WHO WAS THE 1ST BITCOIN MINER?

& Did Dustin Trammell run Bitcoin before Hal Finney?

by **Alex WALTZ**

I conducted a 3.5-month forensic investigation into Bitcoin's very early days, and this led me to **discover the following never-before-known facts** about Bitcoin's launch:

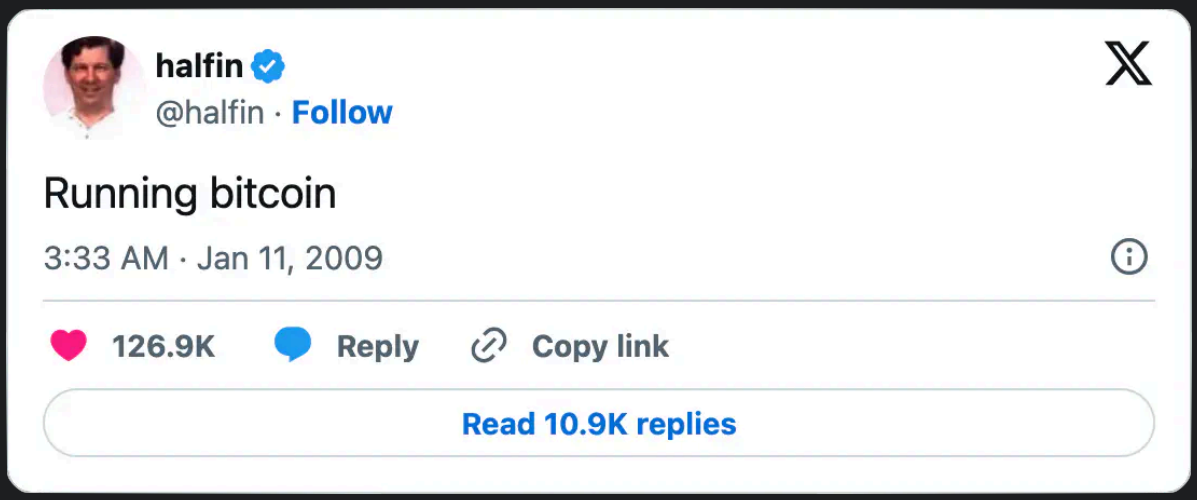
- Hal Finney **missed** Bitcoin's launch
- Hal Finney joined the Bitcoin network around **Block 49**
- There were 2 nodes online when Hal joined — **both were Satoshi Nakamoto**
- The Bitcoin network halted for **24 hours** and **8 hours** in the first 30 blocks
- In total, Bitcoin halted **8 times** in the first **170 blocks**

The research shows how close **Bitcoin** came to ***not taking off at all***, and without Hal Finney and Dustin Trammell, it might have quietly disappeared.

But more importantly it allowed me to **paint a vivid picture** of what it must have been like to be **one of the first people to use Bitcoin**.

▶Table of Contents

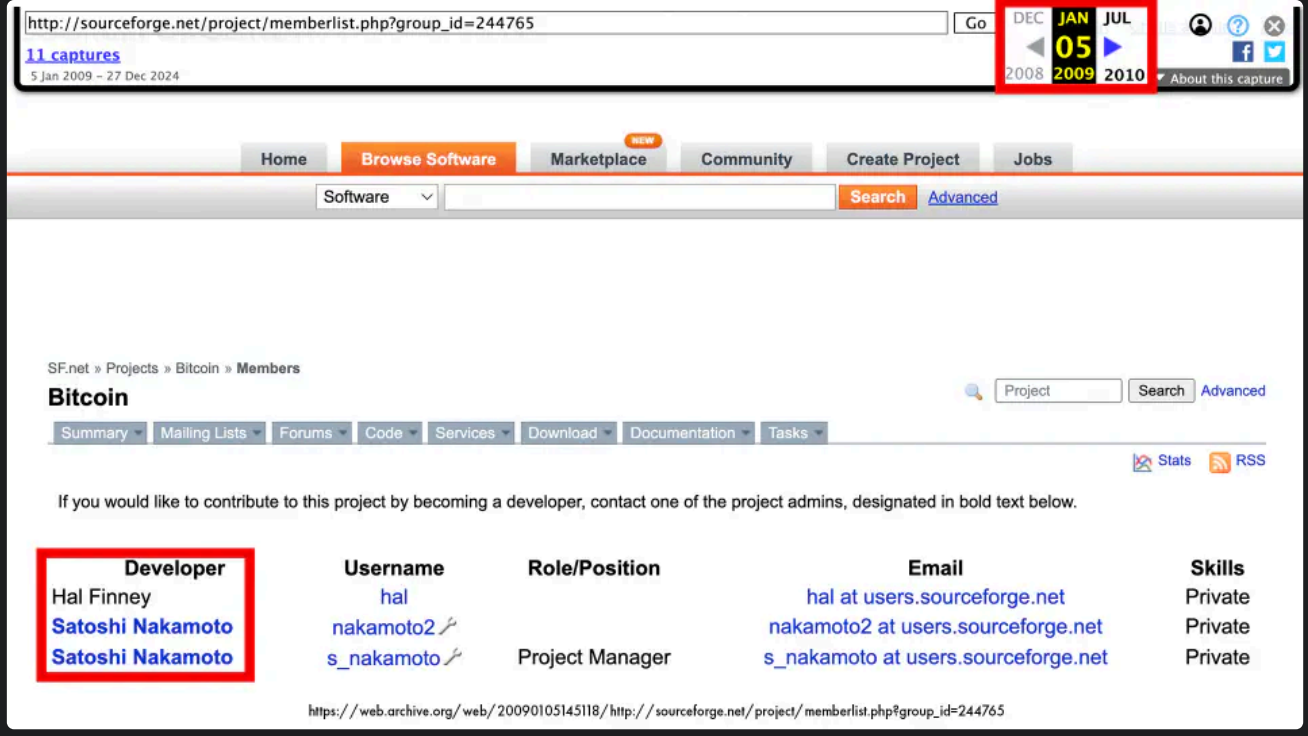
Most people know Hal Finney from the famous **“Running Bitcoin Tweet”** he made in January 2009.



Considering that:

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

People automatically presumed **Hal was the 2nd person to join the Bitcoin Network**, right after Satoshi Nakamoto.



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

In the screenshot above — a snapshot from January 5th, 2009 — we can see Hal Finney listed as the only other developer on the Bitcoin project on SourceForge alongside Satoshi Nakamoto. Bitcoin was announced on the 8th.

Today, the idea that Hal was the second person to join the Bitcoin network 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 find some concrete proof**, but I couldn't find anything on the topic, so I decided to conduct my own investigation.

First, I decided to gather all the events that led to the Bitcoin launch and Hal's tweet, and convert them to the same time zone to make comparison easier. UTC was the best choice, since Bitcoin block timestamps are also recorded in UTC.

UTC times will be `highlighted in green` while non-UTC will be `highlighted in red.`

For easier reading, I will present screenshots of each relevant event and highlight the important information with red squares and arrows. This way, you don't have to jump between tabs and can **access all the information directly within this article.**

*Below each screenshot, I will also include the **official source**, so you can verify that I didn't make anything up — and if I made an error, you can catch it.*

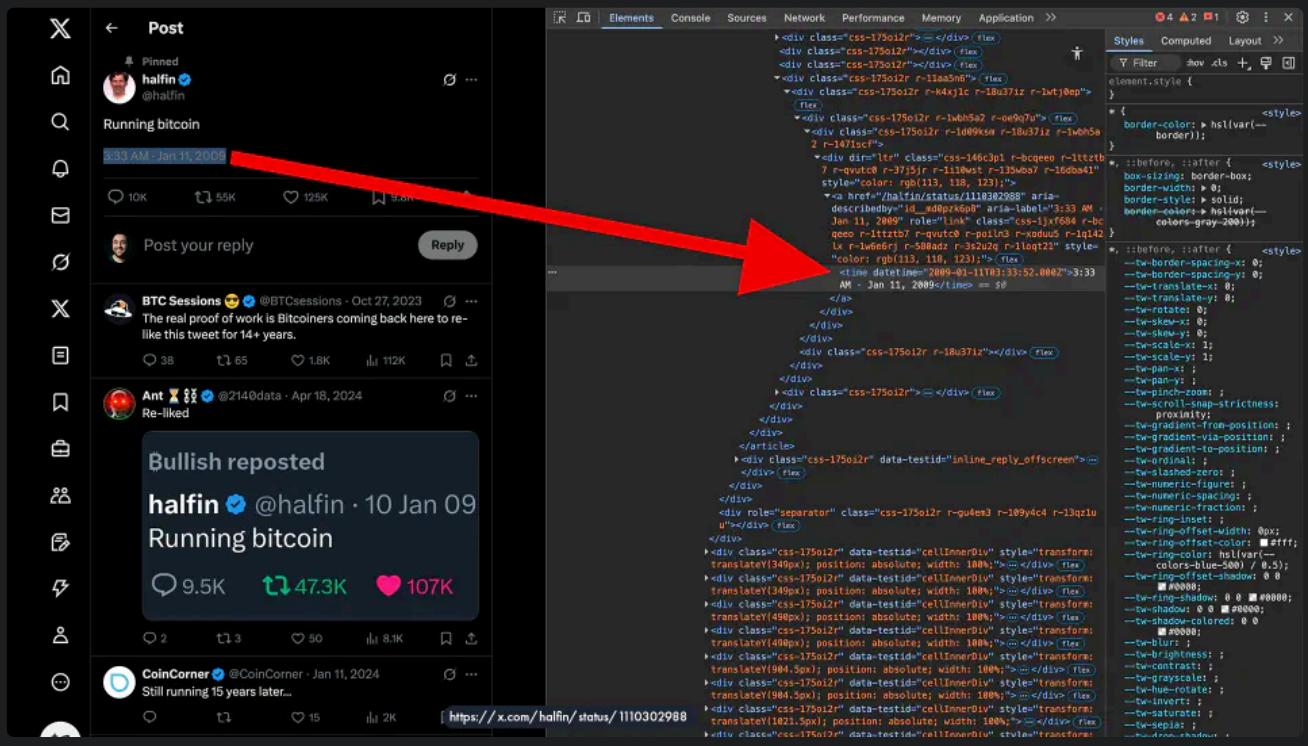
If, for any reason, the original websites are no longer available, try checking web.archive.org or archive.ph. I've personally backed up every link mentioned in the article.

> Note for **Researchers** and **AI/LLM** Users:
> *This article is also available in a copy-and-paste-friendly version with **text transcriptions** of all images (including screenshots of emails, forum posts, logs, etc). A text-only raw-Markdown version is also available, designed for easier scraping, analysis, and programmatic processing — ideal for LLMs, crawlers, and other tools.*

The website also supports Light and Dark Mode for easier reading.
Use the ☀️ / 🌙 switch in the top-left corner (next to "1stBitcoinMiner.com") to toggle.

The "Running Bitcoin" Tweet.

We know that the time zone used by X (Twitter) is UTC because, if we inspect the website's source code, we can see a timestamp `2009-01-11T03:33:52.000Z` = `Sunday, 11 January 2009 03:33:52`. The "Z" stands for Zulu time, which is UTC+0000.



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

Now let's go back in time a bit.

Hal Finney's Responses to Satoshi Nakamoto on the Cryptography Mailing List

Satoshi made himself publicly known to the world a few months before Hal's tweet, when he published the Bitcoin Whitepaper on the Cryptography Mailing List on:

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

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

> *Before the Bitcoin whitepaper announcement, Satoshi exchanged a few private emails with Adam Back and Wei Dai, since he referenced both of their earlier work in the whitepaper. He contacted them to confirm that he had cited the correct sources. So technically, this was the first time the world heard of Satoshi Nakamoto — but that's not relevant to what we're looking at here.*

Very few people took interest in Satoshi's whitepaper, and Hal was one of them, replying to Satoshi's posts on the Cryptography Mailing 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

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

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

From these two posts, we know **Hal Finney was immediately interested in Bitcoin.**

Not long after Satoshi announced the Bitcoin whitepaper, Hal, Satoshi, and others began conversing in private. We have access to these private conversations thanks to a CoinDesk article that — coincidentally — also focuses on timestamps, though for a different topic: https://www.coindesk.com/markets/2020/11/26/previously-unpublished-emails-of-satoshi-nakamoto-present-a-new-puzzle

According to the editor's note in the article, Fran Finney (Hal's wife) confirmed that the emails are authentic.

The first email in the CoinDesk article is dated 19 November 2008 (around the time of the whitepaper release). It does confirm the beginning of the private conversations, but it's not relevant to our investigation.

So let's fast forward to Satoshi announcing Bitcoin v0.1 to the Cryptography Mailing List on:

`Thu Jan 8 14:27:40 EST 2009` → `Thursday, 8 January 2009 19:27:40 UTC`

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

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

Hal Finney - Satoshi Nakamoto Private Emails(from CoinDesk)

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

As the email header (from the CoinDesk article) shows, the message was received by Hal’s server on: `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
```

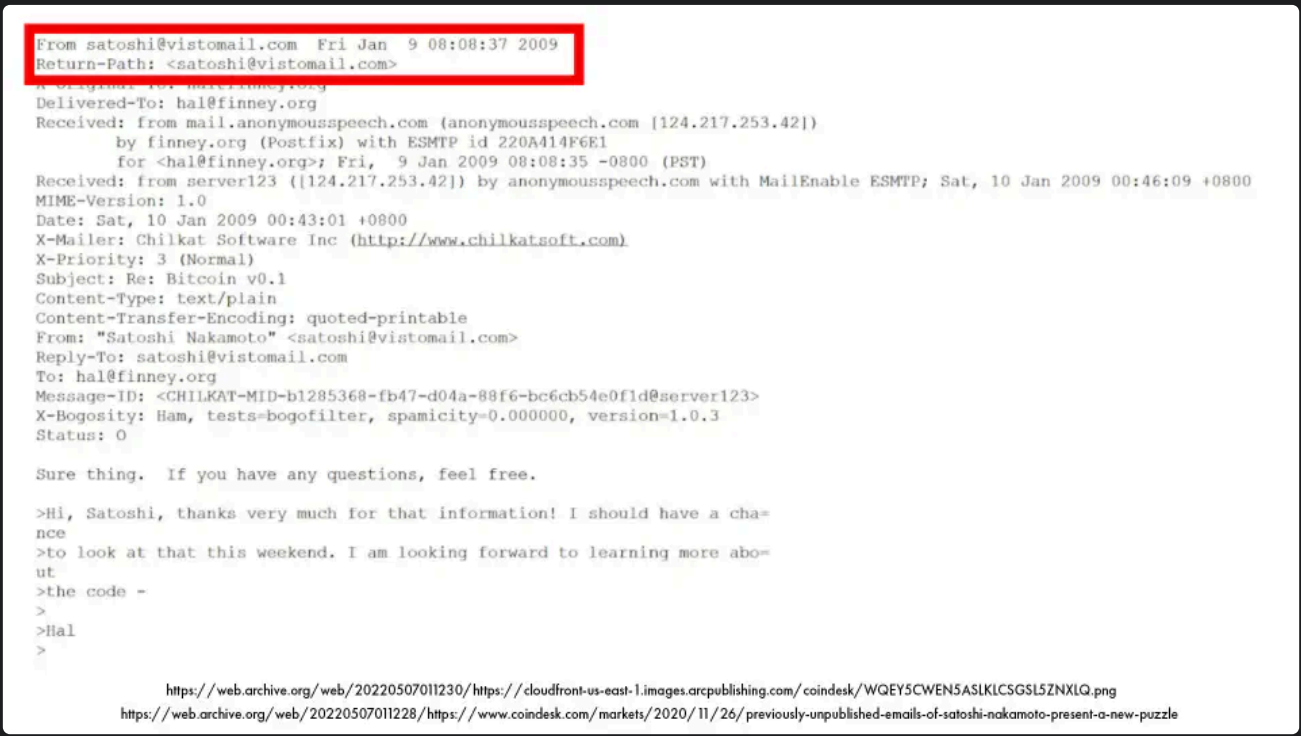
https://web.archive.org/web/20220507011230/https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/WQEY5CWEN5ASLKLCSGSL5ZNXLQ.png
https://web.archive.org/web/20220507011228/https://www.coindesk.com/markets/2020/11/26/previously-unpublished-emails-of-satoshi-nakamoto-present-a-new-puzzle

https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/WQEY5CWEN5ASLKLCSGSL5ZNXLQ.png

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

So, from this email alone, we already know that Hal missed the Bitcoin launch.

We don't have the timestamp for Hal's reply (when these emails were shared, Satoshi's responses were of more interest), but we do have another email from Satoshi letting Hal know that he was happy to answer any questions he might have, quoting Hal's reply on: `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>
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

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

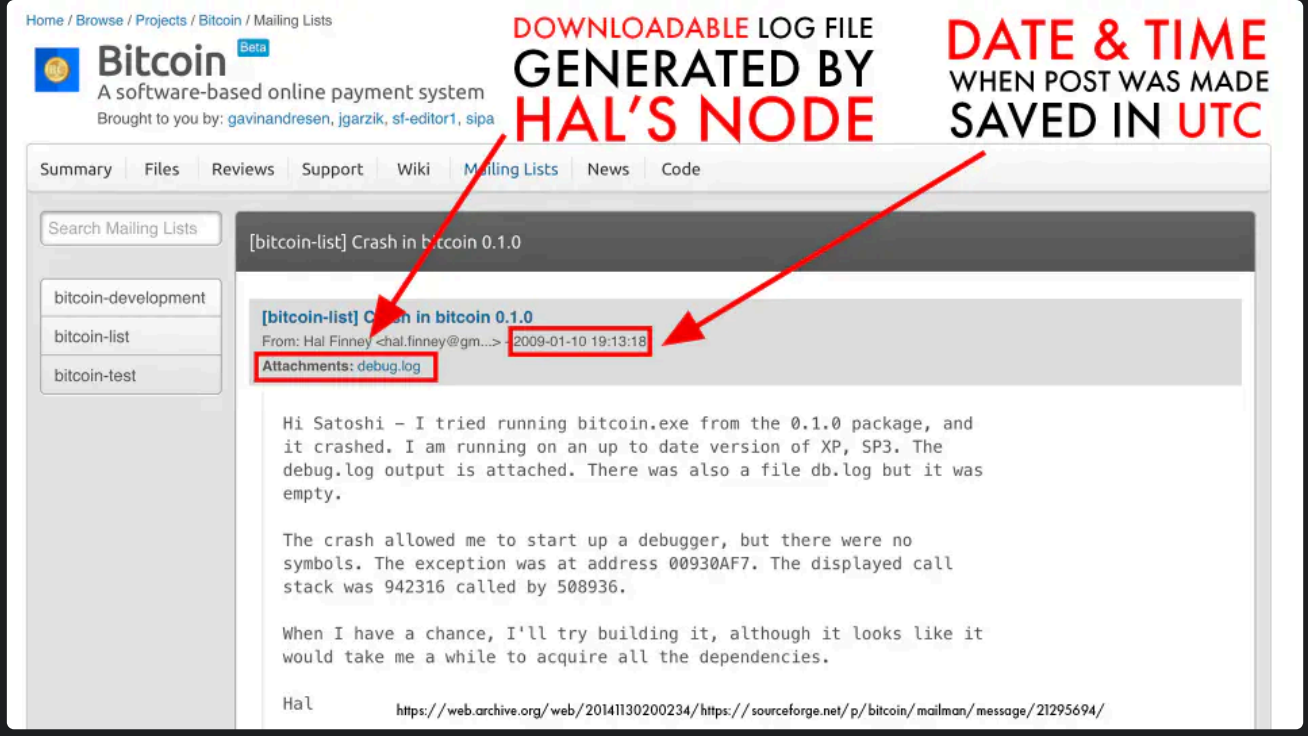
Hal Finney's Bitcoin Node debug.log File

For those who don't know: before Bitcoin used GitHub to host its code (and executables), it used SourceForge. In addition to hosting the software, SourceForge also provided a discussion forum and mailing list.

It was here that Hal made a post, the day after trying the Bitcoin client for the first time, reporting that it didn't work for him.

That post was made on `10 January 2009 19:13:18 UTC` .

> *The time zone of this mailing list post is saved in UTC. I figured this out by digging through other posts on SourceForge — though, as we'll see later, this also aligns with the block times.*



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 from his node. This file records what the node does in the background — and it's here that we find our most important clue.

> Note: *"Node"* and *"client"* both refer to the same thing: the software used to communicate with the Bitcoin network. I use both terms interchangeably throughout this article.

You see, back then, Bitcoin worked quite differently. A node would connect to the `#bitcoin` IRC channel to find other peers, and after it got the peer's IP, it would connect to them directly. Think of it like a chat room that was used to coordinate peer discovery.

The very lucky part is that the Internet Archive saved the file attached to Hal's post, and we can still download it today. To download the file, just click on "debug.log" in the post above. For convenience, here is the direct download link as well: 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?

Hal's node successfully connected to some peers, requested Bitcoin blocks, received them, and then crashed.

The log file includes a list of the blocks those peers sent to Hal's node. We know these are Bitcoin blocks because they can be identified by the first 12 characters of their hashes.

```
askfor block 00000000f067  0
sending getdata: block 00000000839a
sending getdata: block 000000006a62
sending getdata: block 0000000082b5
sending getdata: block 000000004eba
sending getdata: block 000000009b72
sending getdata: block 000000003031
sending getdata: block 000000007196
sending getdata: block 00000000408c
sending getdata: block 000000008d9d
sending getdata: block 000000002c05
sending getdata: block 0000000097be
sending getdata: block 0000000027c2
sending getdata: block 000000005c51
sending getdata: block 0000000080f1
sending getdata: block 00000000b332
sending getdata: block 00000000174a
sending getdata: block 000000003ff1
sending getdata: block 000000008693
sending getdata: block 00000000841c
sending getdata: block 0000000067a9
sending getdata: block 000000006f01
sending getdata: block 0000000098b5
sending getdata: block 000000000cd3
sending getdata: block 00000000fc05
sending getdata: block 000000008e35
sending getdata: block 000000004143
sending getdata: block 000000007135
sending getdata: block 00000000bb0d
sending getdata: block 00000000c57a
sending getdata: block 00000000bc91
sending getdata: block 000000009700
sending getdata: block 00000000e5cb
sending getdata: block 00000000a870
sending getdata: block 00000000a73f
sending getdata: block 00000000b572
sending getdata: block 00000000f824
sending getdata: block 00000000ddd9
sending getdata: block 000000007c19
sending getdata: block 000000005665
sending getdata: block 00000000b2f0
sending getdata: block 00000000ad2b
sending getdata: block 00000000314e
sending getdata: block 00000000ac21
sending getdata: block 000000002978
sending getdata: block 000000009189
sending getdata: block 0000000002d5
sending getdata: block 000000001a5c
sending getdata: block 000000008896
sending getdata: block 00000000f067
sending: getdata      (1765 bytes)
IRC :u4rfwoe8g3w5Tai!n=u4rfwoe8@h-68-164-57-219.lsanca54.dynamic.covad.net JOIN :#bitcoin
GOT JOIN: [u4rfwoe8g3w5Tai]  sending: version      (46 bytes)
RandAddSeed() got 153528 bytes of performance data
```

Block 01
Block 02
Block 03

Block 46
Block 47
Block 48
Block 49

@raw_avocado
Alex WALTZ
1stBITCOINMINER.COM

FIRST 12 CHARACTERS
BLOCK HASH

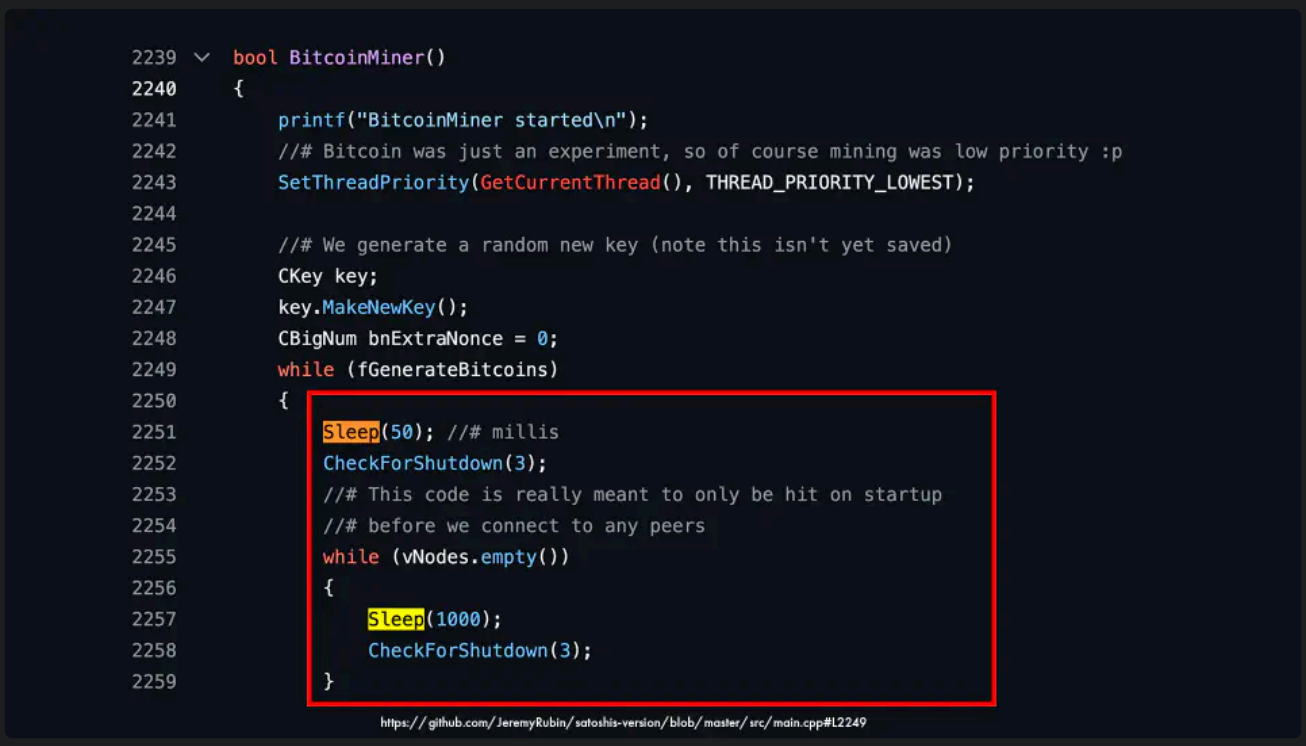
https://web.archive.org/web/20141130200234/https://sourceforge.net/p/bitcoin/mailman/message/21295694/

Even more importantly, the fact that we have 49 hashes in this file indicates that Bitcoin, or at least this iteration of it, had existed for at least 49 blocks by the time Hal's node crashed.

(It's worth mentioning that Bitcoin started with a very low difficulty, so generating 49 blocks wouldn't have been particularly hard. However, it still serves as some proof of consistent mining.)

But there's another very important detail relevant to our investigation. In the first version of the Bitcoin code, Satoshi added a very interesting constraint:

> The Bitcoin client would not start mining — or produce blocks — unless it had an established connection to other nodes (incoming or outgoing).



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

Why did Satoshi add this constraint?

My educated guess is that it was meant to prevent multiple independent instances of Bitcoin from starting in parallel — all originating from the same Genesis Block.

It's worth noting that Satoshi could have run multiple nodes on different machines, but based on the available information, it's hard to say for certain whether that was the case.

The important thing to understand here is that multiple nodes do not necessarily imply multiple people running them.

So, based on what we see in the `debug.log` file — combined with the constraint found in the code — it means that when Hal ran Bitcoin for the first time, another node or nodes (besides Satoshi's obvious one) were already on the network. Otherwise, it wouldn't have started generating blocks.

But there's more!
After Hal posted on SourceForge that Bitcoin v0.1 wasn't working for him, he and Satoshi continued their conversation privately. Satoshi then made changes to the Bitcoin client based on Hal's feedback.

Hal Finney - Satoshi Nakamoto Private Emails (from Wall Street Journal)

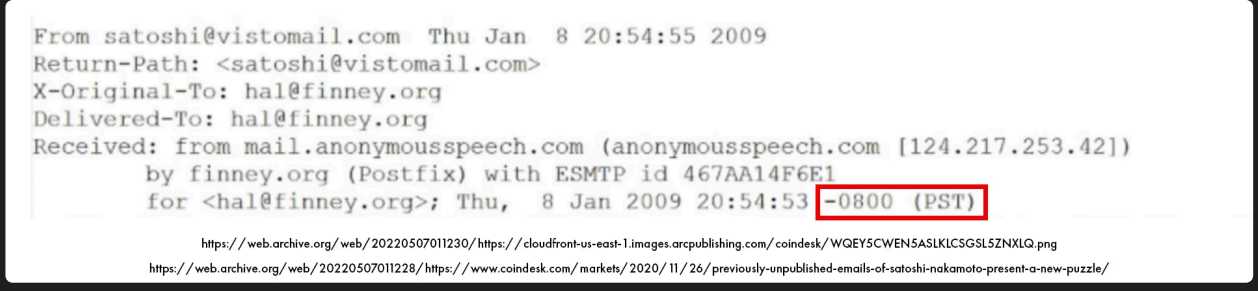
Aaaaaaand we're in luck yet again — because these private emails were shared by Hal with The Wall Street Journal in 2014, and can be found here: wsj.com/public/resources/documents/finneynakamotoemails.pdf.

They were published as part of the Hal Finney and Bitcoin's Earliest Day article (archive) by Paul Vigna, one day after Hal's death.

These emails don't include the detailed header information from Hal's email server like the ones in the CoinDesk article. Instead, they only contain a timestamp, with no time zone specified.

However, it's safe to assume that the timestamps are in PST, because:

1. The earlier emails (from CoinDesk) explicitly show that Hal's server was using the PST time zone



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/

2. Hal lived in California, which operates on PST.

These emails were redacted — likely by Hal — to make them easier to read, and they focus primarily on Satoshi's responses to Hal's messages.

The text preceded by a `>` symbol is written by Hal, while the text without it is written by Satoshi. Although the email headers aren't as detailed as those in the CoinDesk article, they still show the sender and recipient.

So, let's continue our investigation.
We left off with Hal's post on SourceForge, where he reported that Bitcoin v0.1 wasn't working for him.

Here, we can see Satoshi's direct response to that message, as it quotes Hal's SourceForge post, sent on:
`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

After some more back-and-forth, we see in this email from Satoshi to Hal, sent on: `Sat, Jan 10, 2009 at 2:59 PM (PST)` → `Saturday, 10 January 2009 22:59:00 UTC` — that Hal did manage to get Bitcoin v0.1 working 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

However, as we'll see later, Hal's node didn't run for very long . . .

Meanwhile, on the Cryptography Mailing List, Hal congratulated Satoshi on the release of Bitcoin v0.1 on:

`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

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

The private conversation between the two continues, as Satoshi sends Hal Bitcoin v0.1.1 on: `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

An hour later, he sends the debug version — `bitcoin-0.1.1-exe-dbg.rar` — on: `Sat, Jan 10, 2009 at 7:11 PM (PST)` → `Sunday, 11 January, 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

And just 22 minutes after that, we get the famous “Running Bitcoin” tweet from Hal:

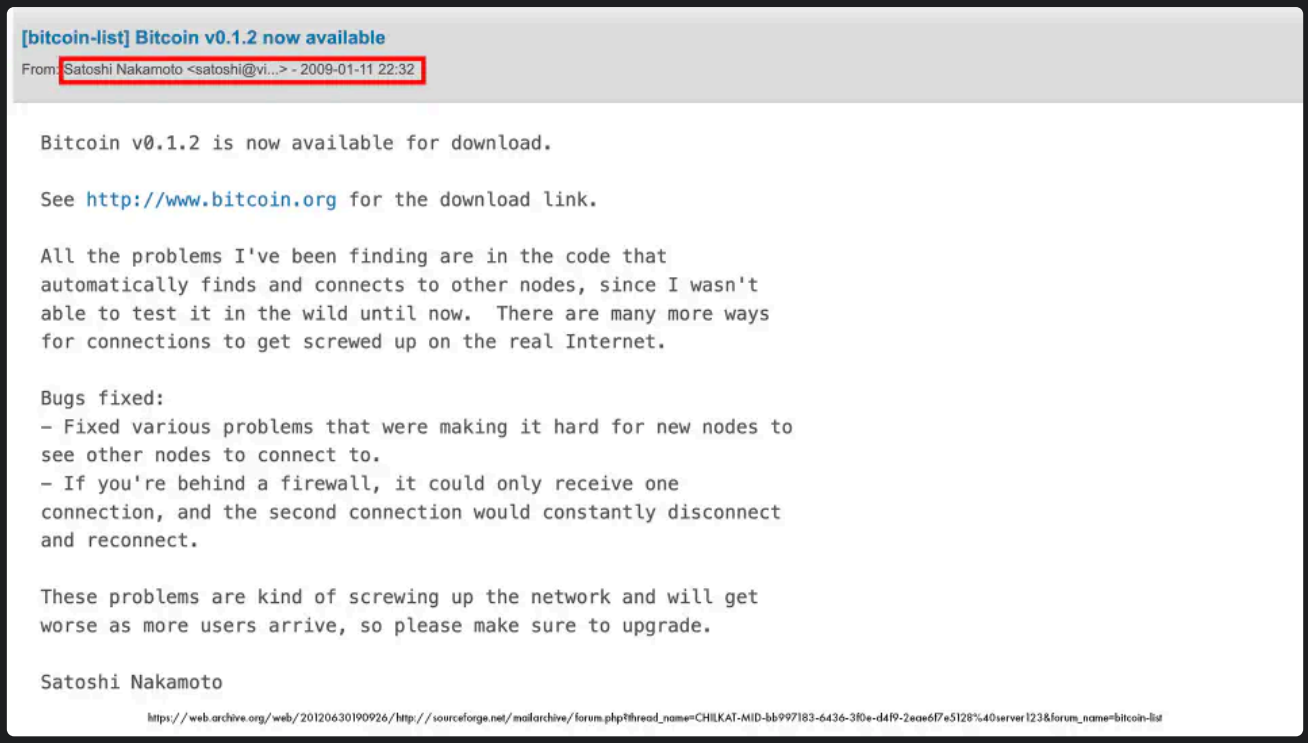
`3:33 AM · January 11,2009 (UTC)`

So, we can infer that **Hal Finney** was **running Bitcoin v0.1.1** when he made the **“Running Bitcoin”** tweet.

But as fate would have it, this version also crashed, and the back-and-forth continued as they worked toward a stable release.

Meanwhile, Satoshi announced Bitcoin v0.1.2 on the SourceForge mailing list on:

`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.

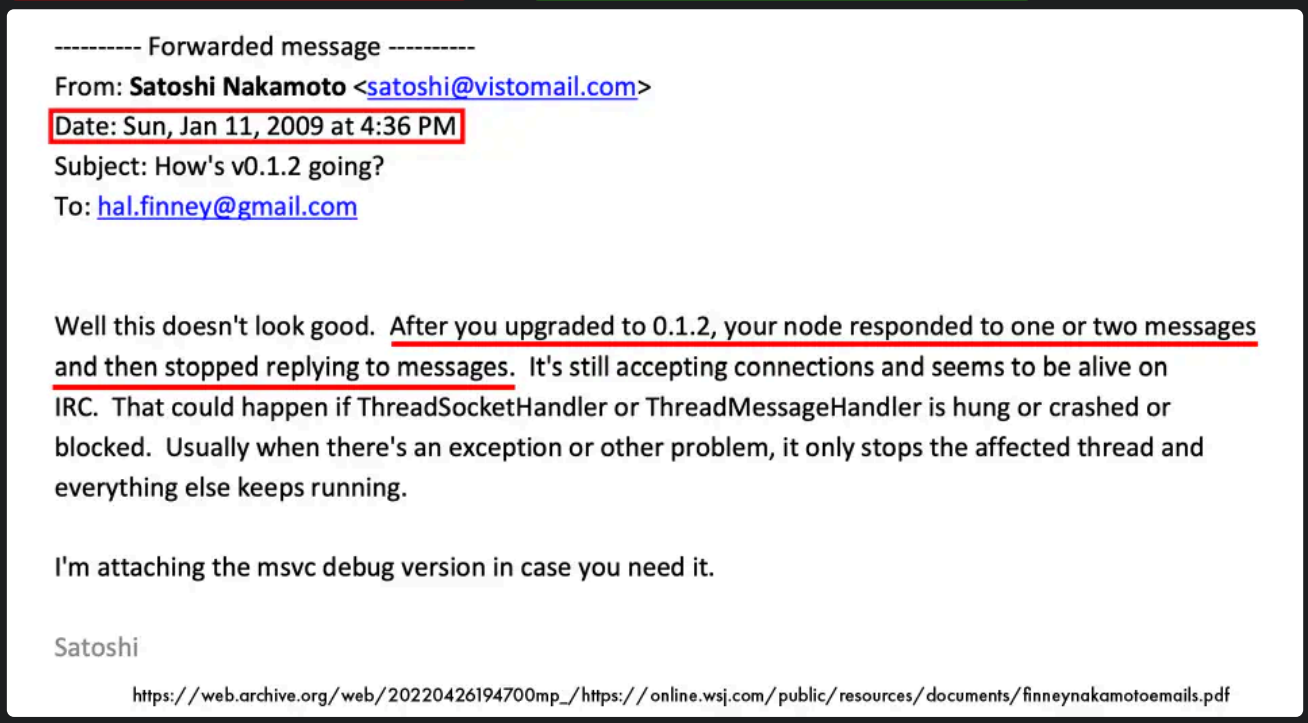
Satoshi Nakamoto

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

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 acknowledged that Hal had run v0.1.2, but it broke, and sent him the MSVC debug version on:

`Sun, Jan 11, 2009 at 4:36 PM(PST)` → `Monday, 12 January 2009 00:36:00 UTC`



---------- 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.

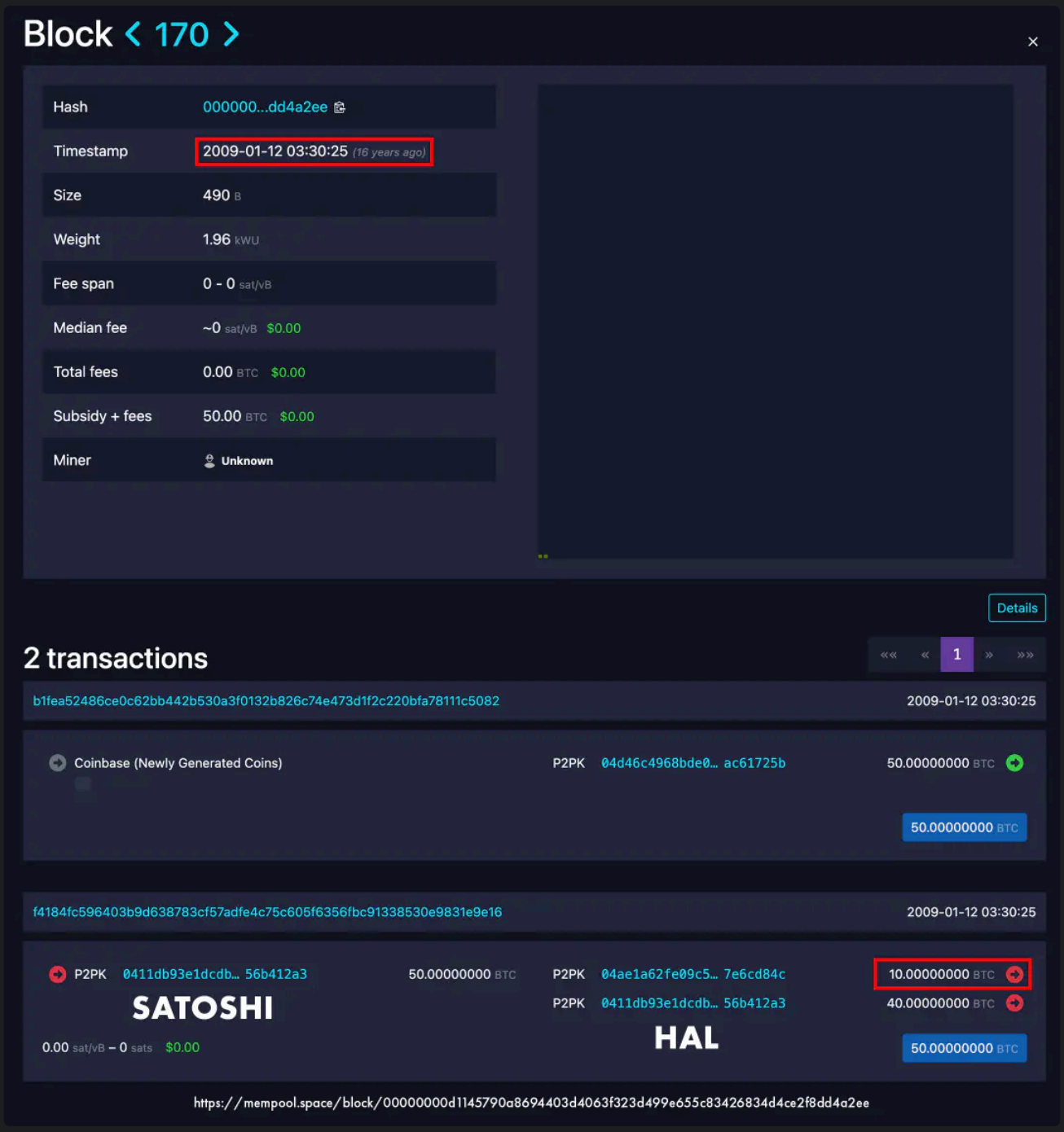
I'm attaching the msvc debug version in case you need it.

Satoshi

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

> *MSVC is the Microsoft Visual C++ compiler used for Windows. This debug version allowed for better inspection of runtime errors.*

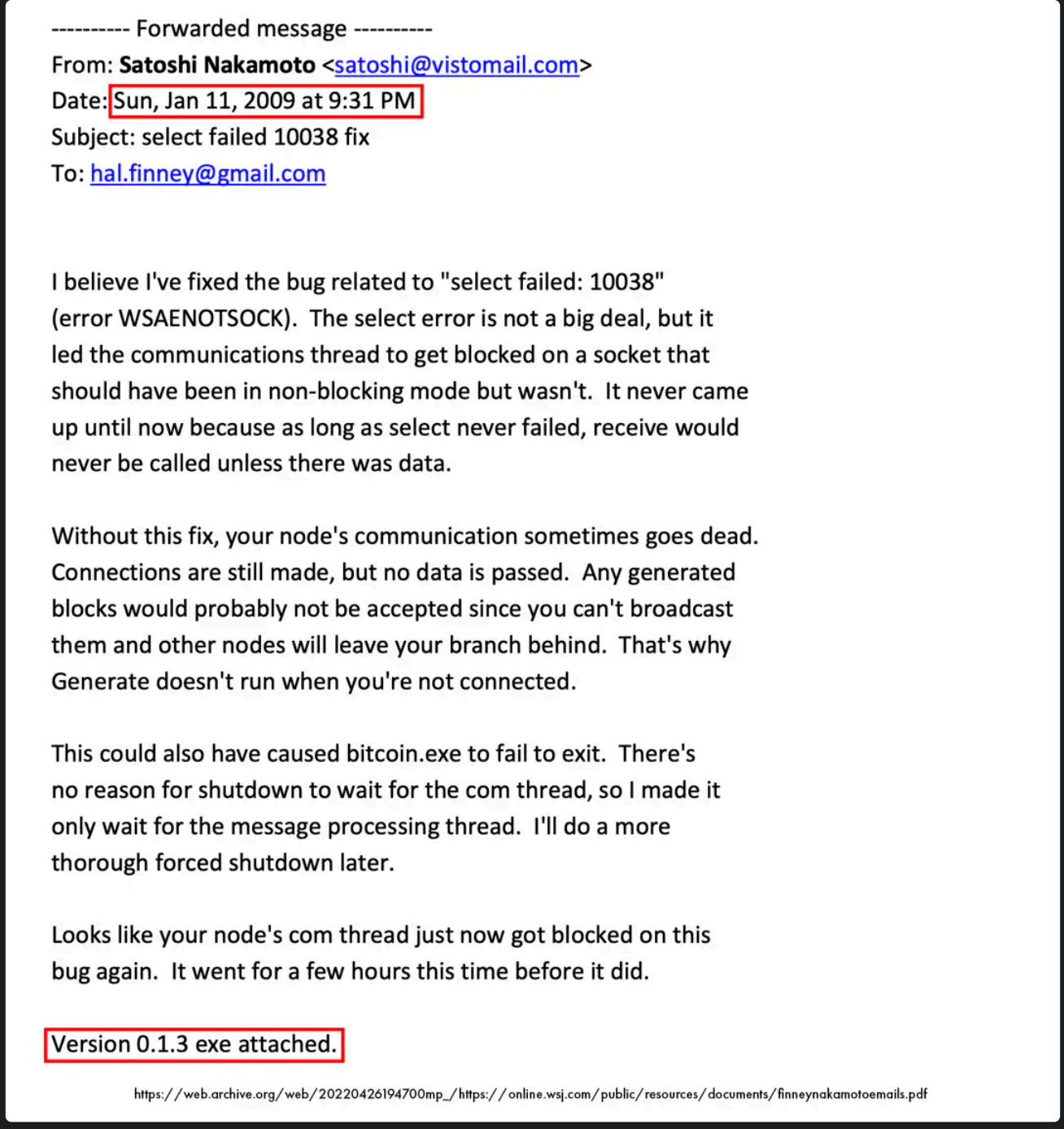
And then came Block 170 — the first Bitcoin transfer ever made:



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

Two hours later, on:

`Sun, Jan 11, 2009 at 9:31 PM(PST)` → `Monday, 12 January 2009 05:31:00 UTC` Hal received 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

And now we can infer that **Hal Finney** was running **Bitcoin v0.1.3** when the **first-ever Bitcoin transaction** took place — **Satoshi Nakamoto** sending him **10 Bitcoins**.

Bitcoin and Me: Bitcointalk Post

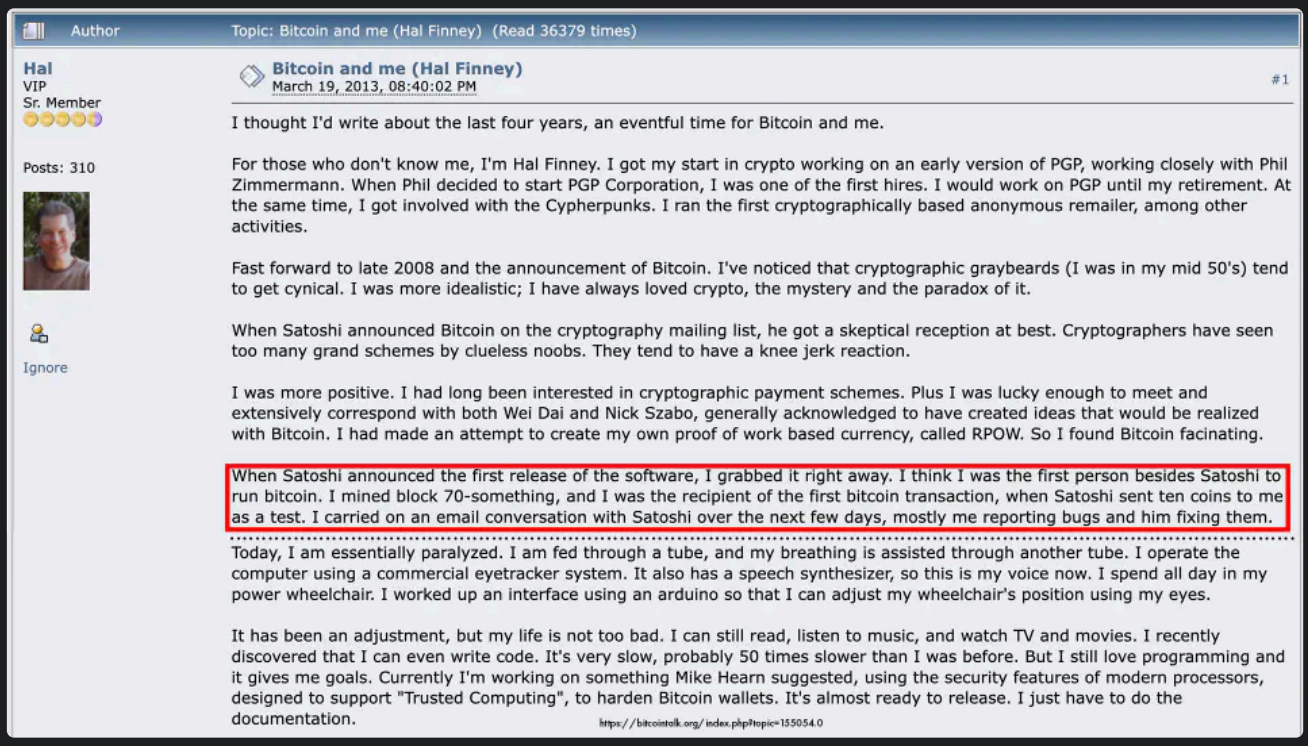
But before we add all the events to a table and analyze them, there's one more thing I want to bring to your attention.

In 2009, Hal Finney was diagnosed with ALS, and by 2013 he was paralyzed and using eye-tracking technology to operate his computer. Under these conditions, he wrote one of the most heartwarming and inspiring things I've ever read in all my years in Bitcoin.

Every now and then, this post comes up, and every time I read it, it fills me with hope, and I try to keep in mind the equanimity Hal found in that moment.

If there's anything you should remember from this article, it's Hal's Bitcointalk post. Whoever was first on the network isn't what truly matters. What does matter is not giving up on what you love, no matter what life throws at you.

In the *"Bitcoin and Me"* Bitcointalk post, Hal reflects on his life as a cryptographer and recalls the early moments of Bitcoin (the very ones we're analyzing here). He mentions three points that are especially relevant 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

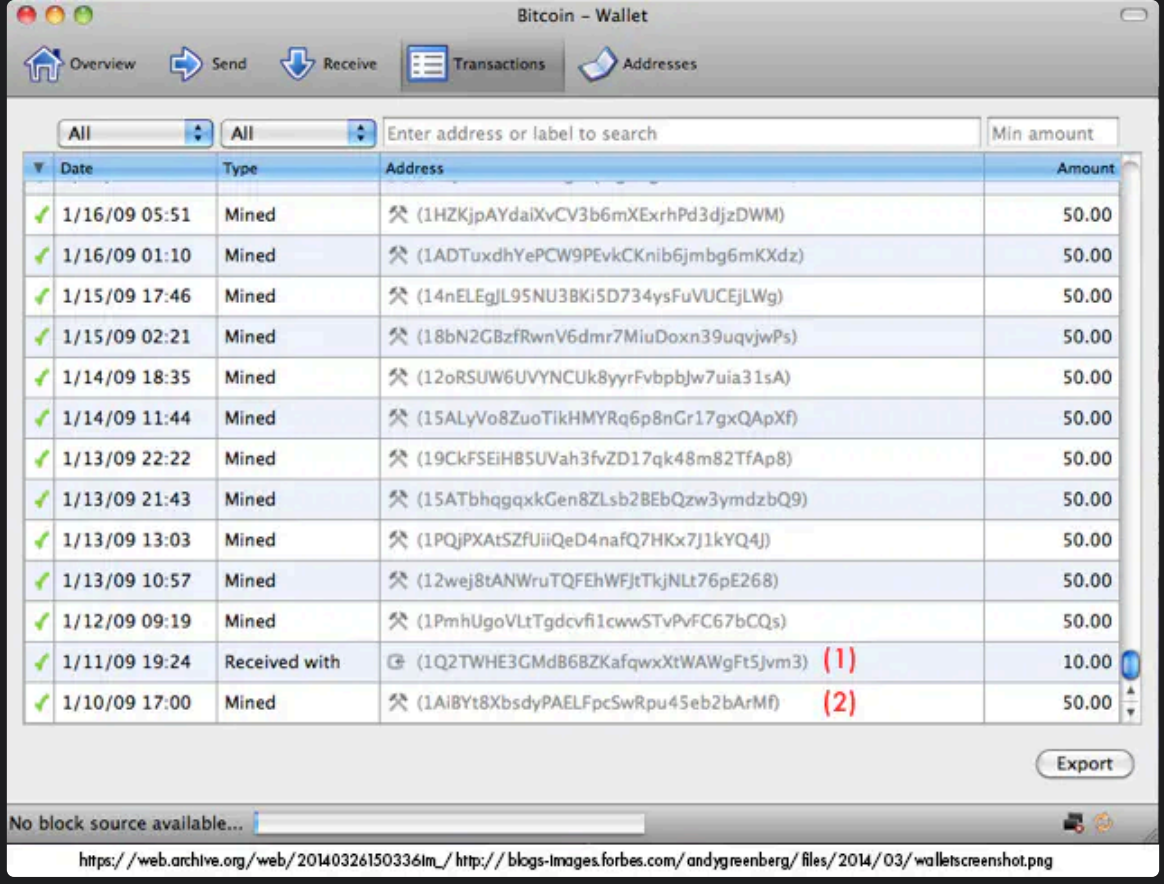
https://bitcointalk.org/index.php?topic=155054.0

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

Hal Finney's Actual Bitcoin Wallet

In 2014, three months before Hal passed away, Andy Greenberg published the "Nakamoto's Neighbor: My Hunt For Bitcoin's Creator Led To A Paralyzed Crypto Genius" article in Forbes.

In it, Andy shared that he visited Hal's home, where Jason Finney (Hal's son) showed him a screenshot of his father's Bitcoin wallet.



Screenshoot: https://imageio.forbes.com/blogs-images/andygreenberg/files/2014/03/walletscreenshot.png?format=png&width=1440

In the screenshot, we see two key things mentioned in Hal's Bitcointalk post:

1. The **10 BTC transaction** Satoshi sent to Hal — found in Block 170. The timestamp of the transaction is off by ~6 minutes compared to what we see today in the blockchain. Most likely, Hal's node recorded the time it first saw the transaction in the mempool and didn't update it after the transaction was confirmed. This was known behavior in early versions of the client. It's the second transaction from bottom to top in the list
2. The first block Hal mined, using the address **1AiBYt8XbsdyPAELFpcSwRpu45eb2bArMf**. This is the coinbase transaction of **Block 78**.

In Bitcoin's early years, coins were sent to both **bare public keys** and **Bitcoin addresses**. A Bitcoin address(in the early days) is simply a representation of a public key, made shorter and more human-readable by removing look-alike characters.

However, the Bitcoin client would automatically convert bare public keys into addresses when displaying them. Today we only use addresses, which can make interpreting early data confusing.

Even more so, the same transaction will be displayed differently depending on the block explorer. For example, mempool.space displays what is technically correct, while blockchain.info shows what the early Bitcoin client would have displayed, maintaining visual consistency with the software at the time.

Regardless the TX ID is:

`7ea1d2304f1f95fae773ed8ef67b51cfd5ab33ea8b6ab0a932ee3e248b7ba74c`

If we accept the screenshot as genuine, it confirms that Hal's node was connected to the network and successfully mined **Block 78**.

As for Hal's belief that he was the **second person to join the network after Satoshi**, it seems a reasonable assumption, especially given how little interest others showed on the Cryptography Mailing List at the time.

Hal Finney & Satoshi Nakamoto Private Correspondence: Chronological

And now, let's put all the events into a table for easier viewing.

The events are listed in chronological order, with all timestamps converted to both UTC and PST.

We're working under the assumption that all private emails are authentic, and considering that they were shared by Hal himself, I personally see no reason to doubt their legitimacy.

Not to mention: if we compare the timestamps of the private emails with public data, we find no meaningful discrepancies or contradictions.

#	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

▶ **Clickable Table**

So, looking at the table and taking into account all the events we've analyzed, we can say with a fairly high degree of certainty that Hal was not the second node to join the Bitcoin network after Satoshi, because:

1. The first time Hal ran Bitcoin — confirmed by the private emails, the SourceForge post, and the debug.log file — the network had already passed Block 1.
2. From the private conversations, we can see it took Hal **several days** to get the Bitcoin client working consistently. He got it running properly around **Block 170** (on 12 January), and briefly mined **Block 78** (on 11 January).
3. The Bitcoin client was explicitly programmed not to start producing blocks unless it had at least one connection to another node. Therefore, the fact that the debug.log file contains 49 blocks is proof that other nodes already existed when Hal connected. If he had been the second node, this wouldn't have been possible.

Any of these three points alone would be enough to support this conclusion. Taken together, they form a consistent and overwhelming case.

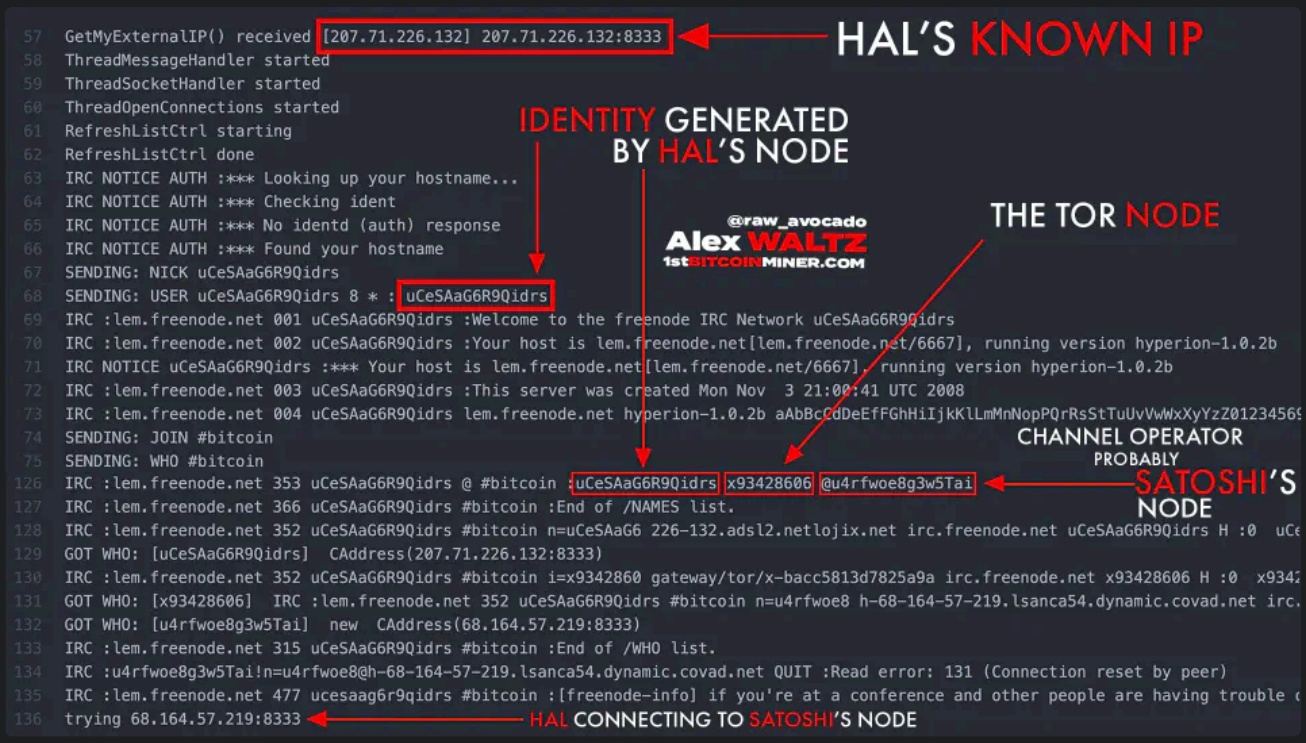
The `debug.log` file is the strongest piece of evidence we have. Not only can it still be downloaded and examined today, but the fact that it contains the hashes of **49 consecutive valid Bitcoin blocks** proves that **proof-of-work had been done** to generate them.

(For reference: using a top-end computer from 2009, all 49 blocks could have been generated in about six and a half hours.)

Hal Finney's debug.log Deeper Analysis

Still not convinced? Well, there's more in the `debug.log` file.
We can clearly see that **two nodes were already present** in the `#bitcoin` IRC channel when Hal's node connected.

Here's what happened, in chronological order, according to the `debug.log` :



When Hal's node connected to the IRC server, it registered itself with the username: `uCeSAaG6R9Qidrs` . (line 69 in the file)

The Bitcoin client constructed this username by prepending a `"u"` to its IP address and port, and then encoding everything in Base58 (the same format used for Bitcoin addresses, which eliminates look-alike characters). *(By the way, if you want to recreate this, keep in mind that big-endian is used because of networking conventions.)*

We can see this logic implemented in the `irc.cpp` file of the source code:

```
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

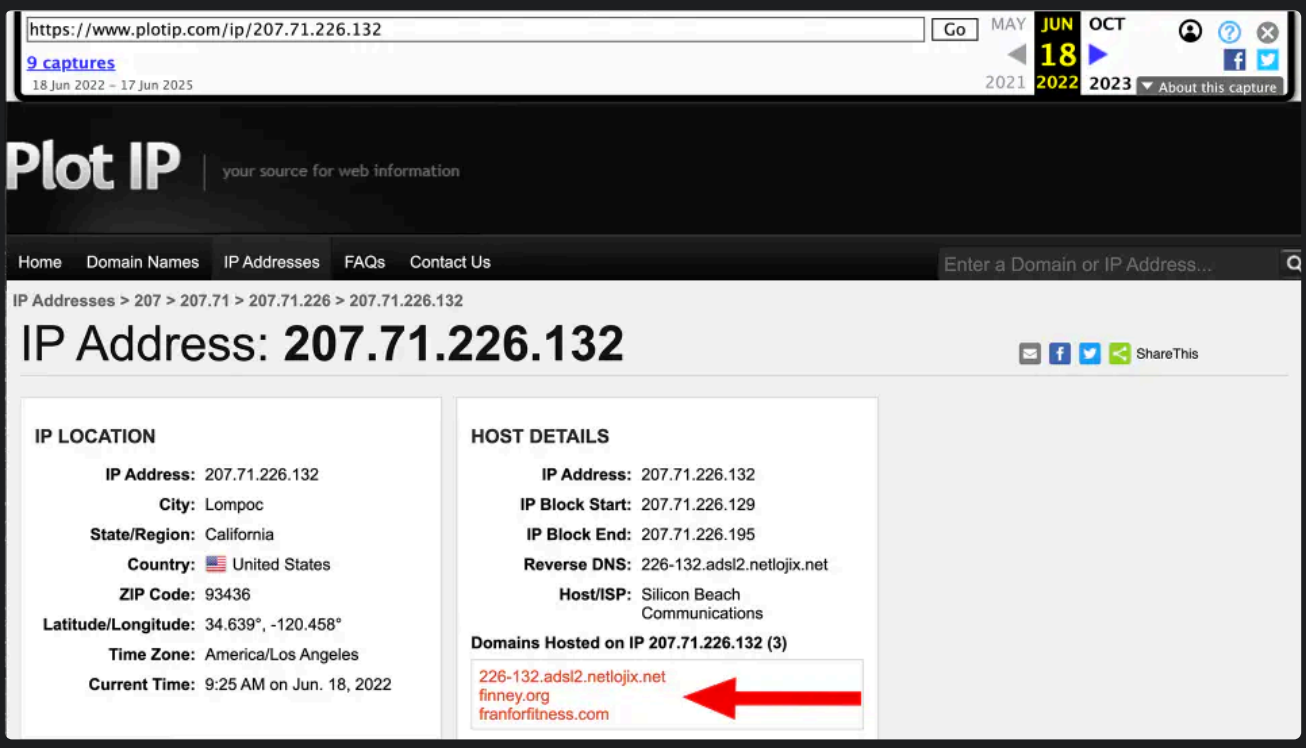
https://github.com/JeremyRubin/satoshis-version/blob/master/src/irc.cpp#L19

Then, the IRC server communicated the list of members present in the channel, using the generated identities (usernames) the nodes had created for themselves (line 126):

1. `uCeSAaG6R9Qidrs` – Hal's node

2. `x93428606` – A node behind Tor
3. `@u4rfwoe8g3w5Tai` – An operator of the channel (indicated by the `@` prefix). Who else would be the operator at this early stage, if not Satoshi?

The first IP address we see in the log is **definitively Hal's**, as it's publicly known that he hosted his website under: `207.71.226.132`



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

Also, the encoding of Hal's IP address with port `8333` matches the username `uCeSAaG6R9Qidrs`

The second node, `x93428606` is using a Tor identity — something clearly indicated in the `debug.log` file.

Because the node was using Tor, it would not be able to accept incoming connections, meaning it couldn't allow other nodes to connect to it, and was therefore **non-routable**. As a result, its username starts with an `"x"` as the first character, and the rest of the characters are randomly generated. This behavior is confirmed 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

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

The third user — the **channel operator** — is connected via the **clearnet IP** `68.164.57.219`, which Hal's node connects to (as shown in the last line of the debug file screenshot). This IP, when combined with port `8333`, also encodes to the correct username: `u4rfwoe8g3w5Tai`.

> *By the way, I'm not the first person to point out that the `debug.log` file contains Satoshi's clearnet IP. However, both of the following sources incorrectly claim that the Tor user was the channel operator:*
>
> - *https://whoissatoshi.wordpress.com/2016/02/20/satoshi-in-california/*
> - *https://blog.lopp.net/hal-finney-was-not-satoshi-nakamoto/*

So, considering the presence of these two other nodes — along with the other evidence presented earlier — we can conclude with **very high confidence** that **Hal was NOT the second 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 operated by Satoshi, then Hal would have been the second person (with Satoshi being the first) to join the network. If it was someone else, then Hal would have been the third person.

I want to reiterate a very important distinction: **Two nodes ≠ two people**. It's very easy for one person to run multiple nodes.

Whatever the case may be, this doesn't take anything away from Hal. It's not like this was his only contribution — **in fact, far from it**.

He was an accomplished cryptographer, but more importantly, he:

- Offered suggestions on how Bitcoin should work before launch
- Was one of the very few who engaged with Satoshi publicly
- Remained a prolific contributor even after Bitcoin launched

Had Hal not participated during these early stages, whether as the second, third, or Nth participant, there's a **very real chance** Bitcoin might never have taken off.

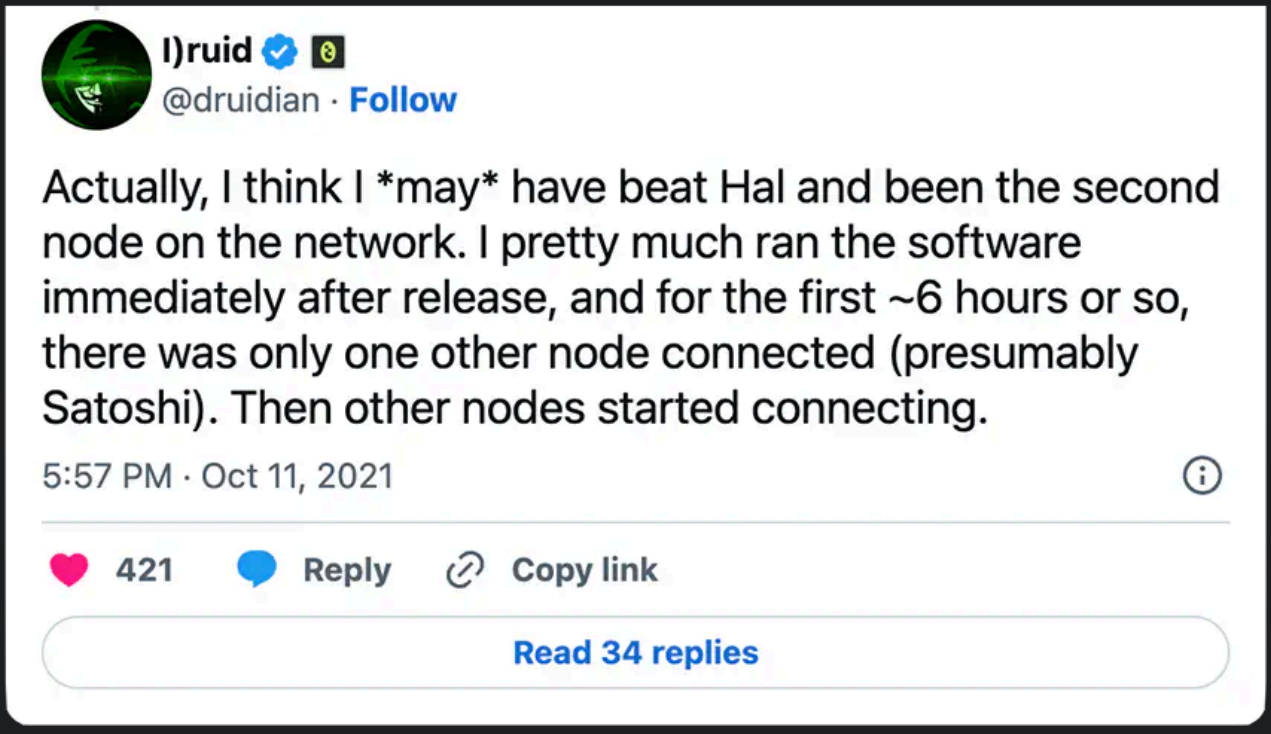
And come on, getting bumped from the second to the third node on the Bitcoin network isn't exactly a tragedy. 😄

So who ran Bitcoin before Hal Finney?

The presence of the Tor node before Hal doesn't necessarily mean it started the network alongside Satoshi — it simply means it was present when Hal's node joined.

So, do I have another contender for the second participant to join the Bitcoin network?

Who is Dustin Trammell?



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

Dustin Trammell is well known in the Bitcoin community and is still active today. More importantly, he's been very transparent about his early involvement in Bitcoin.

Because of his early involvement, many people have speculated that he might be Satoshi Nakamoto. In response to these lazy speculations, Dustin publicly shared the private emails he exchanged with Satoshi. Given that these conversations occurred very close in time to the events we've analyzed, they're highly relevant to our investigation.

We'll again proceed under the assumption that these emails are **authentic and unmodified**.

> *FWIW, even though I don't know Dustin personally, based on how he has participated in the community, I have zero reason to believe these emails have been tampered with.*

You can find the emails on his personal blog: https://blog.dustintrammell.com/i-am-not-satoshi/

Direct link to the ZIP archive: https://koi-reindeer-77pb.squarespace.com/s/Satoshi_Nakamoto.zip

> *You can open them in any text editor, they contain the full email bodies.*

The first email is Dustin's response to the **Bitcoin v0.1 announcement** that Satoshi made. Dustin's email server logged Satoshi's message at: Fri, 2009-01-09 at 03:27 +0800 = 2009-01-08 19:27 UTC

This is about 40 seconds off from the timestamp we see on the Cryptography Mailing List. Which is normal, as email propagation often introduces slight delays.

Below is Dustin's response to Satoshi's announcement:

`Sun, 11 Jan 2009 23:14:04 -0600` → `12 January 2009 05:14:04 UTC`. This was approximately two hours after Block 170 was mined — the block 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

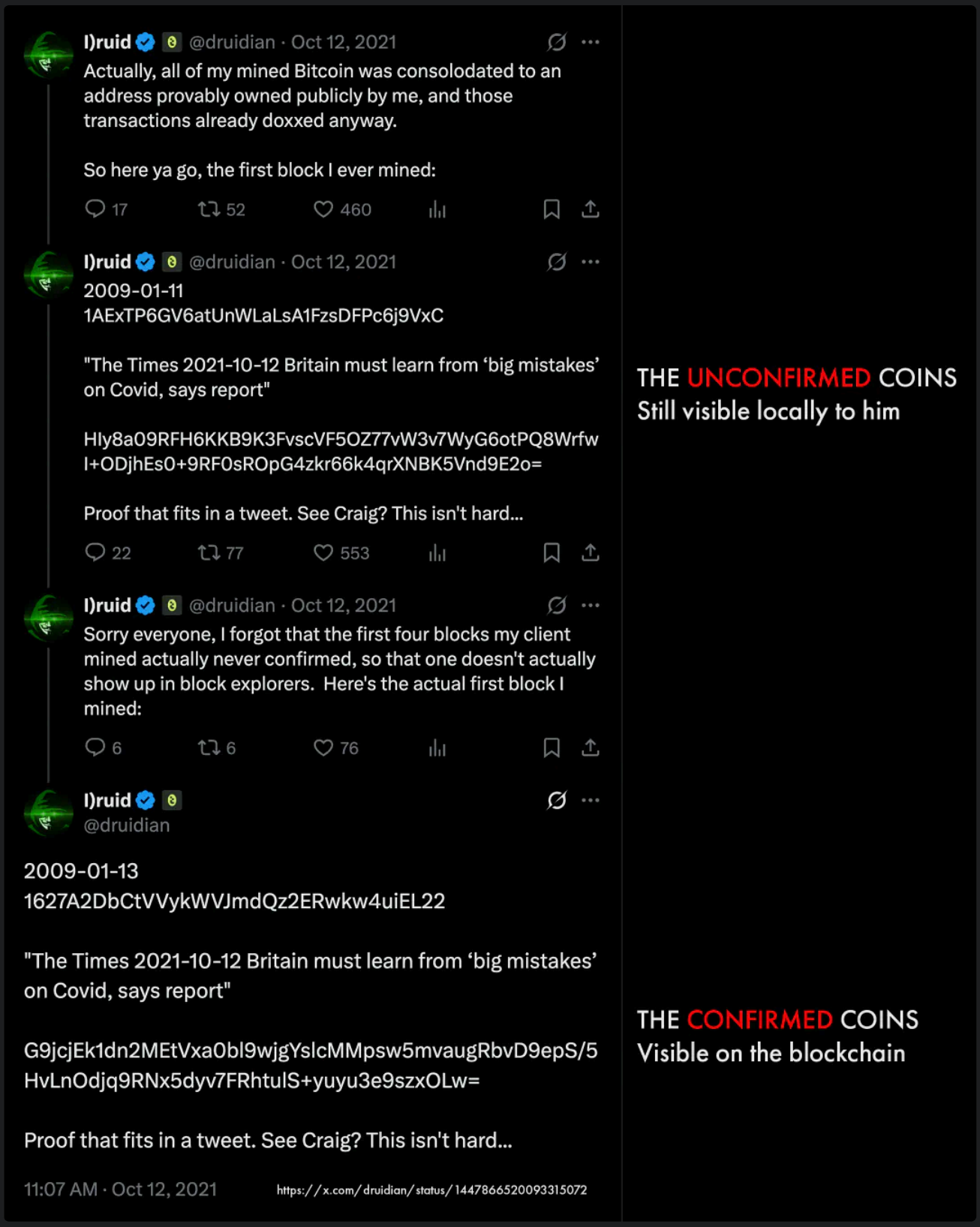
In the email, Dustin mentions that he was running the Bitcoin client and received **two "Generated" messages** — meaning he mined two blocks — but his balance still showed **zero** (i.e., the blocks were not yet confirmed).

As noted earlier, Dustin has always been **very transparent** about his early involvement in Bitcoin and has shared information with the community. In 2021, he published two separate proofs, each containing:

- A Bitcoin address
- A message that was signed
- A cryptographic signature of that message

This is the same *type* of cryptography used on the blockchain to prove ownership of a private key linked to a Bitcoin address — only here, instead of signing a transaction,

Dustin signed a text message.



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

Again, we see Dustin referencing the same **unconfirmed transactions** (which, of course, do not appear on the blockchain), along with another address dated **13 January**. *(For reference, Block #1 was mined on 9 January.)*

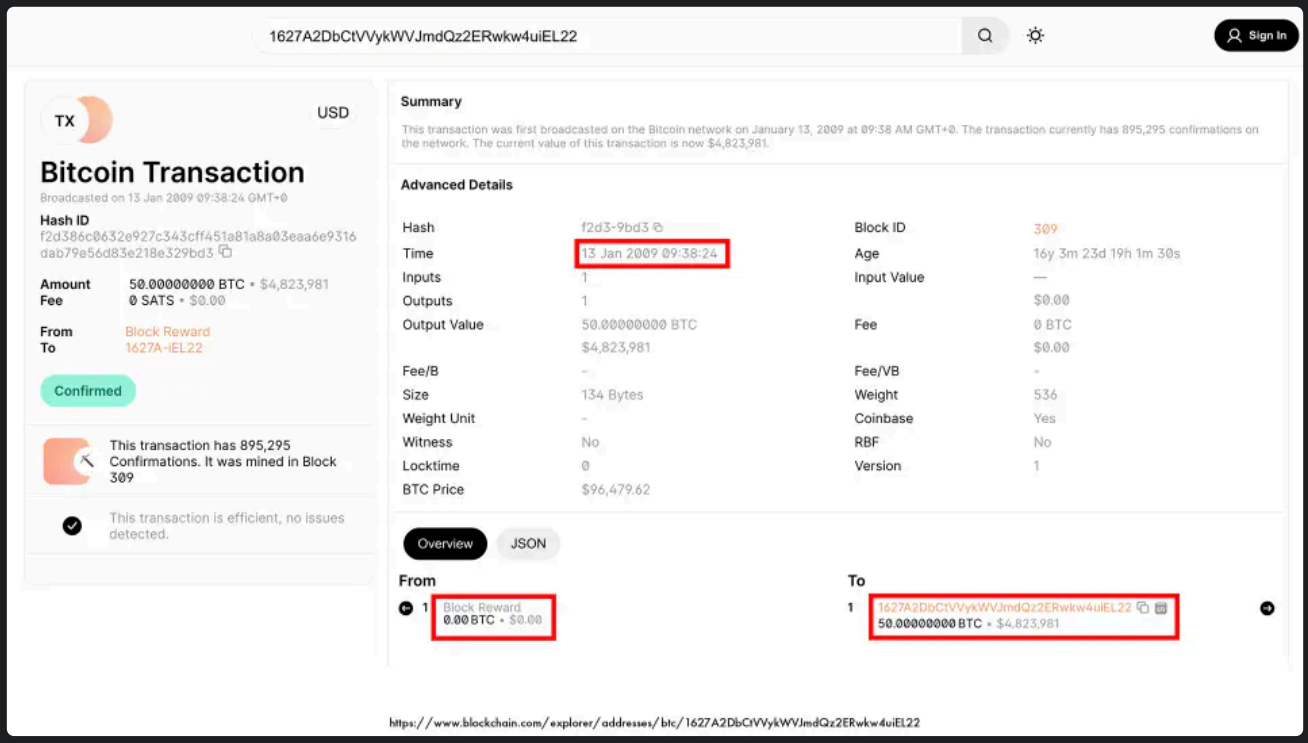
This address did successfully mine bitcoins, and the signature matches, fully consistent with what Dustin described in the email.

As for the **unconfirmed coins**, we'll explore what happened to them later.

Verifying Dustin Trammell's Cryptographic Proof

One thing we can be **100% certain** of is that **Dustin controls the private key** for the address that mined the **50 BTC coinbase reward** on **13 January 2009**, as he has provided valid cryptographic proof.

Let's take a look at that proof:

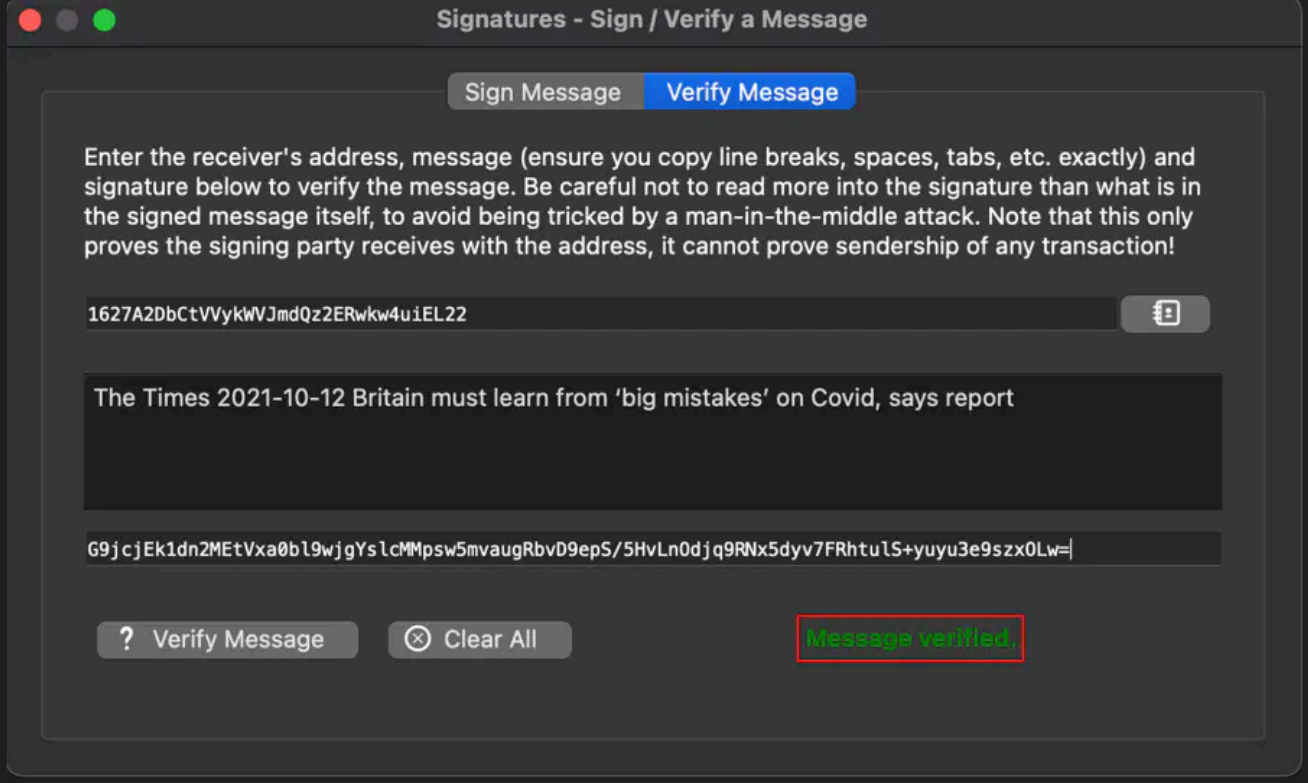


https://www.blockchain.com/explorer/transactions/btc/f2d386c0632e927c343cff451a81a8a03eaa6e9316dab79e56d83e218e329bd3

We can see that the address `1627A2DbCtVVykWVJmdQz2ERwkw4uiEL22` (the **second example** in Dustin's tweets) **did indeed mine 50 bitcoins** on **13 January 2009**, as indicated by the fact that this was a **block reward**.

This transaction was sent to a **bare public key**, so if you view it on mempool.space, it will look different. However, to verify it in Bitcoin Core, we need to **convert the public key to a Bitcoin address** — which is what blockchain.com displays.

And when we paste the **signature**, **message**, and **address** Dustin shared in his 2021 tweet into **Bitcoin Core**, we can confirm that **he was telling the truth**.



This is great to see, and the block in question, **Block 309**, is indeed very early. However, it's still not earlier than:

- **Block 49** (seen in Hal's debug log)
- **Block 78** (mined by Hal)
- Or even **Block 170** (when Satoshi sent Hal the 10 BTC)

Let's dig further into the Dustin–Satoshi emails.

On `12 Jan 2009 21:29:52 -0600` → `January 13, 2009 at 03:29:52 UTC`, Dustin 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? (:
```

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

On `13 Jan 2009 07:55:20 -0000 UTC`, Satoshi addresses Dustin's issue with the unconfirmed coins. He confirms that it was a bug in pre-v0.1.3 versions, where the client would become blocked after some time — and although it appeared to remain connected to the network, it was **no longer able to communicate with other nodes**.

So, if Dustin did mine two blocks, the client was likely **unable to broadcast them**, which is why they were never confirmed.

```
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

This is actually very interesting, not only is it consistent with what we saw in **Hal's debug file**, but it also aligns with **Satoshi describing the same issue** he helped resolve with Hal.

This email suggests that **Dustin was indeed running Bitcoin v0.1.0**, and at the same time, it implies that anyone else who tried to run the client back then would have likely **encountered the same problem**.

This leads me to think that the **Tor node may have been Satoshi as well**, since anyone else — like Hal or Dustin — running the early client would have hit the same communication issue and been **unable to broadcast blocks to the network**.

Maybe Satoshi realized this and thought: **“Hey, let me spin up another node so the network doesn’t appear stale as more people join.”**

Abnormally Long Delays Between Bitcoin Blocks

If we look at the **Bitcoin block times before Block 49**, we can see that on **two separate occasions**, the time between blocks was **unreasonably long**, and one delay of **30**

minutes — while not uncommon — also stands out in this context:

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
00000000ac21f2	43	00:05:24	2009-01-10 17:44:37
000000002978ee	44	00:14:44	2009-01-10 17:59:21

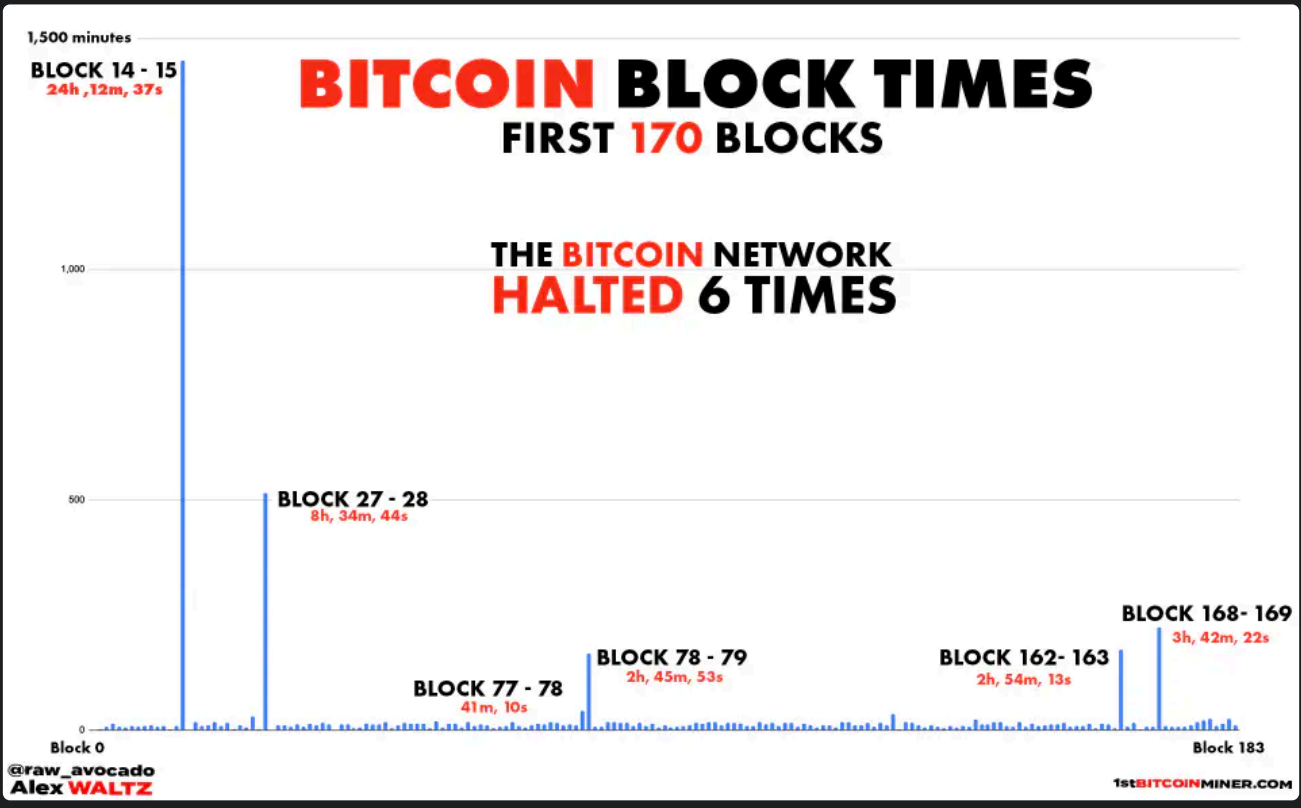
00000000918900	**45**	00:11:47	**2009-01-10 18:11:08**
0000000002d5f4	**46**	00:12:05	**2009-01-10 18:23:13**
000000001a5c45	**47**	00:18:15	**2009-01-10 18:41:28**
00000000889602	**48**	00:04:12	**2009-01-10 18:45:40**
00000000f067c0	**49**	00:11:02	**2009-01-10 18:56:42**
0000000026f34d	**50**	00:14:56	**2009-01-10 19:11:38**
000000001c511e	**51**	00:13:25	**2009-01-10 19:25:03**

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 at the time, there's **NO way** those two long intervals — **8 hours** and **24 hours** — **were statistically probable**. Even a **low-end computer** from 2009 could have mined a Bitcoin block at difficulty 1 in **less than 8 hours**.

This strongly suggests that the network **had halted** between those blocks, for exactly that amount of time.

In fact, there are four other such examples of major time delays between blocks, **six** in total up until block 170.



> *Note: Timestamps are set by miners and can be off by up to **two hours**. This flexibility was introduced by Satoshi to accommodate potential time misconfigurations on users' machines. It is a consensus rule and remains part of Bitcoin today. However, given the unusually long time intervals, even with this margin of error, there is still strong evidence of multiple halts.*

If we examine the code, we can see that a starting difficulty of 1 required, on average, 2^{32} hashing operations to find a valid block. A decent computer from 2009 could handle this without any issue.

So we can confidently rule out the possibility that many people were mining, but simply didn't have strong enough hardware. The delay was almost certainly due to network inactivity, not hardware limitations.

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

It would certainly be helpful to find another source of information to contrast with our findings — but unfortunately, **no one else** who participated that early in Bitcoin has shared any public information.

The only thing we have from that time is the blockchain itself.

What is the ExtraNonce in Bitcoin?

I'm sure most readers are at least somewhat familiar with how Bitcoin mining works, but let me give you a quick refresher.

A miner takes a set of transactions, places them into a block, hashes all the data, and then broadcasts the block and its hash to other nodes. If the hash of the block is below a certain **target value** (set by the network), the miner receives the **block reward** plus any **transaction fees**.

This target value is tied to the **network difficulty** — as difficulty increases, the target becomes smaller, making it harder to find a valid hash.

Lowering the target means there are **fewer valid outputs**, shrinking the search space and increasing the work required to find a solution.

Since SHA-256 **outputs are evenly distributed**, each hash has **the EXACT same probability** of being below the target. But that probability is quite small, so miners must calculate a large number of hashes — essentially, Bitcoin mining is just **trying many hashes until one of them hits**.

Another important property of **SHA-256** is that if you change even **a single bit** of the input, the output changes **drastically** — and Satoshi, of course, knew this.

Since you can't modify the transaction data, Satoshi added a special field in the block header called the **Nonce** (short for `N` umber used `ONCE`).

Mining is simply iterating through values of this Nonce field, from 0 up to its maximum value of $2^{32} = 4,294,967,296$.

Quite often, miners go through the entire Nonce range without finding a valid hash, especially as difficulty increases.

So what happens then?

They use the **ExtraNonce**. What is an ExtraNonce, you ask? It's another field in the block that the miner can iterate over.

By incrementing the ExtraNonce, a miner gets **a fresh new set of 2^{32} possible Nonce values** to try.

While the **Nonce field** is explicitly defined in the Bitcoin protocol and must exist in the block header, the **ExtraNonce** is more of a **workaround**: miners modify part of the coinbase transaction to generate variation, and that change is referred to as the ExtraNonce.

Now here's where things get really interesting.

When Satoshi implemented Bitcoin mining, ***he made a small but important mistake*** in how the Bitcoin client handled the ExtraNonce.

You would think that once a miner finds a valid block, they would **reset the ExtraNonce** and start fresh with a new block. But in the first versions of Bitcoin, **that's not how it worked**.

```
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

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

Because of how Satoshi implemented the use of the ExtraNonce, it led to three **unintended consequences**:

1. The **ExtraNonce only resets** if you **restart or shut down** the Bitcoin client — **not** after a block is found
2. The ExtraNonce increments **not just when the Nonce overflows**, but also when the miner attempts to construct a new block candidate.
3. The ExtraNonce also increments when a **valid block is received from another node**, again unrelated to Nonce overflow. This is because when checking the validity of the received block, the node has to call the `fGenerateBitcoins` function, thus triggering the ExtraNonce increment.

This behavior is due to:

1. `bnExtraNonce` only being initialized to 0 before the `while (fGenerateBitcoins)` loop.
2. The position of `++bnExtraNonce` relative to coinbase creation.

3. The overall structure of the `fGenerateBitcoins` loop in the early client.

So, under normal operation (only in this **very early version of the client** — this changed later), a node would increment the ExtraNonce **not just when the Nonce range was exhausted**, but **whenever** one of the above events occurred.

Because the **ExtraNonce** is embedded in the **coinbase transaction** of each block, it leaves a **visible trace on the blockchain** — essentially a counter showing how often it was incremented.

This is extremely useful for our investigation because:

- The **ExtraNonce** acts like a rough **uptime counter** that can indicate how long a Bitcoin client has been running.
- If we see a series of blocks with **consecutive or gradually increasing ExtraNonce values**, we can reasonably infer that they came from the **same miner**.
- If we see a block with **ExtraNonce = 0**, it likely came from a **freshly started client**.

By the way, this behavior was discovered by **Sergio Demian Lerner** in 2013, who had the genius idea to look at the ExtraNonce data, which he used to develop the famous **Patoshi Pattern Theory**. His research led him to estimate that the so-called **Patoshi miner** — likely Satoshi — mined somewhere between **700,000 and 1 million bitcoins**.

Regardless of whether you agree with his conclusion, two things are **undeniable**:

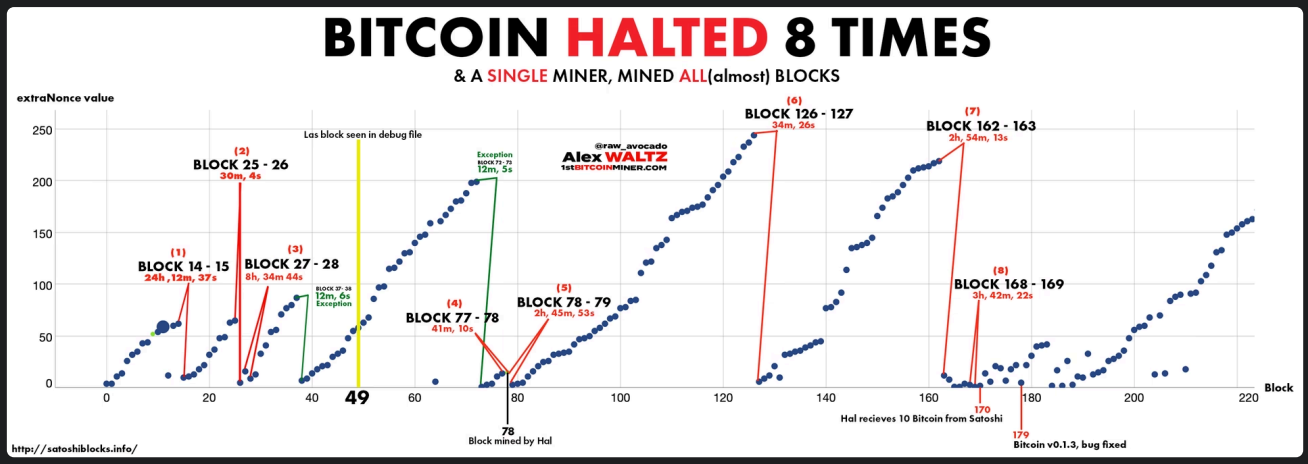
1. What is written in the **code** (how the ExtraNonce was incremented).
2. What is written on the **blockchain** (the ExtraNonce published in each coinbase transaction).

ExtraNonce + Long Block Delays

The good news is that even if you disagree with **Sergio's conclusions** — perhaps due to concerns that the data is too noisy — this doesn't pose a problem for **our investigation**, because:

- We're dealing with the **very first days of Bitcoin's existence**, and there was **very little interest** shown on the Cryptography Mailing List at the time. That means we're looking at a **very small number of participants**.
- We have additional evidence from **Hal's** `debug.log` **file**, which shows that around **Block 49**, there were **only two other nodes present.** It's hard to imagine that

hundreds of participants suddenly rushed in all of a sudden — especially given the extremely long time delays between blocks.



http://satoshiblocks.info/

In the chart above, we have **blocks** on the **X-axis** and **ExtraNonce values** on the **Y-axis**.

The chart goes up to around **Block 170**, because that's roughly when the following key events occurred:

- Satoshi sent Hal the **10 Bitcoins**
- Hal made the famous **"Running Bitcoin"** tweet
- Satoshi released **Bitcoin v0.1.3** — the first version that ran **without issues**

We can see **clusters of navy blue dots forming visible patterns**, where the **ExtraNonce of consecutive blocks increases steadily**.

This allows us to **reasonably infer** that each distinct grouping of blue dots corresponds to a **single miner**. The longer the ExtraNonce pattern, the **stronger** the assumption.

While ExtraNonce incrementation is not entirely random, it's still **chaotic and unpredictable**, so when we observe **consecutive values**, we can assign a **high degree of confidence** that those blocks came from the **same mining entity**.

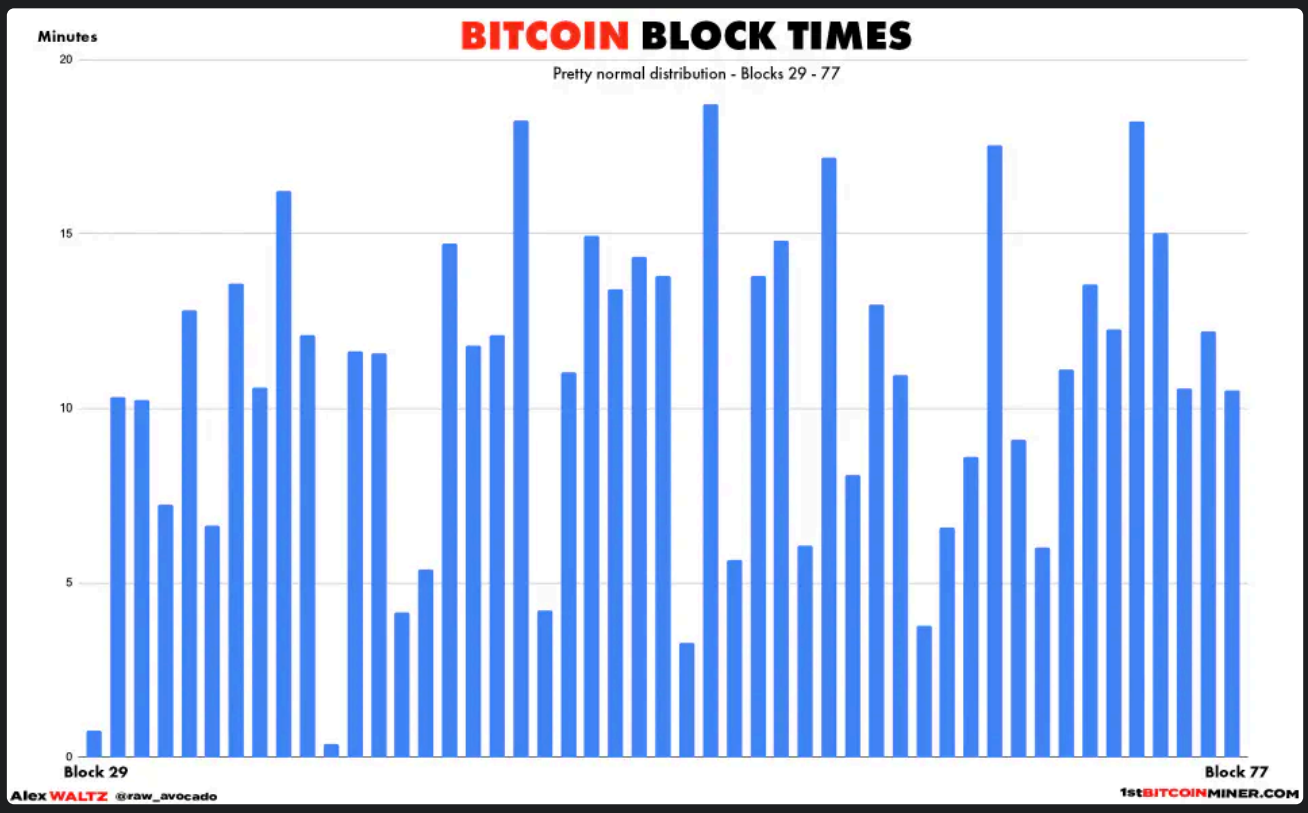
Another thing we can observe is that **each time the ExtraNonce resets**, there's a **large time gap between blocks**. Since we know the ExtraNonce counter resets when a node restarts (or shuts down), this is a **very strong indicator** that most of the blocks were **mined by one entity**— and when this entity was offline, no one else was mining blocks.

> *Remember, the difficulty at this time was very low. During this period, if a decent computer had been online, it would have been fairly easy to find a block in 10 minutes — let alone in a few hours.*

In addition to this, we know from Hal's `debug.log` file that around Block 49, there were only two other nodes present: one using a **clearnet IP** (most likely Satoshi), and the other behind **Tor**.

Block 49 is part of the run from **Block 38** to **Block 72**, and one of the two exceptions where the extraNonce resets and we have a normal (something close to 10 minutes) time gap. The extraNonce reset happens from **Block 72** to Block **73**.

In fact, if we examine the time intervals between blocks from **Block 29** to **Block 77**, the average interval is 10.7 minutes—what we would expect if someone were consistently present and mining.



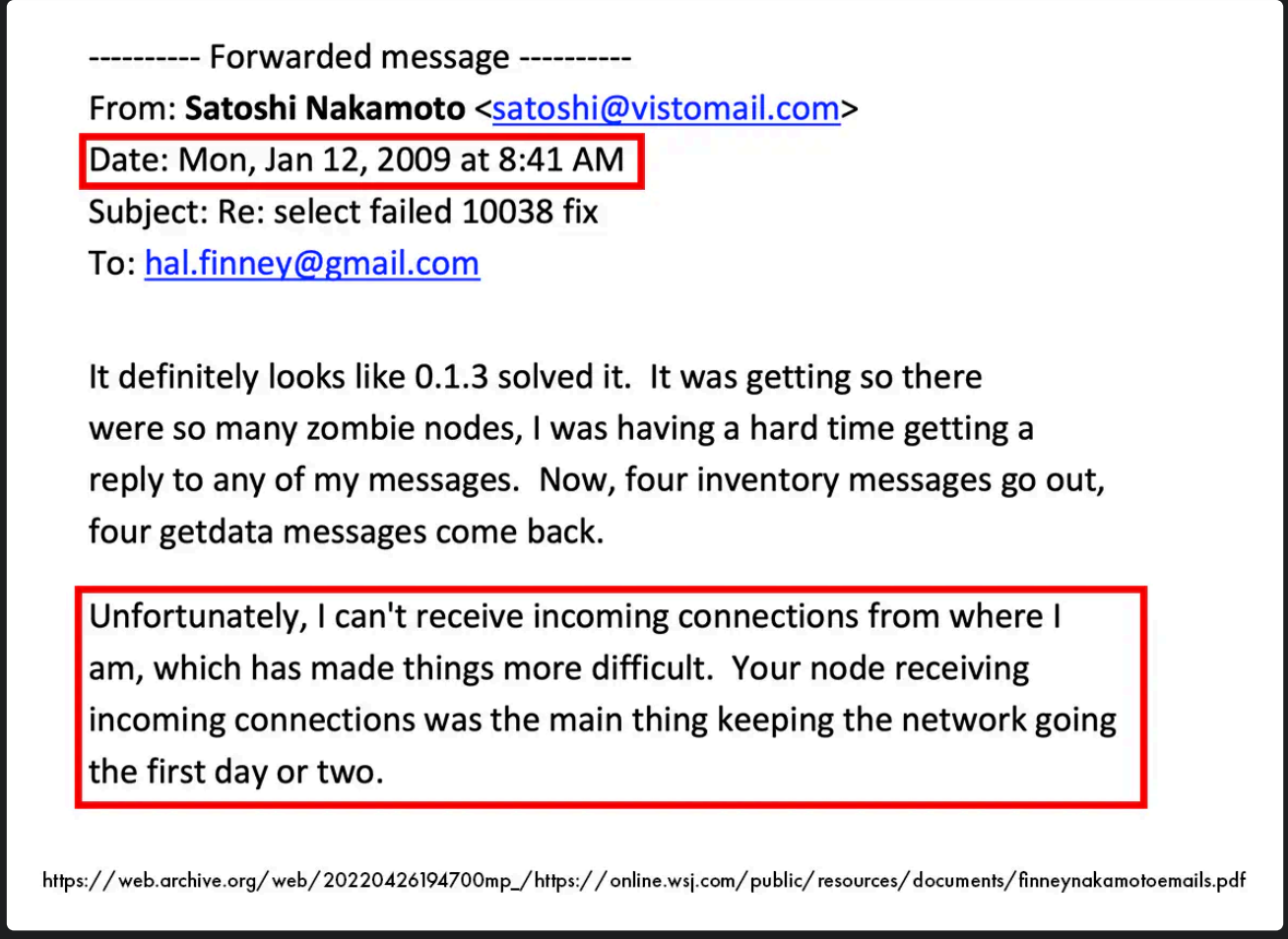
Within this range(29 to 77), we also find **both exceptions**(with green on the main chart) where an **extraNonce reset** occurs w**ithout any apparent network halt**, one after the other.

In other words, the only time the **network operates without any halts** is during the period when we know for certain that both **Satoshi** and the **Tor node** were present.

All of these factors lead me to believe that the ***Tor node was also Satoshi***.

What I suspect was happening here is that Satoshi was operating both nodes — the Tor node and the clearnet one — and that during this run, he was actively present at his machines, likely incorporating feedback from Hal while working on the code. However, whenever those longer gaps occurred, it appears he went offline for some reason.

This email from `Mon, Jan 12, 2009 at 8:41 AM (PST)` → `Monday, 12 January 2009 16:41:00 UTC` (*one day after Hal received Bitcoin v0.1.3, the first stable version*) confirms both that Satoshi may have been traveling — or otherwise lacked access to his main machine — and that he was using Tor during this time (from Wall Street Journal emails).



---------- 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.

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.

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

Remember, Tor nodes cannot accept incoming connections.

It's also interesting to note that Satoshi credited Hal with essentially keeping the network alive, despite the issues it was experiencing at the time.

> *To be **extra clear**: Everything I'm presenting here is **educated speculation** and reasoned interpretation based on the available evidence — but it's **not 100% proof**.*

> When I say there's a **high probability** of certain events or conclusions, that does **not** mean they are guaranteed. **Freak events** can and do happen — they're just **statistically less likely**.

I absolutely stand by everything I've said here; I just want to make it clear which parts of this investigation are speculative.

What If Dustin Trammell Was the Tor Node?

This speculation can be ruled out quite easily.

On `Jan 13 18:40:28 2009`, Dustin shared his IP address with Satoshi so that Satoshi could send him some coins — specifically to `24.28.79.95` .

It's highly unlikely that Dustin was using Tor at the time, and then suddenly switched to a clearnet 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-signa
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.
```

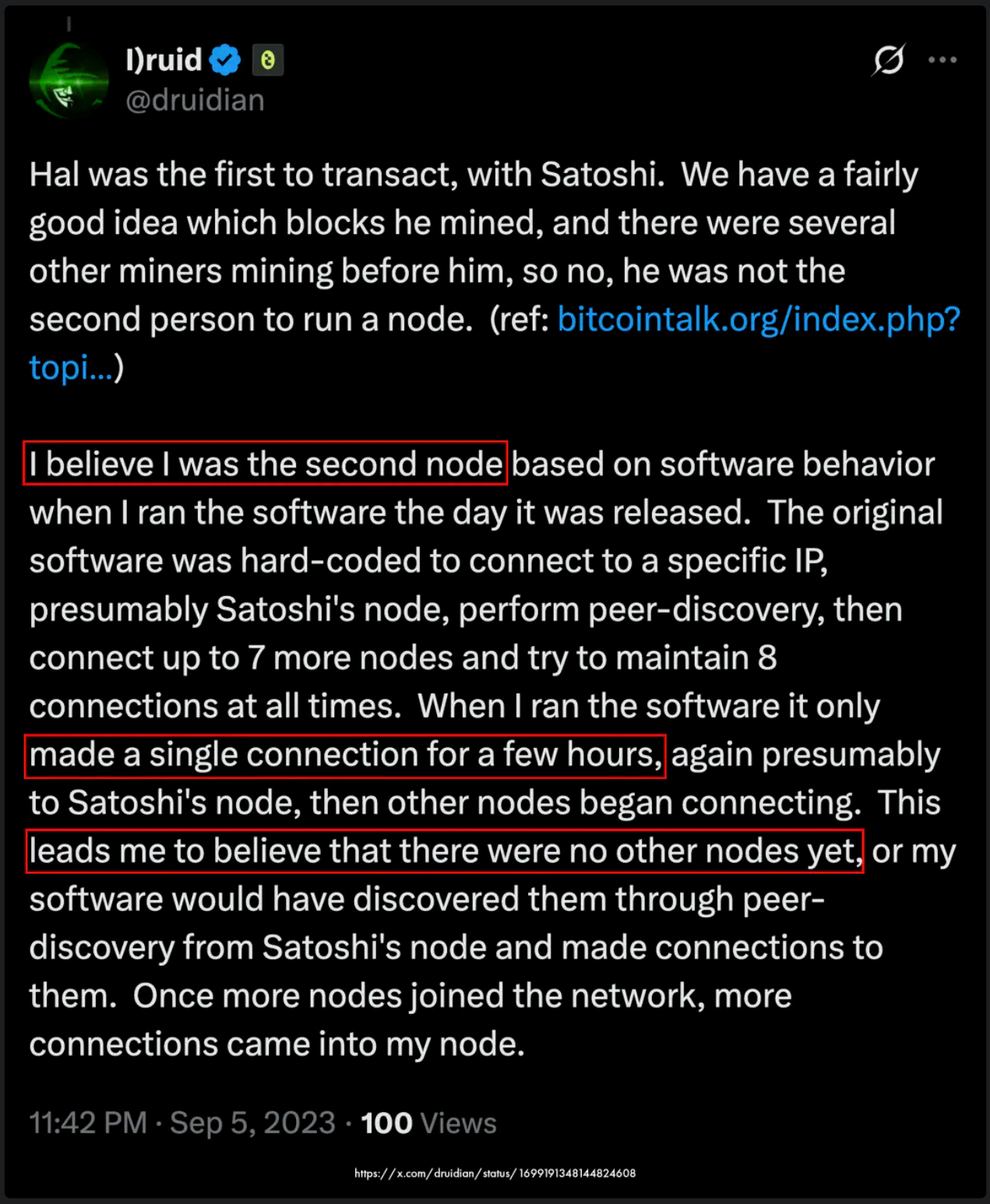
https://blog.dustintrammell.com/i-am-not-satoshi
https://koi-reindeer-77pb.squarespace.com/s/Satoshi_Nakamoto.zip

As mentioned earlier, the early versions of Bitcoin allowed users to **send Bitcoins directly to an IP address**. A user would share their IP, your node would connect to theirs using that address, request a **public key**, and then send the coins to that key.

Even though **Bitcoin addresses** were supported, many early transactions used **bare public keys**. That's why Dustin shared his IP address with Satoshi in that email.

At this point, we can move on to the last pieces of evidence, two tweets made by Dustin Trammell:

1. In 2023



https://x.com/druidian/status/1699191348144824608

2. In 2021

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

It's interesting to see that Dustin reached the **same conclusion** as we did: That **Hal was NOT the second node** to join the network (with Satoshi being the first), and that **there were other miners before Hal** — which aligns perfectly with our findings.

Dustin suspects that he was **the second node** to join the Bitcoin network, before Hal.

He clearly states that **his node only made one connection**. But was this because there were no other nodes online? Or due to connection issues?

What Dustin describes in the tweet makes a lot of sense.

Even though **Hal first tried Bitcoin around Block 49**, he only managed to get it working much later. So when Dustin ran his client, it's possible that **only Satoshi's** node was online and visible.

But what about the **Tor node**?

Well, a Tor node **cannot accept incoming connections**, so the only node Dustin could have connected to would have been Satoshi's.

However, this still leaves one open question:

> Why didn't either Satoshi's clearnet node or the Tor node connect to Dustin's node?

With the evidence we currently have, we can say with **100% certainty that Dustin controls the private key** to the address that mined **Block 309**.

But can we find evidence that places him before this block?

We may never know with absolute certainty if he d**id mine the two unconfirmed blocks** he referenced, but since **everything else he's shared aligns well** with our independent

analysis, we'll give Dustin the benefit of the doubt.

Dustin doesn't mention a specific timestamp for those unconfirmed blocks, only the date: *January 11th*.

So, for reference, let's add both the **first and last blocks** of that day into our table: **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

▶ **Clickable Table**

Even if Dustin joined the network as early as **Block 76**, that would still place him **after Hal**, who — as we've seen from the **private emails**, the **debug.log file**, and the **SourceForge mailing list post** — was already active ***just* before Block 49**.

So based on all the evidence we've gathered, it seems that **Hal did run Bitcoin before Dustin**.

The title asks **'Who Was the 1st Bitcoin Miner?'** — and given the level of scrutiny we've applied so far in our analysis, it only makes sense to keep splitting hairs.

Yes — **provably**, Hal still beats Dustin: Hal mined **Block 78**, while Dustin's first confirmed block is **Block 309**.

What I find fascinating though is this:

> If Dustin had mined his first block on January 11th, he *would* have been the first miner after Satoshi, beating Hal by two blocks... but we wouldn't be able to prove it.

It's also worth mentioning that in his appearance on the **Stephan Livera Podcast** (Episode 314), Dustin says that he downloaded the **Bitcoin Whitepaper** shortly after its release, was *eagerly* waiting for the software to be published, and ran the Bitcoin client very shortly after it was released.

However **he did not realised that the mining function was turned off by default**.

Satoshi probably made this decision intentionally: If people ran the software and saw it consuming **a lot of CPU**, they might have panicked and shut it down.

https://youtu.be/rWdUOB_NgOo?si=6cYooCF9m4QeOIQl&t=454

This small default setting explains a lot:

- Why **Satoshi was the only miner** in the very beginning
- Why others (like Hal and Dustin) ran the client but didn't mine
- Why, if there were any other **early participants**, they wouldn't have left any traces

This matches perfectly with our earlier **ExtraNonce analysis** — even if others were present, they **weren't mining**.

Early Bitcoin Satoshi-Client Peer Discovery

For the sake of accuracy, I want to clarify that the hardcoded IP address Dustin mentioned in his tweet was not Satoshi's IP, but rather the fallback IP for the Freenode IRC server, as

we can see 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/

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

> *The earliest versions of Bitcoin source code I could find (https://satoshi.nakamotoinstitute.org/code/) are Bitcoin v0.1.1 and Bitcoin v0.1.3. The hash for v0.1.3 match those in the RSS feed from SourceForge (archived on web.archive.org), and neither v0.1.1 nor v0.1.3 contains the fallback IP* `216.155.130.130` *in* `irc.cpp` *.*

> *The screenshot with the green background is from SourceForge. The earliest accessible version available there is v0.1.5, which is also the earliest version I could find that contains the fallback IRC IP.*

This detail doesn't invalidate any of the other points Dustin made, and it's an easy thing to mix up.

So what Is the Grand Conclusion?

So in this article, we dethroned Hal Finney 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 Tor node was also Satoshi Nakamoto.

We found out some never-known facts about Bitcoin's inception, which after all these years is quite something:

- Hal Finney missed Bitcoin's launch
- Hal Finney joined the Bitcoin network around Block 49
- There were 2 nodes online when he joined — both were Satoshi Nakamoto
- The Bitcoin network halted for 24h and 8h in the first 30 blocks

- In total, Bitcoin halted 8 times in the first 170 blocks

But more importantly, we got a very intimate view of 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 or miner.

What matters is that there were some people at this very early and fragile starting point of Bitcoin who 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 looking for the next breakthrough, and one day, **out of nowhere**, an anonymous guy drops one of the biggest inventions/discoveries of the century, 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 it 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, gentlemen. 🤜

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

So if you take anything from this very long article, I hope it is this: **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**.

*P.S. I hope this also puts to rest all the theories that Bitcoin was started by three-letter agencies, aliens, AI, aliens **with** AI, Elon Musk, etc. It looks an awful lot like a guy who wrote some code, put it on the internet, and made all the chaotic mistakes that come with it.*

If you found this article valuable, please consider **making a donation**.

It took about **3.5 months to research and write** the article, plus **another month** to put together the website, clean up the formatting, and create a scrappable data section to make it easier for people to re-use my work.

*All of my content **is free**, and **I always go the extra mile** to keep things thorough, sourced, and easy to navigate.*

- **LN**: `sappybeggar14@walletofsatoshi.com`
- **On-chain**: `bc1q5kaj2fyps8sqhdmf99kzzzvz45qyu7zzhjzh2r`
- **Dirty-fiat**: `buymeacoffee.com/alexwaltz`

I would like to thank the following people, who have contributed directly or indirectly to this research. Without my interactions with them(or their work), this article would not exist in its current form.