.com with MailEnable ESMTP; Fri, 09 Jan 2009 13:32:28 +0800
MIME-Version: 1.0
Date: Fri, 09 Jan 2009 13:21:04 +0800
X-Mailer: Chilkat Software Inc (http://www.chilkatsoft.com)
X-Priority: 3 (Normal)
Subject: Bitcoin v0.1
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable
From: "Satoshi Nakamoto" <satoshi@vistomail.com>
Reply-To: satoshi@vistomail.com
To: hal@finney.org
Message-ID: <CHILKAT-MID-c4977816-955c-9f60-e4bf-19bded842d44@server123>
X-Bogosity: Ham, tests=bogofilter, spamicity=0.000000, version=1.0.3
Status: RO

Thought you'd like to know, the Bitcoin v0.1 release with
EXE and full sourcecode is up on Sourceforge:
http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

www.bitcoin.org has release notes and screenshots.

Satoshi
```

https://web.archive.org/web/20220507011230/https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/WQEY5CWEN5ASLKLCSGSL5ZNXLQ.png
https://web.archive.org/web/20220507011228/https://www.coindesk.com/markets/2020/11/26/previously-unpublished-emails-of-satoshi-nakamoto-present-a-new-puzzle

07 - CoinDesk Email #1 -  Thu, 8 Jan 2009 20-54-53

- https://web.archive.org/web/20220507011230/https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/WQEY5CWEN5ASLKLCSGSL5ZNXLQ.png

At some point Hal responds to Satoshi letting him know that he will take a look at Bitcoin over the weekend, remembering the mail was sent on Thursday(PST).

So we already know Hal missed the Bitcoin Launch just from this email alone.

We don't have the time stamps for this email (when these emails were shared, Satoshi's responses were of more interest), but we do have another email from Satoshi letting Hal know he is willing to answer any questions he might have.

Fri, 9 Jan 2009 08:08:37 -0800 (PST) - Friday, 9 January 2009 16:08:37 UTC

```
From satoshi@vistomail.com  Fri Jan  9 08:08:37 2009
Return-Path: <satoshi@vistomail.com>
X-Original-To: hal@finney.org
Delivered-To: hal@finney.org
Received: from mail.anonymousspeech.com (anonymousspeech.com [124.217.253.42])
        by finney.org (Postfix) with ESMTP id 220A414F6E1
        for <hal@finney.org>; Fri,  9 Jan 2009 08:08:35 -0800 (PST)
Received: from server123 ([124.217.253.42]) by anonymousspeech.com with MailEnable ESMTP; Sat, 10 Jan 2009 00:46:09 +0800
MIME-Version: 1.0
Date: Sat, 10 Jan 2009 00:43:01 +0800
X-Mailer: Chilkat Software Inc (http://www.chilkatsoft.com)
X-Priority: 3 (Normal)
Subject: Re: Bitcoin v0.1
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable
From: "Satoshi Nakamoto" <satoshi@vistomail.com>
Reply-To: satoshi@vistomail.com
To: hal@finney.org
Message-ID: <CHILKAT-MID-b1285368-fb47-d04a-88f6-bc6cb54e0f1d@server123>
X-Bogosity: Ham, tests=bogofilter, spamicity=0.000000, version=1.0.3
Status: O

Sure thing.  If you have any questions, feel free.

>Hi, Satoshi, thanks very much for that information! I should have a cha=
nce
>to look at that this weekend. I am looking forward to learning more abo=
ut
>the code -
>
>Hal
>
```

https://web.archive.org/web/20220507011230/https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/WQEY5CWEN5ASLKLCSGSL5ZNXLQ.png
https://web.archive.org/web/20220507011228/https://www.coindesk.com/markets/2020/11/26/previously-unpublished-emails-of-satoshi-nakamoto-present-a-new-puzzle

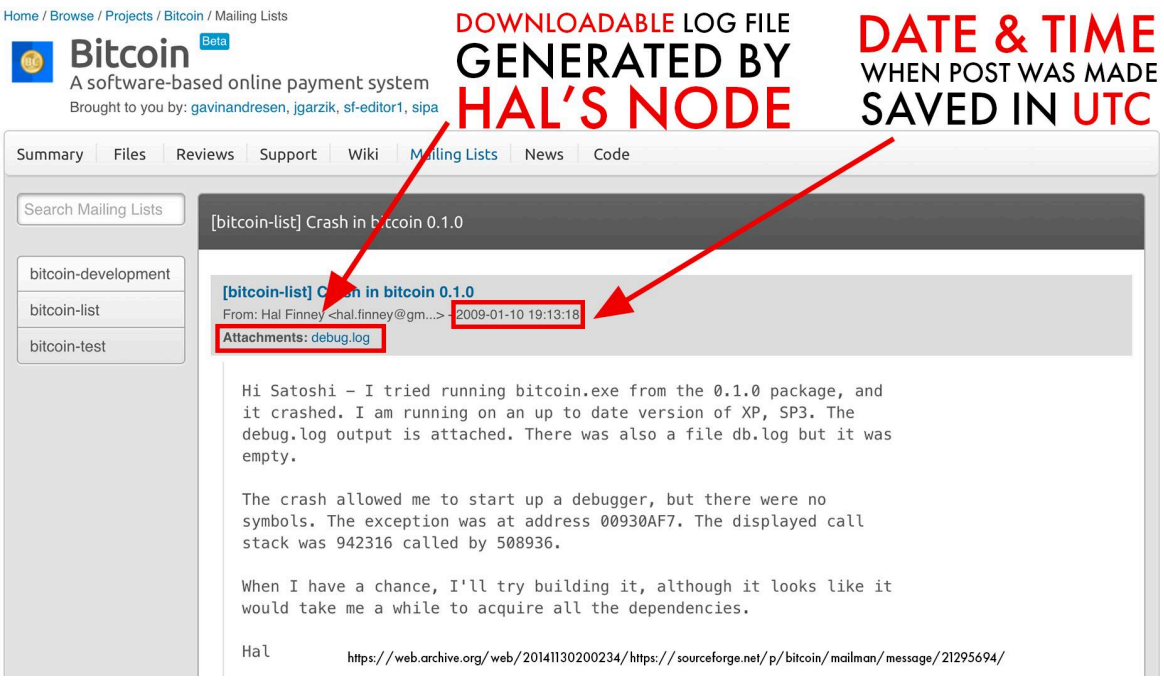
08 - CoinDesk Email #2 - Fri, 9 Jan 2009 08-08-35

- https://web.archive.org/web/20220507011230/https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/66FEUFUEIVC3LOIOA6ESVKGGKM.png

# Hal's debug.log file

For those of you who don't know, before Bitcoin used Github to host the code(and executables) it used Sourceforge, which also provided a discussion forum and mailing list.

It is here where Hal makes a post, the next day, after trying Bitcoin for the 1st time and it did not work for him on Saturday, 10 January 2009 19:13:18 UTC.
*The timezone of this mail list post is saved in UTC, the way I figured this out was by digging through other posts on sourceforge, but we will see later this aligns with the block times.*




09 - Sourceforge Post

- https://web.archive.org/web/20141130200234/https://sourceforge.net/p/bitcoin/mailman/message/21295694/

The most important finding here is that Hal included the **debug.log file** of this node.
In this file the node saves what it does in the background and it is here where we get our most important clue.

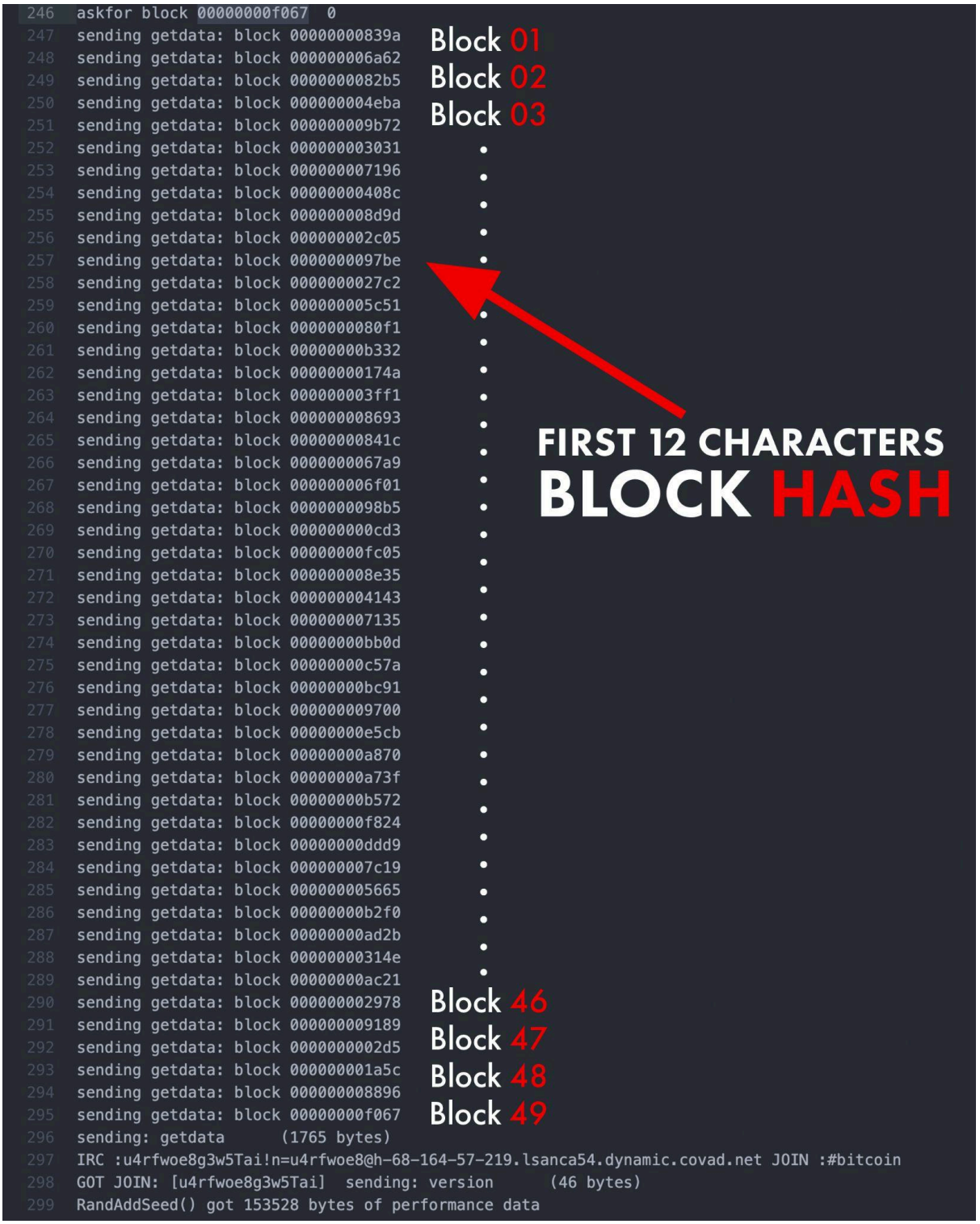
*Note: Node and client both refer to the same thing. The software that is used to communicate with the Bitcoin Network. I use both terms interchangeably throughout the article.*

You see back then Bitcoin worked quite differently, a node would connect to the #bitcoin IRC channel and it would find other peers on this channel and then connect to them. Think of this like a chat room that was used to coordinate finding peers.

The very lucky part is that **Internet Archive saved the attached file and we can still download it today,** just click on the name on the name above, but also direct link here: https://web.archive.org/web/20141130200234/https://sourceforge.net/p/bitcoin/mailman/attachment/da7b3ce30901101113v2ec6bf61xf018265479eb7faf%40mail.gmail.com/1/

So what can we see in this file?

We can see that Hal's node did find some peers, and then it asked the peers for bitcoin blocks.
We know for a fact these are Bitcoin blocks, as they are identified by 12 characters of the hash.




10 - Inside Log file

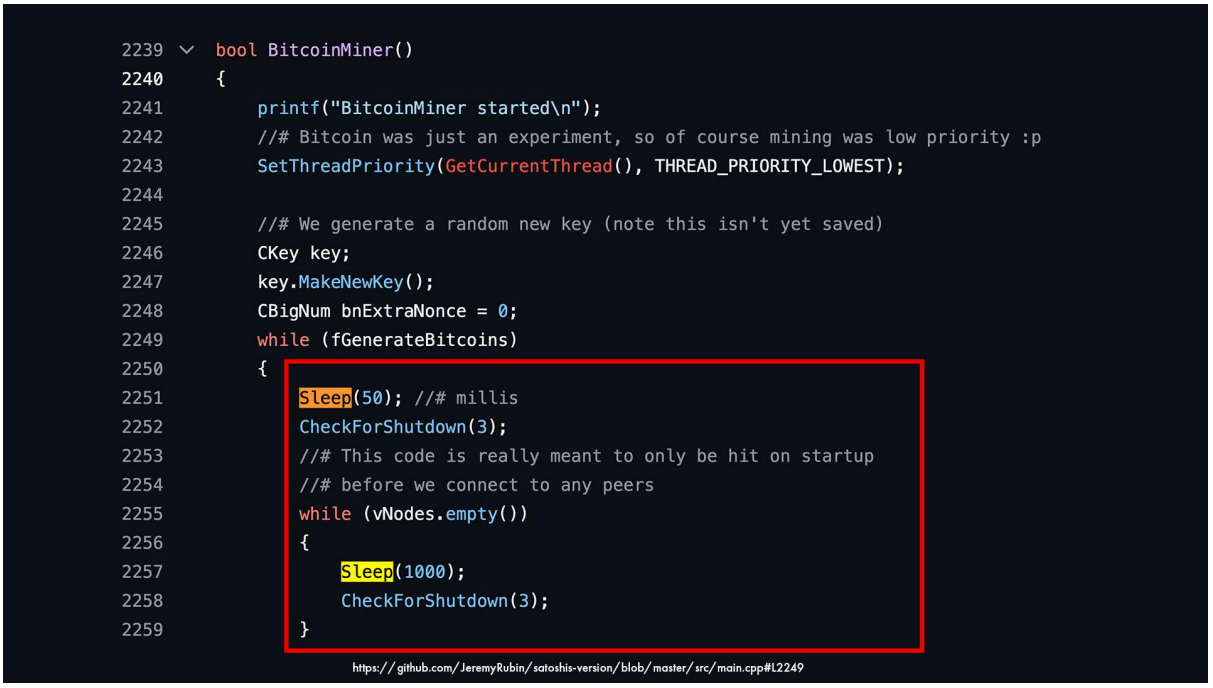
Even more, the fact that we have 49 hashes proves that Bitcoin(or at least this iteration) existed for AT LEAST 49 blocks, when Hal's node crashed.

*(worth mentioning that Bitcoin started with a very low difficulty so generating 49 Bitcoin blocks would not be quite that hard, however still serves of some proof of consistent mining)*


11 - Sourceforge + Log File + Block 49

But there is another very important piece of information.
In the 1st version of the Bitcoin code, Satoshi added a very interesting constraint.

The Bitcoin client would NOT start mining/produce blocks unless it has an established connection to other nodes. (ingoing OR outgoing)




12 - Wait for Peers

- https://github.com/JeremyRubin/satoshis-version/blob/master/src/main.cpp#L2249

Why did Satoshi add this?
My educated speculation is to avoid multiple Bitcoins starting in parallel at the same time

from the same genesis block.

It is worth mentioning that Satoshi **could have run multiple nodes on different machines**, but at this point it is hard to tell from the available information.
The important thing to note here is that different nodes does not necessarily mean a different person running them!

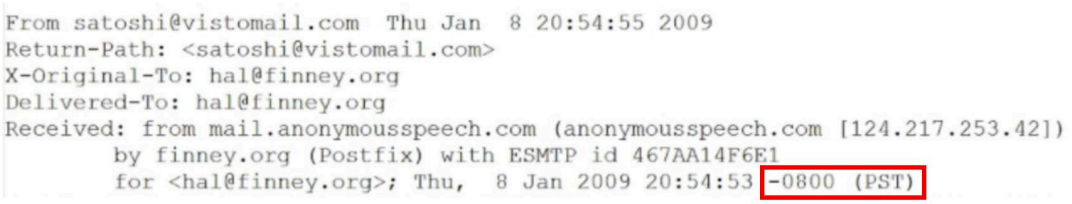
So from what we see in the debug.log file plus the constraint we see in the code, it means that **when Hal ran Bitcoin for the 1st time, another node/nodes**(beside Satoshi's obvious node) **was already on the network**, otherwise it would have not started generating blocks.

But there is more!
After Hal made the post on Sourceforge sharing that Bitcoin v0.1 was not working for him, Satoshi and Hal continued conversing in private, and Satoshi made modifications to the Bitcoin client based on the feedback he was getting from Hal.

AAAAAnd we are in luck yet again, because these private emails were shared by Hal with the WSJ in 2014 and can be found in an archived copy here:
https://web.archive.org/web/20220426194700mp_/https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf

These emails don't contain the detailed header information from Hal's email server like the ones from the Coindesk article do, just a timestamp with no time zone.
But it is safe to assume the timezone of these timestamps is PST because:

1. The previous emails(from CoinDesk) show very explicitly that Hal's server was indeed using the PST timezone




https://web.archive.org/web/20220507011230/https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/WQEY5CWEN5ASLKLCSGSL5ZNXLQ.png
https://web.archive.org/web/20220507011228/https://www.coindesk.com/markets/2020/11/26/previously-unpublished-emails-of-satoshi-nakamoto-present-a-new-puzzle/

13 - PST Time zone Hal's Mail Headers

2. He lived in California, which is on PST time

These emails were redacted (probably by Hal to make them easier to read) and focus on Satoshi responding to Hal's replies.

So the text that has > in front of it is text written by Hal, and the text that does not have > in front of it, is written by Satoshi.
The email headers (though not as verbose) still show the recipient and sender of the emails.

Sooo let's continue our investigation.
We left off when Hal posted on Sourceforge that Bitcoin v0.1 does not work for him.

We can see here Satoshi's direct response to the message in question, as it is quoting Hal's Sourceforge post at Sat, Jan 10, 2009 at 11:52 AM(PST) = Saturday, 10 January 2009 19:52:00 UTC

---------- 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!

SAME MESSAGE HAL POSTED ON SOURCEFORGE

>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

https://web.archive.org/web/20220426194700mp_/https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf

---

## 14 - WSJ #1 - Satoshi Responds To Hal's SF post

After some more back and forth we see in this email from Satoshi to Hal Sat, Jan 10, 2009 at 2:59 PM = Saturday, 10 January 2009 22:59:00 UTC that Hal did manage to get Bitcoin v0.1 to work and left it running for a while.

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.

>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

https://web.archive.org/web/20220426194700mp_/https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf

---

## 15 - WSJ #2 - Hal leaves v0.1 running for a while

However we as we will later see Hal's node did not work for too long..

In the meantime on the Cryptography Mailing List, Hal congratulates Satoshi on the release of Bitcoin v0.1
Sat Jan 10 21:22:01 EST 2009 = Sunday, 11 January 2009 02:22:01 UTC

# Bitcoin v0.1 released

**Hal Finney** hal at finney.org
*Sat Jan 10 21:22:01 EST 2009*

- Previous message: feds try to argue touch tone content needs no wiretap order
- Next message: What risk is being defended against here?
- **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ]

---

```
Satoshi Nakamoto writes:
> Announcing the first release of Bitcoin, a new electronic cash
> system that uses a peer-to-peer network to prevent double-spending.
> It's completely decentralized with no server or central authority.
>
> See bitcoin.org for screenshots.
>
> Download link:
> http://downloads.sourceforge.net/bitcoin/bitcoin-0.1.0.rar

Congratulations to Satoshi on this first alpha release.  I am looking
forward to trying it out.
```

https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html

16 - Hal congratulates Satoshi - Crypto Mail List

- https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html

The private conversations continue between the two, as Satoshi sends Hal, Bitcoin v0.1.1 at Sat, Jan 10, 2009 at 6:55 PM (PST) = Sunday, 11 January 2009 02:55:00 UTC

---------- 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

https://web.archive.org/web/20220426194700mp_/https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf

---

17 - WSJ #3 - Satoshi sends - bitcoin-0.1.1.rar

And an hour later the debug version bitcoin-0.1.1-exe-dbg.rar at Sat, Jan 10, 2009 at 7:11 PM (PST) = Sunday, January 11, 2009 at 03:11 UTC

---------- 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

https://web.archive.org/web/20220426194700mp_/https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf

18 - WSJ #4 - Satoshi sends - bitcoin-0.1.1-exe-dbg.rar

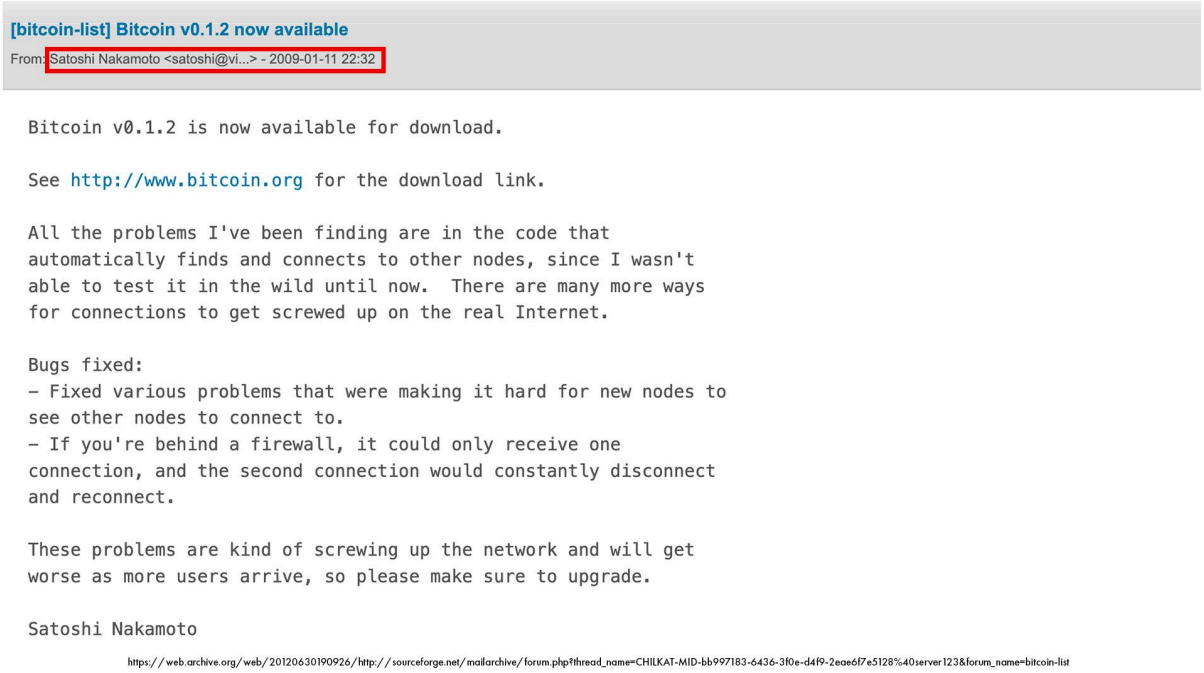
And 22 minutes later we get the Running Bitcoin tweet from Hal at 3:33 AM · January 11,2009 (UTC)

## 19 - Hal Makes the tweet

So we can even deduce what version Hal was running when he made the tweet.

But as fate has it, this version also crashed and the back and forth continues as they progress towards a working version.

Meanwhile Satoshi announces Bitcoin v0.1.2 on the Sourceforge mailing list at Sunday, 11 January 2009 22:32:00 UTC



**[bitcoin-list] Bitcoin v0.1.2 now available**

From: Satoshi Nakamoto <satoshi@vi...> - 2009-01-11 22:32

Bitcoin v0.1.2 is now available for download.

See http://www.bitcoin.org for the download link.

All the problems I've been finding are in the code that
automatically finds and connects to other nodes, since I wasn't
able to test it in the wild until now. There are many more ways
for connections to get screwed up on the real Internet.

Bugs fixed:
- Fixed various problems that were making it hard for new nodes to
see other nodes to connect to.
- If you're behind a firewall, it could only receive one
connection, and the second connection would constantly disconnect
and reconnect.

These problems are kind of screwing up the network and will get
worse as more users arrive, so please make sure to upgrade.

Satoshi Nakamoto

https://web.archive.org/web/20120630190926/http://sourceforge.net/mailarchive/forum.php?thread_name=CHILKAT-MID-bb997183-6436-3f0e-d4f9-2eae6f7e5128%40server123&forum_name=bitcoin-list

## 20 - Satoshi ANN SourceForge v0.1.2

- https://web.archive.org/web/20120630190926/http://sourceforge.net/mailarchive/forum.php?thread_name=CHILKAT-MID-bb997183-6436-3f0e-d4f9-2eae6f7e5128%40server123&forum_name=bitcoin-list

Next, Satoshi acknowledges that Hal ran v0.1.2 but broke and sends him the msvc debug version Sun, Jan 11, 2009 at 4:36 PM(PST) = Monday, 12 January 2009 00:36:00 UTC
*MSVC is the Microsoft Visual compiler for C++ that was used for Windows, and this debug version would allow for better inspection of certain errors.*

---------- 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.

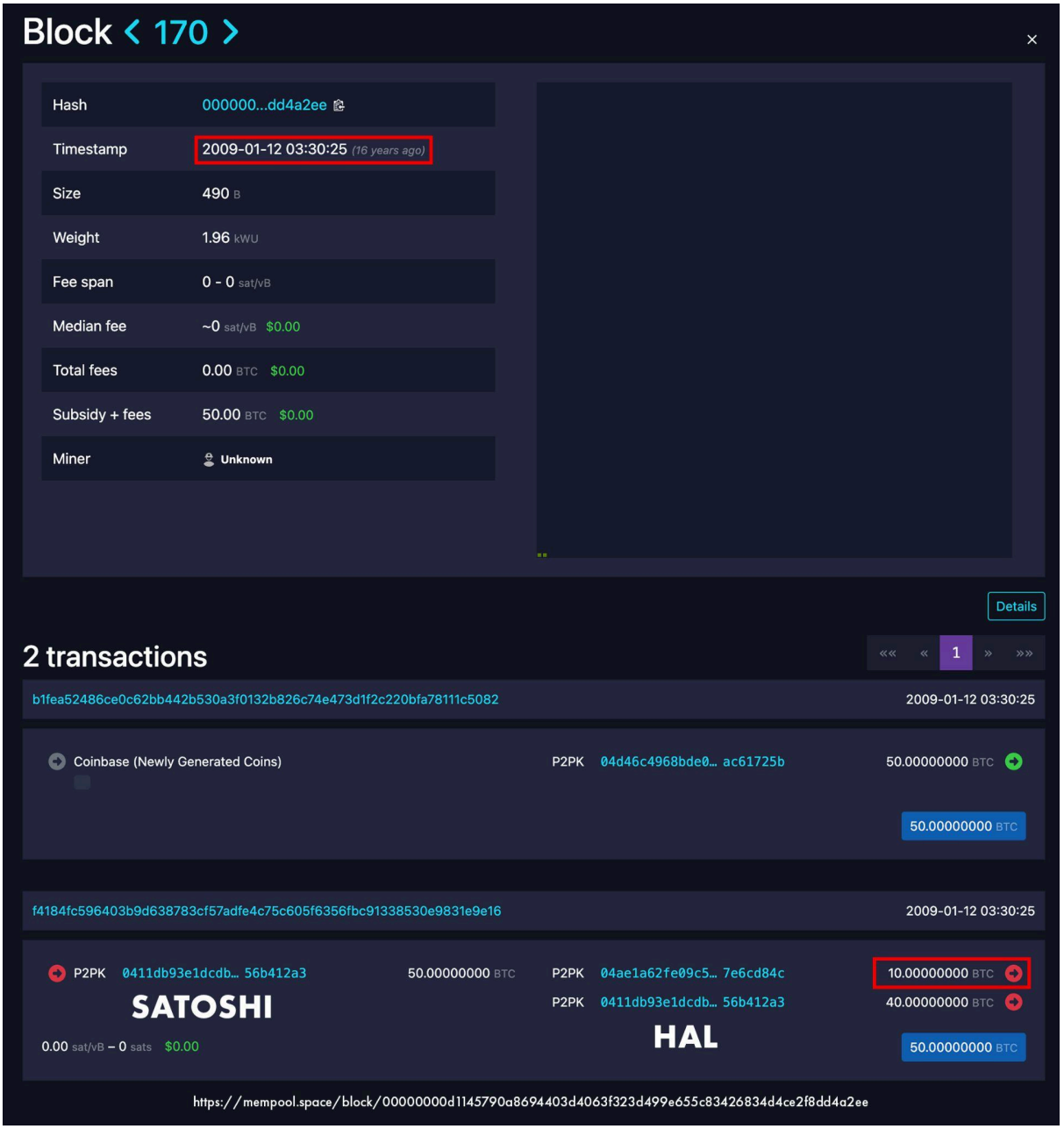
I'm attaching the msvc debug version in case you need it.

Satoshi

https://web.archive.org/web/20220426194700mp_/https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf

## 21 - Satoshi acknowledges Hal ran 0.1.2 and broke

And along comes Block 170, which is the 1st Bitcoin transfer ever made.




22 - Block 170

- https://mempool.space/block/00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee

And just 2 hours later at Sun, Jan 11, 2009 at 9:31 PM(PST) = Monday, 12 January 2009 05:31:00 UTC Hal receives Bitcoin v0.1.3 from Satoshi.

---------- 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.

https://web.archive.org/web/20220426194700mp_/https://online.wsj.com/public/resources/documents/finneynakamotoemails.pdf

23 - Satoshi sends v01.3 to Hal

And now we can infer what version Hal was running when the transaction took place.

# Bitcoin and me, bitcointalk post

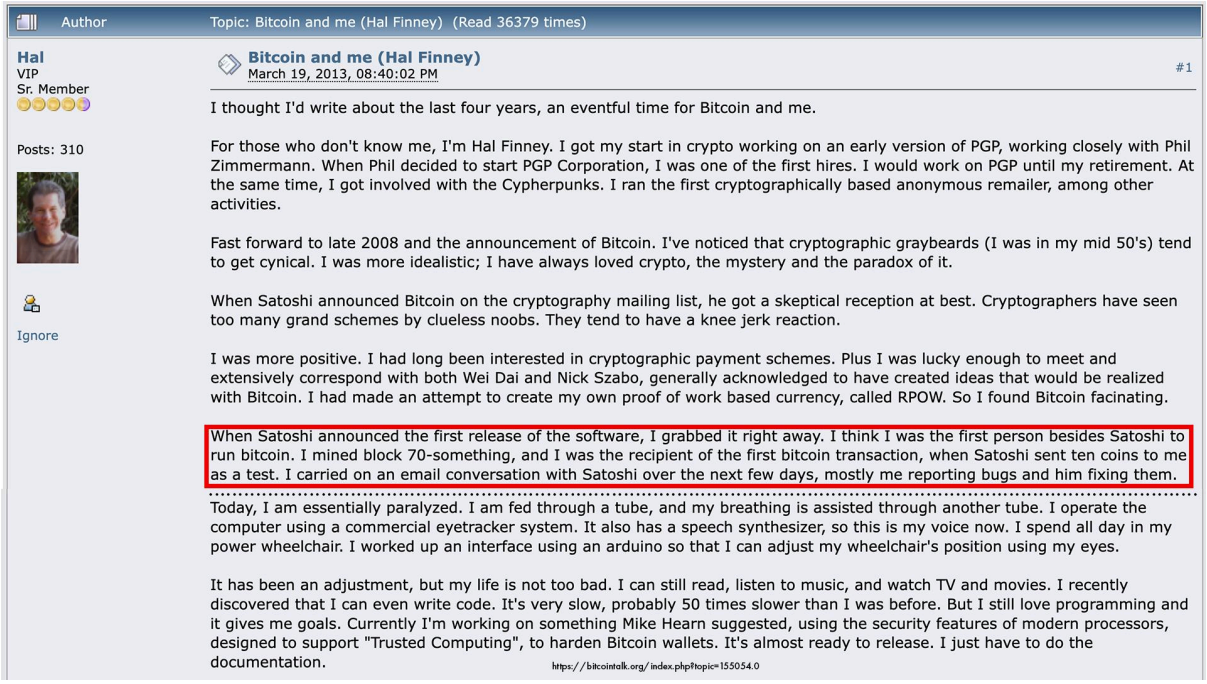
But before we add all the events to a table and analyse them, there is one more thing I want to bring to your attention.

In 2009 Hal Finey got diagnosed with ALS, and by 2013 he was paralysed and using his eye to operate the computer.
Under these conditions he wrote one of the most heartwarming and inspiring things I ever read in all my Bitcoin years.

Every now and then this post comes to my attention, and everytime I read it it just fills me with hope and I tell myself to remember the equanimity Hal found in this very difficult situation.

If there is anything you should remember from this article, it is Hal's Bitcointalk post, as whoever was 1st on the network, it's not that important, but this post shows what it means to be a great human no matter what life throws at you!

In the "Bitcoin and me" Bitcointalk post, Hal takes a look back at his life as a cryptographer and remembers the 1st few moments of Bitcoin (which we are analysing here) and mention 3 things of interest to our investigation:



Author | Topic: Bitcoin and me (Hal Finney) (Read 36379 times)

**Hal**
VIP
Sr. Member

Posts: 310

Ignore

**Bitcoin and me (Hal Finney)**
March 19, 2013, 08:40:02 PM #1

I thought I'd write about the last four years, an eventful time for Bitcoin and me.

For those who don't know me, I'm Hal Finney. I got my start in crypto working on an early version of PGP, working closely with Phil Zimmermann. When Phil decided to start PGP Corporation, I was one of the first hires. I would work on PGP until my retirement. At the same time, I got involved with the Cypherpunks. I ran the first cryptographically based anonymous remailer, among other activities.

Fast forward to late 2008 and the announcement of Bitcoin. I've noticed that cryptographic graybeards (I was in my mid 50's) tend to get cynical. I was more idealistic; I have always loved crypto, the mystery and the paradox of it.

When Satoshi announced Bitcoin on the cryptography mailing list, he got a skeptical reception at best. Cryptographers have seen too many grand schemes by clueless noobs. They tend to have a knee jerk reaction.

I was more positive. I had long been interested in cryptographic payment schemes. Plus I was lucky enough to meet and extensively correspond with both Wei Dai and Nick Szabo, generally acknowledged to have created ideas that would be realized with Bitcoin. I had made an attempt to create my own proof of work based currency, called RPOW. So I found Bitcoin facinating.

When Satoshi announced the first release of the software, I grabbed it right away. I think I was the first person besides Satoshi to run bitcoin. I mined block 70-something, and I was the recipient of the first bitcoin transaction, when Satoshi sent ten coins to me as a test. I carried on an email conversation with Satoshi over the next few days, mostly me reporting bugs and him fixing them.

Today, I am essentially paralyzed. I am fed through a tube, and my breathing is assisted through another tube. I operate the computer using a commercial eyetracker system. It also has a speech synthesizer, so this is my voice now. I spend all day in my power wheelchair. I worked up an interface using an arduino so that I can adjust my wheelchair's position using my eyes.

It has been an adjustment, but my life is not too bad. I can still read, listen to music, and watch TV and movies. I recently discovered that I can even write code. It's very slow, probably 50 times slower than I was before. But I still love programming and it gives me goals. Currently I'm working on something Mike Hearn suggested, using the security features of modern processors, designed to support "Trusted Computing", to harden Bitcoin wallets. It's almost ready to release. I just have to do the documentation.

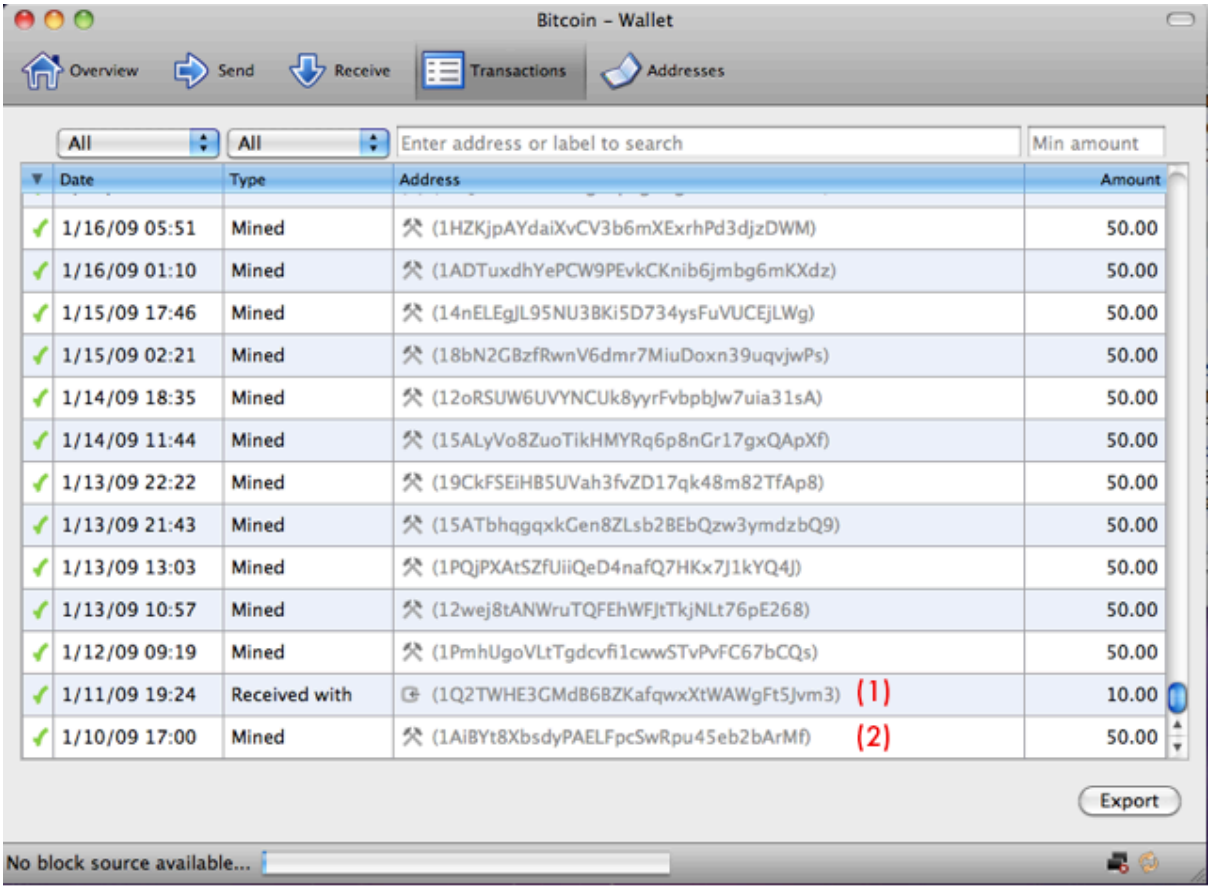
https://bitcointalk.org/index.php?topic=155054.0

24 - Hal's Bitcointalk and Me Post

- https://bitcointalk.org/index.php?topic=155054.0

1. He is the recipient of the 1st Bitcoin transaction
2. He mined block 70-something
3. He ***thinks*** he was the 1st person to join the network (besides Satoshi)

In 2014, 3 months before Hal passed away, Andy Greenberg published an article in Forbes. In this article Andy shares that he visited Hal's home, and here Jason Finney(Hal's son) shared with Andy a screenshot of his father's wallet.




https://web.archive.org/web/20140326150336im_/http://blogs-images.forbes.com/andygreenberg/files/2014/03/walletscreenshot.png

25 - Hal's Wallet Forbes

- https://web.archive.org/web/20140326104029im_/http://blogs-images.forbes.com/andygreenberg/files/2014/03/walletscreenshot.png
- https://web.archive.org/web/20140326104029/http://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/#42e4aeba4a37#:~:text=Image%3A%20walletscreenshot

In the screenshot of the wallet we see 2 things mentioned in the Bitcointalk post:

1. **The 10 Bitcoin transaction Satoshi sent to Hal, the one that is found in Block 170** *(time stamp of the transaction is off by ~6 minutes from what we see today in the blockchain, but most probably Hal's node saved the time when it saw the transaction in the mempool, and did not update it when the transaction got confirmed. This is known behaviour with the early client. It is the 2nd transaction from down to up.*

2. **The 1st Block Hal mined** with the address **1AiBYt8XbsdyPAELFpcSwRpu45eb2bArMf**. This is the coinbase of **Block 78**.
For the 1st few years Bitcoins were sent to both Bitcoin Addresses and bare Public Keys. The thing is that a Bitcoin address is a bare Public Key that's made more human readable (eliminating look-alike characters) and shorter.

*However, the Bitcoin client would convert this bare Public Key to an address when displaying it. Today we ONLY use addresses but this can be quite confusing. Even more so if we look at the same transaction on mempool.space and blockchain.info we will see 2 different*

*things. Mempool.space showing what is "correct", but blockchain.info showing consistent what the Bitcoin client showed.*
*Regardless the TX ID is:*
*7ea1d2304f1f95fae773ed8ef67b51cfd5ab33ea8b6ab0a932ee3e248b7ba74c*

So if we accept the screenshot as being real this means **Hal's node was connected to the network and mined Block 78**.

As for Hal ***thinking*** he was the 2nd person to join the network after Satoshi, seems like a reasonable assumption considering the very low interest others showed on the Cryptography Mail List.

And now let's add all the events in a table to get an easier view.
The events are listed in chronological order and all timezones converted to the UTC time zone, and PST.

| # | Description | UTC Conversion | PST Conversion |
|---|---|---|---|
| 1 | Bitcoin v0.1 announcement on Cryptography Mailing List | Thu, 8 Jan 2009 19:27:40 | Thu, 8 Jan 2009 11:27:40 PST |
| 2 | Bitcoin Block 1 gets mined | Fri, 9 Jan 2009 02:54:25 | Thu, 8 Jan 2009 18:54:25 PST |
| 3 | Private Email #1: Satoshi announces Bitcoin 0.1 launch to Hal (CoinDesk) | Fri, 9 Jan 2009 04:54:55 | Thu, 8 Jan 2009 20:54:53 PST |
| 4 | Private Email #2: Satoshi offers answers to Hal's questions (CoinDesk) | Fri, 9 Jan 2009 16:08:37 | Fri, 9 Jan 2009 08:08:37 PST |
| **5** | **Block 49(last seen in Hal's debug log)** | **Sat, 10 Jan 2009 18:56:42** | **Sat, 10 Jan 2009 10:56:42 PST** |
| **6** | **Hal reports crash in Bitcoin 0.1.0 on Sourceforge mailing list** | **Sat, 10 Jan 2009 19:13:18** | **Sat, 10 Jan 2010 11:13:18 PST** |
| 7 | Satoshi replies to Hal's 0.1 crash with debug.log (WSJ) | Sat, 10 Jan 2009 19:52:00 | Sat, 10 Jan 2009 11:52:00 PST |
| 8 | Satoshi narrows the bug, Hal leaves running 0.1 for a while(WSJ) | Sat, 10 Jan 2009 22:59:00 | Sat, 10 Jan 2009 14:59:00 PST |
| **9** | **Block 78 - Mined by Hal \| Forbes Article** | **Sun, 11 Jan 2009 01:00:54** | **Sat, 10 Jan 2009 17:00:54 PST** |
| 10 | **Hal congratulates Satoshi on Cypherpunk mailing list** | **Sun, 11 Jan 2009 02:22:01** | **Sat, 10 Jan 2009 18:22:01 PST** |
| **11** | Satoshi sends v0.1.1 to Hal (WSJ) | Sun, 11 Jan 2009 02:55:00 | Sat, 10 Jan 2009 18:55:00 PST |
| **12** | Satoshi sends bitcoin-0.1.1-exe-dbg.rar (WSJ) | Sun, 11 Jan 2009 03:11:00 | Sat, 10 Jan 2009 19:11:00 PST |
| 13 | **Hal's tweet about running Bitcoin** | **Sun, 11 Jan 2009 03:33:52** | **Sat, 10 Jan 2009 19:33:52 PST** |
| 14 | Satoshi announcement SourceForge v0.1.2 | Sun, 11 Jan 2009 22:32:00 | Sun, 11 Jan 2009 14:32:00 PST |
| 15 | Satoshi acknowledges Hal ran 0.1.2 and broke( sends msvc version) (WSJ) | Mon, 12 Jan 2009 00:36:00 | Sun, 11 Jan 2009 16:36:00 PST |
| 16 | **Block 170 gets mined** | **Mon, 12 Jan 2009 03:30:25** | **Sun, 11 Jan 2009 19:30:25 PST** |
| **17** | Satoshi sends 0.1.3 exe to Hal(WSJ) | Mon, 12 Jan 2009 05:31:00 | Sun, 11 Jan 2009 21:31:00 PST |

26 - Table Hal's Timestamps

We are working under the **assumption that all private emails are authentic**. But considering that the emails are shared by Hal, I personally can not see any reason why they would not be.
Not to mention the fact that if we compare the times of the private emails with the dates of public data, there are no contradicting discrepancies.

We can say with pretty big certainty that Hal was not the 2nd node to join the Bitcoin network after Satoshi because:

1. The 1st time he ran bitcoin, confirmed by both private emails and the Sourceforge post and debug.log file, Bitcoin had already passed Block 1, and a client Bitcoin had to have connections with other nodes in order to produce blocks.

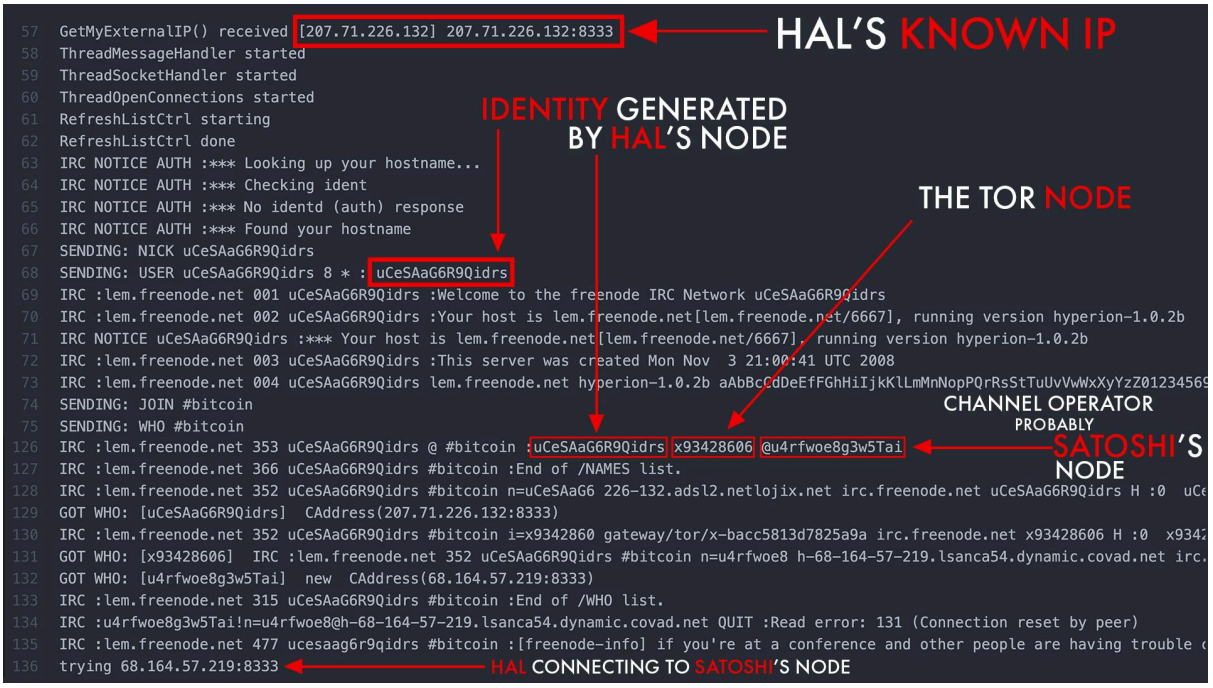
2. From the private conversations, we can see that it took Hal quite some time to get the Bitcoin client working properly, got it to work consistently around Block 170, 4 days after the launch(12 January), and for a short time just to mine Block 78(11 January)

3. Since the Bitcoin client was programmed to not start producing blocks unless at least one connection with another node, there is just no way for the debug file to have the 49 blocks inside, if Hal was the 2nd node to join.

Any of these 3 points on their own would be enough to prove our conclusion, let alone the fact that we have 3 things that point to the same thing.

But the debug file is the most solid piece of evidence, as it can be downloaded and inspected today, plus the fact that we found 49 Bitcoin Blocks hashes are present means some proof of work was done to generate them.
*(with a top end computer from 2009 could all 49 blocks could have been generated in about 6 hours and a half for reference)*

Still not convinced? Well there is more in the debug file.
We can clearly see 2 nodes already present in the #bitcoin IRC channel, when Hal's node arrived.



27 - Hal debug file - joining IRC

Here is what happens in chronological order according to the debug file.

When Hal's node connected to the IRC server it registered itself with the **uCeSAaG6R9Qidrs** username.

The Bitcoin client would construct its username by adding "u" as the 1st character + the IP address + the port, encoded in base58(same format used in Bitcoin addresses that eliminates lookalike characters).

We can see this in the irc.cpp file of the source file:

```
17  string EncodeAddress(const CAddress& addr)
18  {
19      struct ircaddr tmp;
20      tmp.ip    = addr.ip;
21      tmp.port  = addr.port;
22
23      vector<unsigned char> vch(UBEGIN(tmp), UEND(tmp));
24      return string("u") + EncodeBase58Check(vch);
25  }
26
```

https://github.com/JeremyRubin/satoshis-version/blob/master/src/irc.cpp#L19

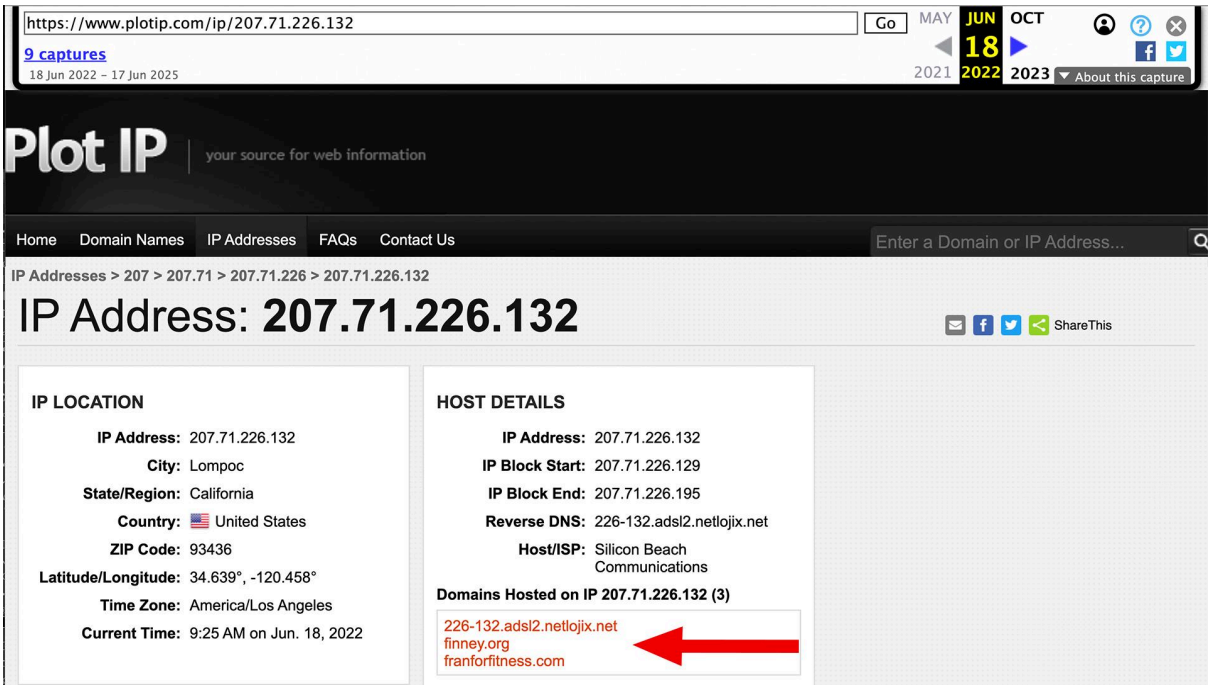
28 - IRC generate username

- https://github.com/JeremyRubin/satoshis-version/blob/master/src/irc.cpp#L19

Then the IRC server communicates who are the members present in the channel(using these generated identities/usernames by the nodes):

1. **uCeSAaG6R9Qidrs** - Hal's node
2. **x93428606** - A node behind Tor
3. **@u4rfwoe8g3w5Tai** - An operator of the chanell. We know he is the operator because of the **"@"** in front of name. Who else would be the operator at this early time, if not Satoshi?

The 1st IP we see in the picture we know for sure it is Hal since it's publicly known he hosted his stuff under **207.71.226.132**.




29 - Hal's IP hostings

- https://web.archive.org/web/20220618162516/https://www.plotip.com/ip/207.71.226.132

Also the encoding of this IP with port 8333 matches to "**uCeSAaG6R9Qidrs**"

The 2nd node "**x93428606**" is under a Tor identity, we can see this clearly mentioned in the debug file.
But also because the node was using Tor, it means that it would not be able to accept incoming connections = can not allow other nodes to connect to it = is not routable, so the username will start with an **"x"** as the 1st character, and the rest of the characters will be random. (as seen in the irc.cpp file)

```
164             string strMyName = EncodeAddress(addrLocalHost);
165
166             if (!addrLocalHost.IsRoutable())
167                 strMyName = strprintf("x%u", GetRand(1000000000));
```

https://github.com/0xMagnuz/Bitcoin-v0.1/blob/master/bitcoin0.1/src/irc.cpp#L166

30 - IRC generate TOR username

- https://github.com/JeremyRubin/satoshis-version/blob/master/src/irc.cpp#L176

The 3nd user, the operator, is connected via the clearnet IP **68.164.57.21**, which Hal's node connects to.(last line in the picture of the debug file).
This IP + port 8333 also encodes to the correct username of **u4rfwoe8g3w5Tai**

*Btw I am not the 1st person to write about the fact that this debug.log file contains Satoshi's clearnet IP:.*

- *https://whoissatoshi.wordpress.com/2016/02/20/satoshi-in-california/*
- *https://blog.lopp.net/hal-finney-was-not-satoshi-nakamoto/*

*However both of these incorrectly said the Tor user was the admin of the chanell.*

So considering the presence of these 2 other nodes + the other evidence presented in the 1st part, **we can conclude with very BIG certainty that Hal was not the 2nd node to join the Bitcoin Network**.

But this opens a new question, **who was the node running behind Tor?**

If the Tor node was also Satoshi, then Hal was the 2nd person(Satoshi being the 1st) to join the network, if it was someone else, then Hal was the 3rd person to join the network.

I want to re-iterate the very important distinction that **2 nodes does NOT mean 2 different people/persons**. **It is very easy for someone to run two nodes.**

Whatever the case may be, this does not really take anything away from Hal.
I mean it's not like this was his only achievement, in fact far from it.
He was a very accomplished cryptographer, but more importantly someone who offered suggestions on how Bitcoin should work before launch, one of the few who engaged with

Satoshi when posting about Bitcoin, and a prolific contributor even after the launch of Bitcoin.

If Hal would have not participated in these early stages(as 2nd, 3rd, or Nth participant), there is a VERY HIGH chance Bitcoin would have not took off.

And cmon, being moved from the 2nd node to join the Bitcoin Network to the 3rd is not a tragedy. :)

**So who ran Bitcoin before Hal?**

The presence of the Tor node before Hal, does not necessarily mean the Tor node started the network with Satoshi, just meanest it was present when Hal's node joined.

So do I have another contender for the 2nd participant to join the Bitcoin Network?

# Enter Dustin Tramell

https://x.com/druidian

Dustin is very well known in the Bitcoin community and still active today but even more importantly he was very transparent about his early involvement in Bitcoin.
And because of his early involvement this led a lot of people to speculate he was Satoshi.

As a response to these lazy speculations, Dustin shared the private conversations he had with Satoshi, so considering these conversations took place very close to the events we analysed, it is of interest to us to check them out.

We will again presume these emails are real and not modified.
*FWIW even though I do not know Dustin personally, but from the way he participated in the community I have 0 reasons to suspect these emails have been tampered with.*

The emails can be found on his personal blog:
https://blog.dustintrammell.com/i-am-not-satoshi/

And here is the direct download link:
https://koi-reindeer-77pb.squarespace.com/s/Satoshi_Nakamoto.zip
*You can open them with a text editor and they will show full body.*

The 1st email is Dustin's response to the announcement of Bitcoin v0.1 Satoshis made.

Dustin's email server logged Satoshi's Announcement at Fri, 2009-01-09 at 03:27 +0800 = 2009-01-08 19:27 UTC
Which is 40 seconds off compared to the time we see on Cryptography Maillist, but this is pretty normal as emails propagate with small lag over the internet.

Below we can see Dustin's response to Satoshi Announcement at Sun, 11 Jan 2009 23:14:04 -0600 = 12 January 2009 05:14:04 UTC which is **~2 hours after Block 170 was mined**(the one where Satoshi sent Hal 10 Bitcoins).

```
From dtrammell@dustintrammell.com Sun Jan 11 23:14:04 2009
Subject: Re: Bitcoin v0.1 released
From: "Dustin D. Trammell" <dtrammell@dustintrammell.com>
To: satoshi@vistomail.com
In-Reply-To: <CHILKAT-MID-3d087dc8-b531-1fd3-bebb-15dcffb225ce@server123>
References: <CHILKAT-MID-3d087dc8-b531-1fd3-bebb-15dcffb225ce@server123>
Content-Type: multipart/signed; micalg=pgp-sha1; protocol="application/pgp-signature"; boundary="=-5xGWqC9OFcGt3lgdaUyl"
Message-Id: <1231737244.9962.52.camel@localhost>
Mime-Version: 1.0
X-Mailer: Evolution 2.10.3 Dropline GNOME
Date: Sun, 11 Jan 2009 23:14:04 -0600
X-Evolution-Format: text/plain
X-Evolution-Account: 1169982963.29994.8@slimer
X-Evolution-Transport:
 smtp://dustintrammell-dtrammell;auth=CRAM-MD5@mail.oaklabs.net/;use_ssl=always
X-Evolution-Fcc: mbox:/home/druid/.evolution/mail/local#Sent


--=-5xGWqC9OFcGt3lgdaUyl
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable

On Fri, 2009-01-09 at 03:27 +0800, Satoshi Nakamoto wrote:
> Announcing the first release of Bitcoin, a new electronic cash
> system that uses a peer-to-peer network to prevent double-spending.
> It's completely decentralized with no server or central authority.

I'm currently reading through your paper.  At the timestamp server
section you mention newspapers and usenet, so I thought you might be
interested in this if you have not seen it already:

http://www.publictimestamp.org/

By the way, I'm also currently running the alpha code on one of my
workstations.  So far it has two "Generated" messages, however the
"Credit" field for those is 0.00 and the balance hasn't changed.  Is
this due to the age/maturity requirement for a coin to be valid?

Cheers,

--=20
Dustin D. Trammell
dtrammell@dustintrammell.com
http://www.dustintrammell.com
```

https://blog.dustintrammell.com/i-am-not-satoshi

https://koi-reindeer-77pb.squarespace.com/s/Satoshi_Nakamoto.zip

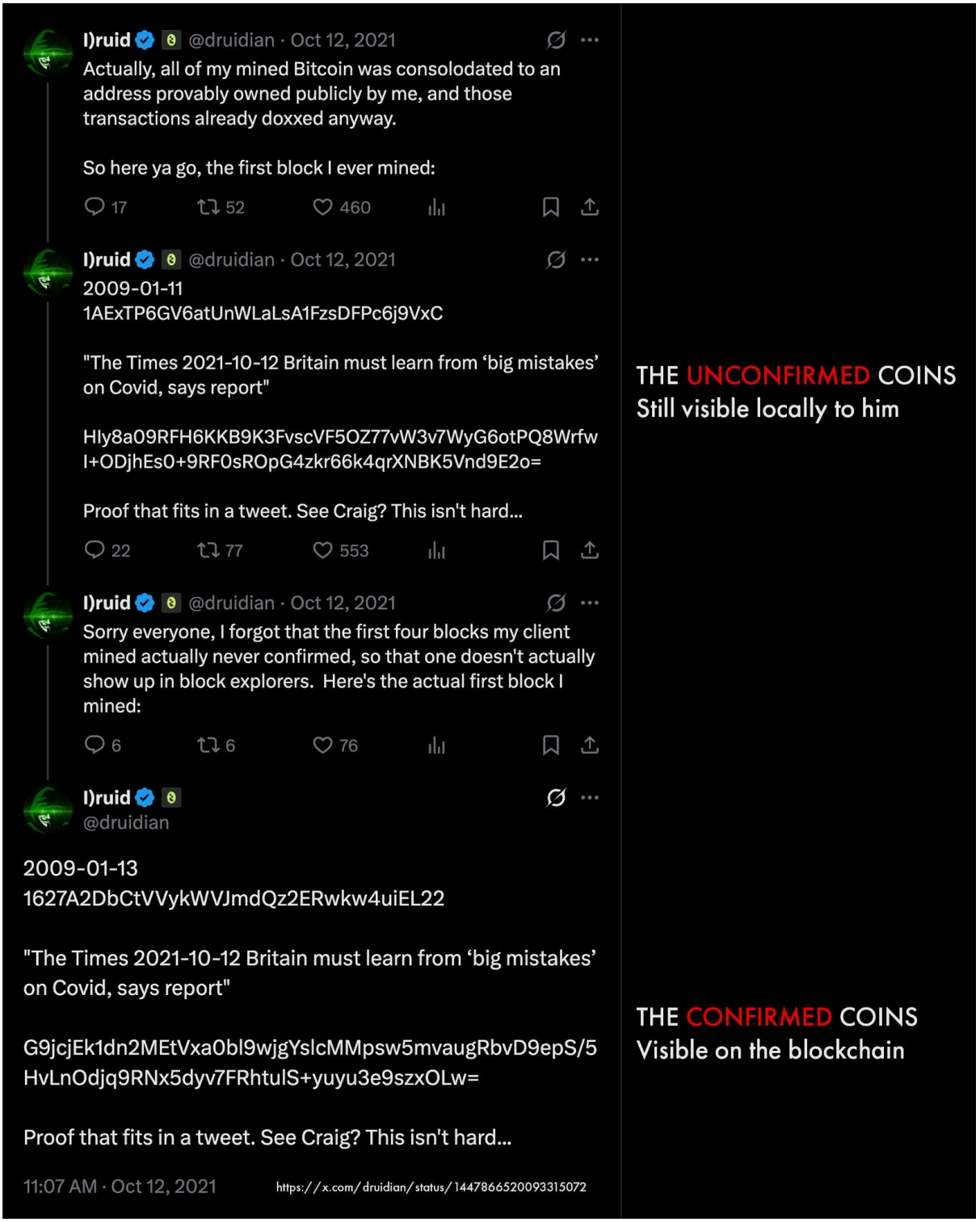
31 - Dusin 1st email
(downloaded from Dustin's website link above)

In the email Dustin mentions that he was running the Bitcoin client, and got 2 Generated messages (as in he mined 2 blocks) but the balance is still zero (as in not confirmed).

As mentioned above Dustin was very transparent about his early involvement, and always shared information with the community and in 2021 he shared two separate proofs both containing:

- Bitcoin address
- Generated message
- A signature of this message

This uses the same type of cryptography we use on the blockchain to prove ownership of a private key, just that here Dustin signed a message instead of a Bitcoin Transaction, to prove control over a certain Bitcoin address.



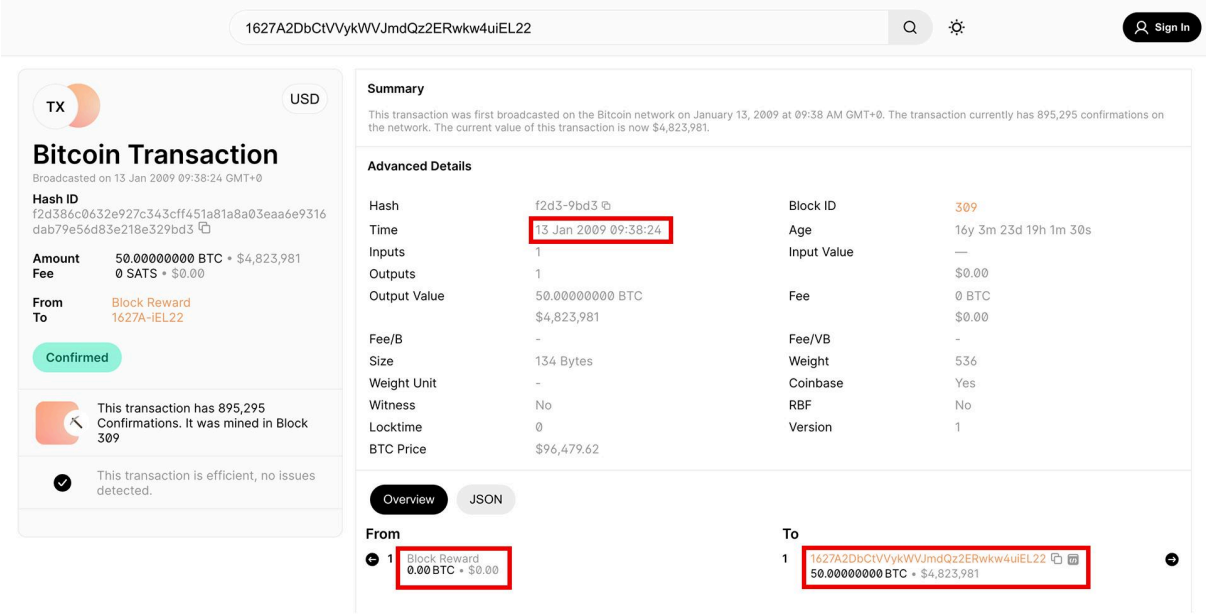

32 - Dustin shows addresses

- https://x.com/druidian/status/1447866520093315072

Again we see Dustin mentioning the same unconfirmed transactions(which obviously do not show up on the blockchain) together with another address from the 13th January(for reference Block #1 was mined on the 9th January) which did mine bitcoins and the signature matches.

This is indeed consistent with what was said in the email. Regarding the non-confirmed coins, we will see later what happened.

One thing that we can be 100% sure about is that Dustin has the private key to the address that mined the 50 Bitcoin coinbase on the 13th of January 2009, since he provided the cryptographic proof for it.
Let's check his proof.




https://www.blockchain.com/explorer/addresses/btc/1627A2DbCtVVykWVJmdQz2ERwkw4uiEL22

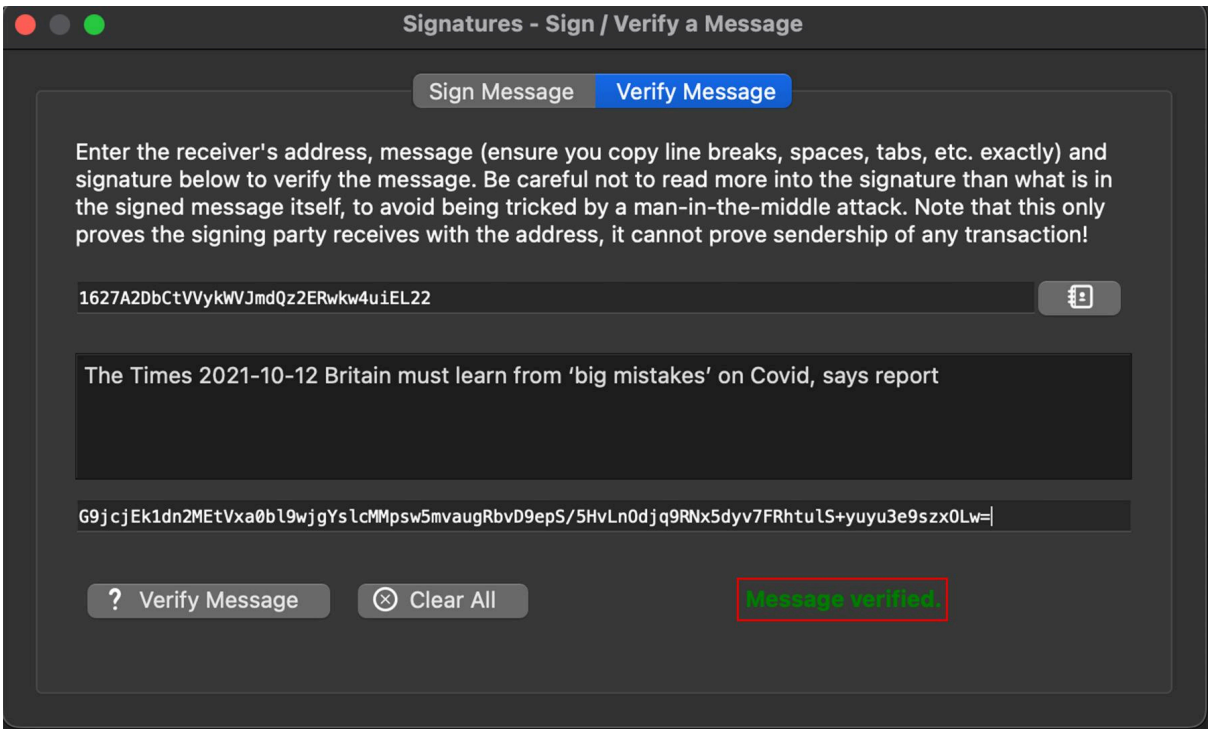
33 - Dustin's address Blockchain

- https://www.blockchain.com/explorer/transactions/btc/f2d386c0632e927c343cff451a81a8a03eaa6e9316dab79e56d83e218e329bd3

We can see the address 1627A2DbCtVVykWVJmdQz2ERwkw4uiEL22(the 2nd example in the tweets) did indeed mine 50 Bitcoins on the 13th of January 2009, as indicated by the fact that that is a block reward.

This transaction was made to a bare Public Key, so if you look at it on mempool.space it will look different, however in order to verify it in Bitcoin Core, we need to convert it to an address, which is what blockchain.com displays.

And if we paste the signature he shared in the 2021 tweet + the message + the address in Bitcoin Core we can see Dustin told the truth.



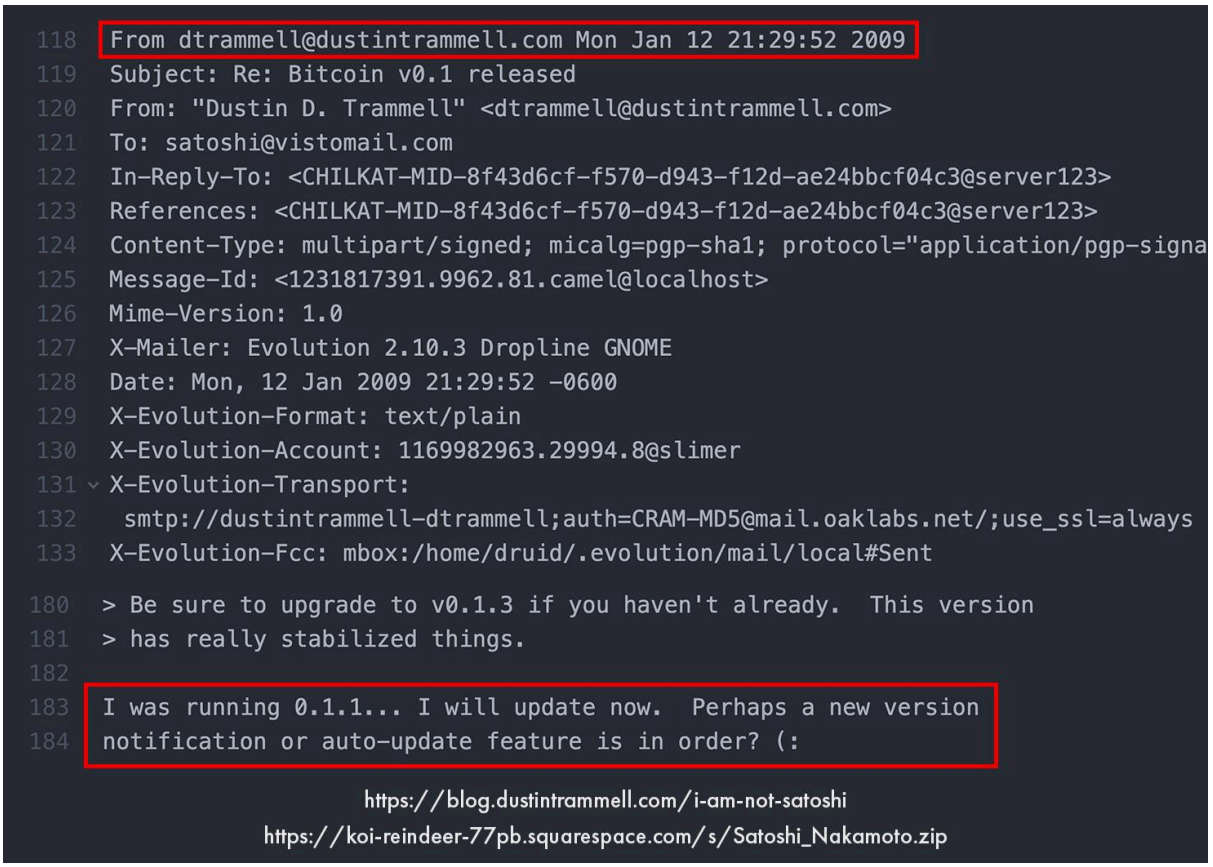

34 - Distin Bitcoin Core Verification

This is great to see, and the block in question is 309, which is very early indeed, but still not earlier than Hal's Block 49 from the log file, or even Block 78(mined by Hal) or even Block 170 when Satoshi sent him the 10 Bitcoins.

Let's dig further in the Dustin - Satoshi emails.

On the 12 Jan 2009 21:29:52 -0600 = January 13, 2009 at 03:29:52 UTC, Dusting confirms he was running Bitcoin v0.1.1, when Satoshi advised him to update to v0.1.3(the version that

finally worked for Hal)

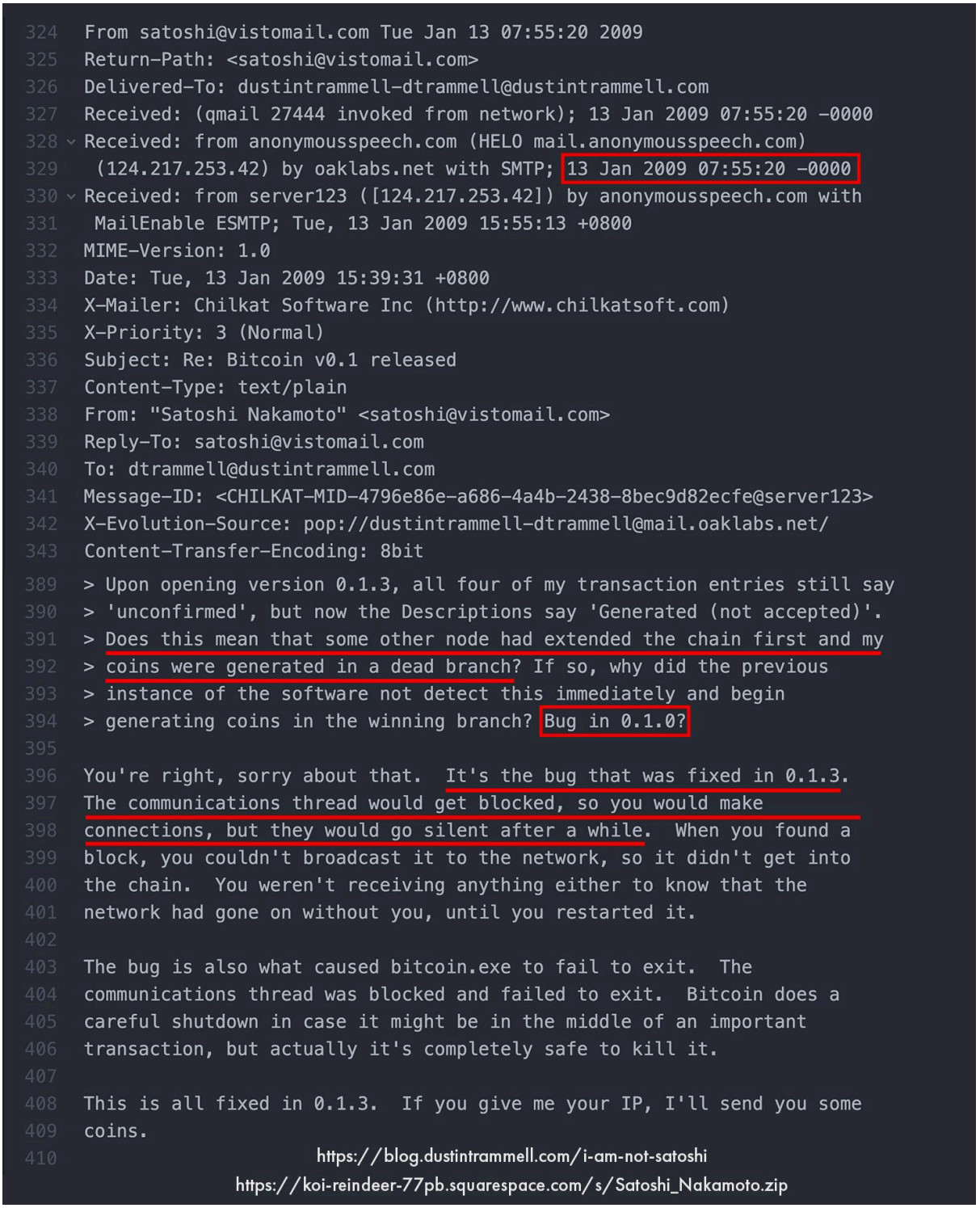


```
From dtrammell@dustintrammell.com Mon Jan 12 21:29:52 2009
Subject: Re: Bitcoin v0.1 released
From: "Dustin D. Trammell" <dtrammell@dustintrammell.com>
To: satoshi@vistomail.com
In-Reply-To: <CHILKAT-MID-8f43d6cf-f570-d943-f12d-ae24bbcf04c3@server123>
References: <CHILKAT-MID-8f43d6cf-f570-d943-f12d-ae24bbcf04c3@server123>
Content-Type: multipart/signed; micalg=pgp-sha1; protocol="application/pgp-signa
Message-Id: <1231817391.9962.81.camel@localhost>
Mime-Version: 1.0
X-Mailer: Evolution 2.10.3 Dropline GNOME
Date: Mon, 12 Jan 2009 21:29:52 -0600
X-Evolution-Format: text/plain
X-Evolution-Account: 1169982963.29994.8@slimer
X-Evolution-Transport:
 smtp://dustintrammell-dtrammell;auth=CRAM-MD5@mail.oaklabs.net/;use_ssl=always
X-Evolution-Fcc: mbox:/home/druid/.evolution/mail/local#Sent

> Be sure to upgrade to v0.1.3 if you haven't already.  This version
> has really stabilized things.

I was running 0.1.1... I will update now.  Perhaps a new version
notification or auto-update feature is in order? (:
```



35 - Dustin Jan 12

On the 13 Jan 2009 07:55:20 -0000 UTC Satoshi addresses Dustin's non-confirmed coins problem.
Satoshi confirms it was a bug with pre v0.1.3 versions where the client would get blocked after some time, and even if it would still be connected to the nodes, it could not communicate with them.
So if he did mine 2 blocks, but was unable to comunicate the mined blocks to the network.



```
From satoshi@vistomail.com Tue Jan 13 07:55:20 2009
Return-Path: <satoshi@vistomail.com>
Delivered-To: dustintrammell-dtrammell@dustintrammell.com
Received: (qmail 27444 invoked from network); 13 Jan 2009 07:55:20 -0000
Received: from anonymousspeech.com (HELO mail.anonymousspeech.com)
 (124.217.253.42) by oaklabs.net with SMTP; 13 Jan 2009 07:55:20 -0000
Received: from server123 ([124.217.253.42]) by anonymousspeech.com with
 MailEnable ESMTP; Tue, 13 Jan 2009 15:55:13 +0800
MIME-Version: 1.0
Date: Tue, 13 Jan 2009 15:39:31 +0800
X-Mailer: Chilkat Software Inc (http://www.chilkatsoft.com)
X-Priority: 3 (Normal)
Subject: Re: Bitcoin v0.1 released
Content-Type: text/plain
From: "Satoshi Nakamoto" <satoshi@vistomail.com>
Reply-To: satoshi@vistomail.com
To: dtrammell@dustintrammell.com
Message-ID: <CHILKAT-MID-4796e86e-a686-4a4b-2438-8bec9d82ecfe@server123>
X-Evolution-Source: pop://dustintrammell-dtrammell@mail.oaklabs.net/
Content-Transfer-Encoding: 8bit

> Upon opening version 0.1.3, all four of my transaction entries still say
> 'unconfirmed', but now the Descriptions say 'Generated (not accepted)'.
> Does this mean that some other node had extended the chain first and my
> coins were generated in a dead branch? If so, why did the previous
> instance of the software not detect this immediately and begin
> generating coins in the winning branch? Bug in 0.1.0?

You're right, sorry about that.  It's the bug that was fixed in 0.1.3.
The communications thread would get blocked, so you would make
connections, but they would go silent after a while.  When you found a
block, you couldn't broadcast it to the network, so it didn't get into
the chain.  You weren't receiving anything either to know that the
network had gone on without you, until you restarted it.

The bug is also what caused bitcoin.exe to fail to exit.  The
communications thread was blocked and failed to exit.  Bitcoin does a
careful shutdown in case it might be in the middle of an important
transaction, but actually it's completely safe to kill it.

This is all fixed in 0.1.3.  If you give me your IP, I'll send you some
coins.
```

https://blog.dustintrammell.com/i-am-not-satoshi

https://koi-reindeer-77pb.squarespace.com/s/Satoshi_Nakamoto.zip

36 - Dustin Jan 13

This is actually very interesting, because this is not only consistent with what we saw in Hal's debug file but also Satoshi mentioning the same problem he solved with Hal.

This email suggests that Dusting was indeed running Bitcoin v0.1.0, but at the same time this means that if other people would have tried running the client, they would have encountered the same problem.

This makes me think that the **node behind Tor may have been Satoshi**, since other people who would have tried to run Bitcoin would have run into the same problem as Hal and Dustin, and they would have not been able to communicate the blocks to the network.

**Maybe** Satoshi realised this, and he said, hey let me spin off another node, so the network does not look stale as others join.

If we look at the Bitcoin blocks times before Block 49, we can see on 2 different occasions the time between blocks was UNREASONABLY big and one 30 minutes which does happen from time to time.

| Block Hash | Block Number | Diff betwen blocks | Block Time |
|---|---|---|---|
| 000000000019d6 | 0 | | 2009-01-03 18:15:05 |
| 00000000839a8e | 1 | 5 days, 8 hours, 39 minutes | 2009-01-09 02:54:25 |
| 000000006a625f | 2 | 00:01:19 | 2009-01-09 02:55:44 |
| 0000000082b501 | 3 | 00:07:09 | 2009-01-09 03:02:53 |
| 000000004ebadb | 4 | 00:13:35 | 2009-01-09 03:16:28 |
| 000000009b7262 | 5 | 00:07:20 | 2009-01-09 03:23:48 |
| 000000003031a0 | 6 | 00:06:01 | 2009-01-09 03:29:49 |
| 0000000071966c | 7 | 00:09:40 | 2009-01-09 03:39:29 |
| 00000000408c48 | 8 | 00:06:14 | 2009-01-09 03:45:43 |
| 000000008d9dc5 | 9 | 00:08:56 | 2009-01-09 03:54:39 |
| 000000002c05cc | 10 | 00:11:13 | 2009-01-09 04:05:52 |
| 0000000097be56 | 11 | 00:06:48 | 2009-01-09 04:12:40 |
| 0000000027c248 | 12 | 00:08:48 | 2009-01-09 04:21:28 |
| 000000005c51de | 13 | 00:02:12 | 2009-01-09 04:23:40 |
| 0000000080f17a | 14 | 00:09:29 | 2009-01-09 04:33:09 |
| 00000000b3322c | 15 | 24 hours, 12 minutes, 37 seconds | 2009-01-10 04:45:46 |
| 00000000174a25 | 16 | 00:00:12 | 2009-01-10 04:45:58 |
| 000000003ff1d0d | 17 | 00:17:13 | 2009-01-10 05:03:11 |
| 000000008693e9 | 18 | 00:09:03 | 2009-01-10 05:12:14 |
| 00000000841cb8 | 19 | 00:10:40 | 2009-01-10 05:22:54 |
| 0000000067a97a | 20 | 00:17:01 | 2009-01-10 05:39:55 |
| 000000006f0163 | 21 | 00:09:18 | 2009-01-10 05:49:13 |
| 0000000098b58d | 22 | 00:15:14 | 2009-01-10 06:04:27 |
| 000000000cd339 | 23 | 00:02:24 | 2009-01-10 06:06:51 |
| 00000000fc051fb | 24 | 00:11:06 | 2009-01-10 06:17:57 |
| 000000008e35a1 | 25 | 00:06:09 | 2009-01-10 06:24:06 |
| 0000000041438e | 26 | 30 minutes, 4 seconds | 2009-01-10 06:54:10 |
| 00000000713507 | 27 | 00:02:03 | 2009-01-10 06:56:13 |
| 00000000bb0d94 | 28 | 8 hours ,34 minutes, 44 seconds | 2009-01-10 15:30:57 |
| 00000000c57a1b | 29 | 00:00:46 | 2009-01-10 15:31:43 |
| 00000000bc919c | 30 | 00:10:19 | 2009-01-10 15:42:02 |
| 000000009700ff3 | 31 | 00:10:14 | 2009-01-10 15:52:16 |
| 00000000e5cb7c | 32 | 00:07:15 | 2009-01-10 15:59:31 |
| 00000000a87073 | 33 | 00:12:48 | 2009-01-10 16:12:19 |
| 00000000a73fb2 | 34 | 00:06:39 | 2009-01-10 16:18:58 |
| 00000000b572a4 | 35 | 00:13:35 | 2009-01-10 16:32:33 |
| 00000000f824d6 | 36 | 00:10:36 | 2009-01-10 16:43:09 |
| 00000000ddd96d | 37 | 00:16:13 | 2009-01-10 16:59:22 |
| 000000007c19ee | 38 | 00:12:06 | 2009-01-10 17:11:28 |
| 000000005665d5 | 39 | 00:00:23 | 2009-01-10 17:11:51 |
| 00000000b2f01f3 | 40 | 00:11:37 | 2009-01-10 17:23:28 |
| 00000000ad2b48 | 41 | 00:11:35 | 2009-01-10 17:35:03 |
| 00000000314e90 | 42 | 00:04:10 | 2009-01-10 17:39:13 |
| 00000000ac21f28 | 43 | 00:05:24 | 2009-01-10 17:44:37 |

37 - Big block times up to 49

1. From Block **14 to 15 ~ 24 hours**
2. From Block 25 to 26 ~ 30 minutes
3. From Block **27 to 28 ~ 8 hours 34 minutes**

Since the starting difficulty was very low during this time there is no way these 2 instances of 8 hours and 24 hours were statistically probable.
Even a low - end computer from 2009 would be able to mine a Bitcoin block at the starting difficulty of 1 in less than 8 hours.

This means that the **network halted** pretty much between the blocks and for that amount of time.

If we look at the code we can see that the starting difficulty of 1 required 2^32 operations(on average) to find a valid hash, and a decent computer from 2009 could have handled this with no issue.
So we can rule out the possibility that there were a lot of people mining but their hardware was not powerful enough to find a block for 8 hours.

I can only imagine the reason for this big time difference is because Satoshi's node was alone on the network, and it would not produce blocks, because of the constraint he added in the code, that it needs other connections. Or there was literally no one running a Bitcoin node.

So I would lean towards the **Tor node being also Satoshi**.

It would sure be nice to find another source of information, to contrast our findings, but there is no one else that participated so early in Bitcoin and shared any public information, the only thing we have from back then is The Blockchain.

# Enter **ExtraNonce**

I am sure most readers are somewhat familiar with how Bitcoin mining works, but let me give you a quick refresh.

A miner takes a bunch of transactions and puts them in a block, hashes all the data and then sends the block with the hash to other nodes.
If the hash of the block is below a **certain value**(set by the network), the miner gets the block reward + the transaction fees.
This value is proportional with the difficulty, and as the difficulty rises this value gets smaller.
Since when you lower this value, there are less possible valid options = you have a smaller search space, so it's hard to find valid block hashes.

SHA256 outputs are evenly distributed, meaning that **each hash you calculate has the EXACT same probability of being below that certain value**.

But this probability is quite small, so you have to calculate a lot of hashes, and I know everyone knows at least intuitively that **Bitcoin mining is just trying a lot of hashes until you get lucky.**

Another important property of SHA256 is that if you change even a single bit of the thing you are hashing, the **output changes drastically,** and Satoshi obviously knew this also.
Since you can't change the transactions data, Satoshi created a special field in the block called **Nonce** = **N**umber used **ONCE**.

So mining is just iterating the values of this Nonce field from 1 to the maximum its value of 2^32 = 4,294,967,296.
Quite often miners go through all that range and still did not find a block, even more so as the difficulty increases.

So what does it do then?
It uses an **ExtraNonce**. The miner can increment this extraNonce and with each increment it gets a new set of 2^32 values.

While the Nonce field is specified in the protocol and has to exist in the block header, the extraNonce field is kinda a hack, and you just change something in the coinbase TX and call it **ExtraNonce**.

Now here is where things get really interesting.
You see when Satoshi implemented Bitcoin mining he made a small mistake when handling the ExtraNonce.

You would think that a miner goes a few times through the Nonce range, iterating the extraNonce everytime, and once he finds a block, he **would** reset the ExtraNonce and start

working on a new block, but that's not how it worked in the first versions of Bitcoin.

```
2183  bool BitcoinMiner()
2184  {
2185      printf("BitcoinMiner started\n");
2186      SetThreadPriority(GetCurrentThread(), THREAD_PRIORITY_LOWEST);
2187
2188      CKey key;
2189      key.MakeNewKey();
2190      CBigNum bnExtraNonce = 0;
2191      while (fGenerateBitcoins)
2192      {
2193          Sleep(50);
2194          CheckForShutdown(3);
2195          while (vNodes.empty())
2196          {
2197              Sleep(1000);
2198              CheckForShutdown(3);
2199          }
2200
2201          unsigned int nTransactionsUpdatedLast = nTransactionsUpdated;
2202          CBlockIndex* pindexPrev = pindexBest;
2203          unsigned int nBits = GetNextWorkRequired(pindexPrev);
2204
2205
2206          //
2207          // Create coinbase tx
2208          //
2209          CTransaction txNew;
2210          txNew.vin.resize(1);
2211          txNew.vin[0].prevout.SetNull();
2212          txNew.vin[0].scriptSig << nBits << ++bnExtraNonce;
2213          txNew.vout.resize(1);
2214          txNew.vout[0].scriptPubKey << key.GetPubKey() << OP_CHECKSIG;
2215
```

https://github.com/JeremyRubin/satoshis-version/blob/master/src/main.cpp#L2248

38 - extraNonce

- https://github.com/JeremyRubin/satoshis-version/blob/master/src/main.cpp#L2248

Because of the way Satoshi implemented the usage of the ExtraNonce it ended up having 3 unintended consequences:
1) the ExtraNonce ONLY resets if you restart/shutdown the Bitcoin Client and not after a block is found
2) the ExtraNonce also increments, when you try to construct a possible block, not only when the Nonce overflows
3) the ExtraNonce also increments when it gets valid block from another node, not only when the Nonce overflows

1) *because bnExtraNonce only gets initialised to 0 before the while(fGenerateBitcoins)*
2) *because of the position of ++bnExtraNonce, in regards to coinbase creation.*

3) *because of how the fGenerateBitcoins loop is positioned.*

So in normal operation a Bitcoin node(only in this very early client, things changed later) would increase the ExtraNonce not just when the Nonce range would have to be repeated, but every time one of the above mentioned operations would get triggered.

And since the extraNonce gets **published in the coinbase transaction of each block**, the miner **leaves a trace on the blockchain of how many times the extraNonce was incremented**.

This is great for our investigation, because:

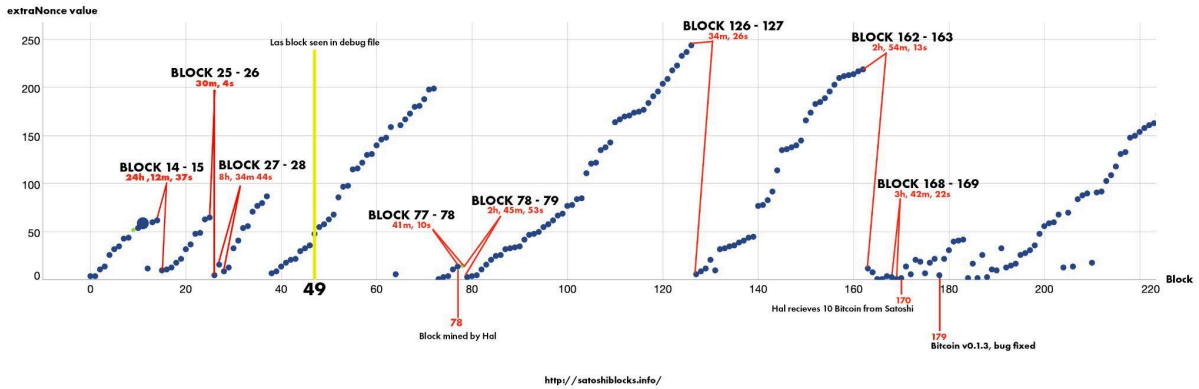
1) The ExtraNonce field acts like a counter giving us an idea for how long a bitcoin client was running for
2) If we see consecutive extraNonce values, or if we see a series of blocks that their nonces increment by small amounts we can be **fairly** certain this is a single miner.
3) And if we see a block with ExtraNonce 0, we can conclude this is a miner that just started his client.

Btw this was discovered by Sergio Demian Lerner, which led him to develop the Patoshi Pattern, which led him to assess this Patoshi miner(who probably was Satoshi) has between 700k-1 MIL Bitcoins.
Regardless if you agree with his conclusion or not, **2 things are undeniable**:

1) What is written in the code(how the extraNonce was incremented)
2) What is written on the blockchain(the extraNonce published in the coinbase transactions)

The good news is that even if you disagree with Sergio conclusions because maybe the data is too noisy, for our investigation this is not a problem because:

1) we are dealing with the very first days of Bitcoins existence and VERY low interest was shown on the Cryptography Mail List, so we are dealing with a few participants
2) We have additional information from Hal's debug file that around block 49 there were ONLY 2 other nodes preset, hard to imagine all of a sudden hundreds rushed in




39 - Patoshi + block s+ times

- http://satoshiblocks.info/

In the chart above we have Blocks on the OX axis and extraNonce values on the OY.

We can see some blue dots forming a pattern, as the ExtraNonce of consecutive blocks increases.

We can assume with a great degree of certainty that each one of those groupings of blue points is one individual miner. The higher the value the more certain we can be.

Even though the ExtraNonce incrementation is not random, it is pretty chaotic, and unpredictable, so when we get consecutive values we can assess a fairly high probability to our assumption that one grouping of blue dots represents one entity.

The goes chart is up until around Block 170 because around this time:

1) Satoshi sent Hal the 10 Bitcoins
2) Hal made the Running Bitcoin tweet
3) Satoshi released Bitcoin v0.1.3, the 1st one that ran without problems.

It seems that everytime the **ExtraNonce resets, we get a big time between blocks**, the only exception being from Block 72 to Block 73, which is the segment during which Hal connected briefly to the network and we got the debug file with the last block in the file being 49.
At the moment we know there were only 2 other nodes present. The clearnet-most-probably-Satoshi node, and the Tor node.

This leads me to believe that not only each grouping was done by the same miner, all of the groupings were done by the same entity, which the most reasonable assumption is Satoshi, since the only other person that was interested in bitcoin, Hal, had problems running the node.

So that's why I think the Tor node was also Satoshi.

And again, the fact that we have big time gaps between blocks, when the ExtraNonce resets, which we know happens when the node is turned off, makes a good case that there was no one else mining this early, otherwise they would have found a block.

To be extra clear all of what I am saying is **educated speculation** and reasoning with the evidence but this is **not 100% proof**.
When I say some of these events have a high chance that does not mean it's a guarantee. Freak events happen from time to time, they just happen statistically less likely.

**What if Dustin was the Tor node?**
This speculation can be eliminated very easily.

On Jan 13 18:40:28 2009, Dustin shared his IP address with Satoshi, so Satoshi could send him some coins to 24.28.79.95.
So I doubt Dustin would have been using Tor, and then switch to a clear net IP.

```
From dtrammell@dustintrammell.com Tue Jan 13 18:40:28 2009
Subject: Re: Bitcoin v0.1 released
From: "Dustin D. Trammell" <dtrammell@dustintrammell.com>
To: satoshi@vistomail.com
In-Reply-To: <CHILKAT-MID-4796e86e-a686-4a4b-2438-8bec9d82ecfe@server123>
References: <CHILKAT-MID-4796e86e-a686-4a4b-2438-8bec9d82ecfe@server123>
Content-Type: multipart/signed; micalg=pgp-sha1; protocol="application/pgp-signat
Message-Id: <1231893628.9962.116.camel@localhost>
Mime-Version: 1.0
X-Mailer: Evolution 2.10.3 Dropline GNOME
Date: Tue, 13 Jan 2009 18:40:28 -0600
X-Evolution-Format: text/plain
X-Evolution-Account: 1169982963.29994.8@slimer
X-Evolution-Transport:
 smtp://dustintrammell-dtrammell;auth=CRAM-MD5@mail.oaklabs.net/;use_ssl=always
X-Evolution-Fcc: mbox:/home/druid/.evolution/mail/local#Sent

> This is all fixed in 0.1.3.  If you give me your IP, I'll send you some
> coins.

I'm currently at 24.28.79.95, but that's dynamic so it may change.  I've
had that address for a while though so hopefully my dhcp client is being
successful at renewing and not losing my address.  It does change from
time to time, but that address should be good for a while.
```

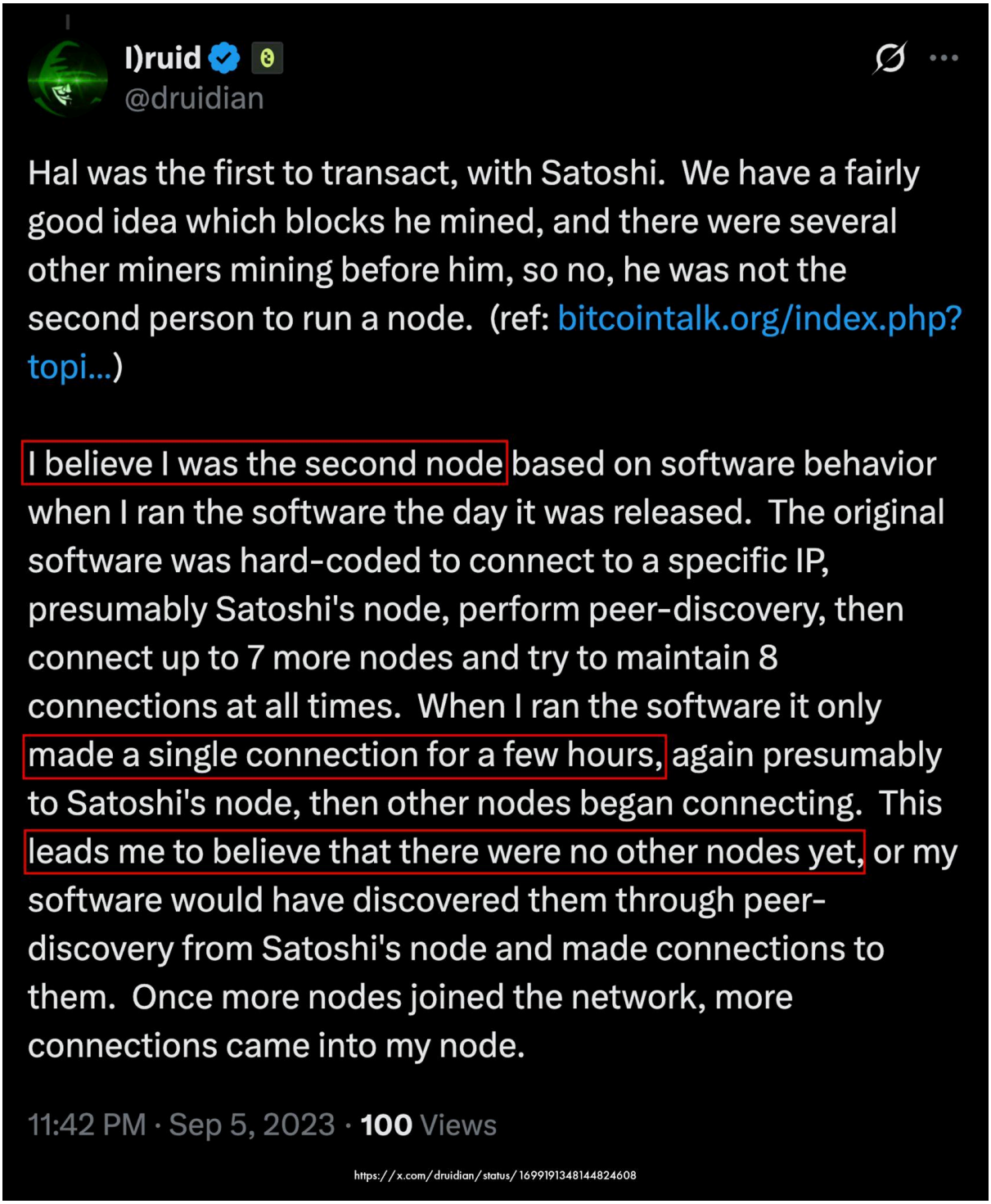
https://blog.dustintrammell.com/i-am-not-satoshi
https://koi-reindeer-77pb.squarespace.com/s/Satoshi_Nakamoto.zip

40 - Dustin Jan 13 shares IP.psd

*As mentioned earlier, the early versions of Bitcoin would allow you to send Bitcoins to a node's IP address. Someone would give you their IP, your node would connect to their node using the provided IP address, and then, ask the node for a Public Key, and then send Bitcoins to that Public Key.*

*Even though addresses were supported, a lot of early transactions used bare Public Keys, and that's why Dustin shared his IP address with Satoshi in this email.*

So at this point we can move on to the last pieces of evidence, two tweets made by Dustin: 1)2023




41 - Dustin tweet 1st 2023

- https://x.com/druidian/status/1699191348144824608
- https://archive.fo/Bjw7I

2) 2021


42 - Dusting tweet 1st 2021

- https://x.com/druidian/status/1447607399720890370

It is interesting to see that **Dustin reached the same conclusion as us**, that Hal was NOT the second node to join the network(Satoshi being the first), and that indeed there were other miners before Hal, which is consistent with our findings.

Dustin suspects he was the 2nd node to join the Bitcoin network, before Hal.
He is clearly saying his node only made 1 connection. But was this because there were no other nodes to connect to, or some connection problems?

What Dustin describes in the tweet makes a lot of sense, since even though Hal tried Bitcoin at Block 49, he only managed to get it working way later, when Dustin would have ran his client, only Satoshi would be present.

But what about the Tor node?
Well the **Tor node would have not allowed incoming connections**, so the only node Dustin could have connected to, would have been Satoshi.

However this still leaves an open question, why did the Tor node and Satoshi's node both not connect to Dustin's node?

With the evidence we have so far, we can only assert with 100% certainty that Dustin has access to the private key of the address that mined Block 309, but can we find other evidence that places him before this block?

We can never know with 100% certainty if he did indeed mined the two unconfirmed blocks, but considering that everything else he says fits very well with our own independent analysis, let's give Dustin the benefit of the doubt.

Dustin does not mention a timestamp of the two unconfirmed blocks, only the date of 11th of January, so lets add in our table the first and last blocks of that day, Block 76, and Block 168.

| # | Description | UTC Conversion | PST Conversion |
|---|---|---|---|
| 1 | Bitcoin v0.1 announcement on Cryptography Mailing List | Thu, 8 Jan 2009 19:27:40 | Thu, 8 Jan 2009 11:27:40 PST |
| 2 | Bitcoin Block 1 gets mined | Fri, 9 Jan 2009 02:54:25 | Thu, 8 Jan 2009 18:54:25 PST |
| 3 | Private Email #1: Satoshi announces Bitcoin 0.1 launch to Hal (CoinDesk) | Fri, 9 Jan 2009 04:54:55 | Thu, 8 Jan 2009 20:54:53 PST |
| 4 | Private Email #2: Satoshi offers answers to Hal's questions (CoinDesk) | Fri, 9 Jan 2009 16:08:37 | Fri, 9 Jan 2009 08:08:37 PST |
| **5** | **Block 49(last seen in Hal's debug log)** | **Sat, 10 Jan 2009 18:56:42** | **Sat, 10 Jan 2009 10:56:42 PST** |
| **6** | **Hal reports crash in Bitcoin 0.1.0 on Sourceforge mailing list** | **Sat, 10 Jan 2009 19:13:18** | **Sat, 10 Jan 2010 11:13:18 PST** |
| 7 | Satoshi replies to Hal's 0.1 crash with debug.log (WSJ) | Sat, 10 Jan 2009 19:52:00 | Sat, 10 Jan 2009 11:52:00 PST |
| 8 | Satoshi narrows the bug, Hal leaves running 0.1 for a while(WSJ) | Sat, 10 Jan 2009 22:59:00 | Sat, 10 Jan 2009 14:59:00 PST |
| | Block 76 | Sun, 11 Jan 2009 00:09:14 | Sat, 10 Jan 2009 16:09:14 PST |
| **9** | **Block 78 - Mined by Hal \| Forbes Article** | **Sun, 11 Jan 2009 01:00:54** | **Sat, 10 Jan 2009 17:00:54 PST** |
| 10 | **Hal congratulates Satoshi on Cypherpunk mailing list** | **Sun, 11 Jan 2009 02:22:01** | **Sat, 10 Jan 2009 18:22:01 PST** |
| **11** | Satoshi sends v0.1.1 to Hal (WSJ) | Sun, 11 Jan 2009 02:55:00 | Sat, 10 Jan 2009 18:55:00 PST |
| **12** | Satoshi sends bitcoin-0.1.1-exe-dbg.rar (WSJ) | Sun, 11 Jan 2009 03:11:00 | Sat, 10 Jan 2009 19:11:00 PST |
| 13 | **Hal's tweet about running Bitcoin** | **Sun, 11 Jan 2009 03:33:52** | **Sat, 10 Jan 2009 19:33:52 PST** |
| | Block 168 | Sun, 11 Jan 2009 23:39:41 | Sun, 11 Jan 2009 at 15:39:41 PST |
| 14 | Satoshi announcement SourceForge v0.1.2 | Sun, 11 Jan 2009 22:32:00 | Sun, 11 Jan 2009 14:32:00 PST |
| 15 | Satoshi acknowledges Hal ran 0.1.2 and broke( sends msvc version) (WSJ) | Mon, 12 Jan 2009 00:36:00 | Sun, 11 Jan 2009 16:36:00 PST |
| 16 | **Block 170 gets mined** | **Mon, 12 Jan 2009 03:30:25** | **Sun, 11 Jan 2009 19:30:25 PST** |
| **17** | Satoshi sends 0.1.3 exe to Hal(WSJ) | Mon, 12 Jan 2009 05:31:00 | Sun, 11 Jan 2009 21:31:00 PST |

43 - Table Hal + Dustin Timestamps

Even if Dusting would have joined the network at Block 76, that would still not be before Hal, which we know from the private emails + the debug.log file + sourceforge mail list post he did just before Block 49.

So even though Dustin is a VERY early adopter of Bitcoin, Hal still beat him to it, by 30 blocks or so. Sorry Dustin :)

*For the sake of correctness, I want to clarify that the hardcoded IP Dustin mentioned in the tweet, was not Satoshi's IP, but the fallback IP of the freenode IRC server as we can see here in the code hosted on sourceforge.*

```
+void ThreadIRCSeed(void* parg)
+{
+    SetThreadPriority(GetCurrentThread(), THREAD_PRIORITY_NORMAL);
+    int nErrorWait = 10;
+    int nRetryWait = 10;
+
+    while (!fShutdown)
+    {
+        CAddress addrConnect("216.155.130.130:6667");
+        struct hostent* phostent = gethostbyname("chat.freenode.net");
+        if (phostent && phostent->h_addr_list && phostent->h_addr_list[0])
+            addrConnect = CAddress(*(u_long*)phostent->h_addr_list[0], htons(6667));
+
```

In the irc.cpp file: https://sourceforge.net/p/bitcoin/code/1/

44 - hardcoded IP

- https://sourceforge.net/p/bitcoin/code/1/?fbclid=IwAR1ZR36qInRQsc7WyPfrtGbNVDjX2xg__ztVp0uEajPK4az0nMwrdIwTQYY#diff-19

*The earliest versions of Bitcoin with the source code(https://satoshi.nakamotoinstitute.org/code/) I can find were Bitcoin v0.1.1 and Bitcoin v0.1.3. The hashes for both versions match the hashes in the RSS feed from sourceforge*

*found on web.archive.com, and both v0.1.1 & v0.1.3 do not have the 216.155.130.130 fallback IP in irc.cpp*
*The screenshot with green background is from sourceforge, and the earliest version we can access here is Bitcoin v0.1.5, and this is the 1st version to have the IP.*

*This detail does not really invalidate the other things Dustin said, and it is a pretty easy thing to confuse.*

# So what is the grand conclusion?

So in this article we **dethroned Hal from being the 2nd node to join the Bitcoin Network to the 3rd node**, thus making him the 3rd person also, but then we **re-instated him to the 2nd person**, as we suspect the 2nd Tor node was also Satoshi.

We found out some never know facts about Bitcoin's inception which after this many years is quite something:

- Hal missed Bitcoin's Launch
- Hal join Bitcoin around Block 49
- There were 2 nodes present when Hal joined
- Bitcoin halted for 24 hours and 8 hours in the first 30 blocks

But more importantly we got a very intimate view on how fragile these early days were, and how Bitcoin barely took off.

But anyway in the grand scheme of things it doesn't matter who actually was 1st and who was 2nd node.

What matters is that there were some people in this very early and fragile starting point of Bitcoin that decided to run the Bitcoin Client, and **if not for them Bitcoin may have never taken off.**

Here there were all these cryptographers on the Cryptography Mailing List, most of them probably waiting for the next breakthrough in cryptography, and one day out of nowhere an anonymous guy drops one of the biggest invention/discovery of the century, just like that, and almost everyone ignores it!

But for some reason Dustin and Hal, looked at this strange project that promised so much, without any trace of cynicism and judged for what it is.
They saw **Bitcoin as Bitcoin, not as Bitcoin made by this strange Satoshi** character!

And because of this very simple and honest gesture they changed the world and deserve a place in history! And for that I want to say a very sincere thank you Gentleman.

Another important thing to note is that Hal's debug file was available for 16 years and the emails for 10 years, and yet no one bothered to look at them and even Dustin when himself mentioned he was the 1st and only 100 people took interest in the tweet.

So if you take anything from this very long article is to **ALWAYS verify** what other people are saying, and next time you encounter a strange new idea that makes big promises, **be like Hal and Dustin**, you may just change the world yourself.