Satoshi - Sirius emails 2009-2011

This is the correspondence between myself (Martti Malmi, AKA Sirius) and Satoshi Nakamoto, the creator of Bitcoin. I did not feel comfortable sharing private correspondence earlier, but decided to do so for an important trial in the UK in 2024 where I was a witness. Also, a long time has passed now since the emails were sent. The archive is incomplete and contains only emails from my address @cc.hut.fi. My university email addresses changed to @aalto.fi in early 2011, and I don't have backups of those emails. There are some passwords and a street address mentioned in the emails, but those are no longer valid or relevant.

Follow me on Nostr or Twitter

Font size:

Email #1
Date: Sat, 02 May 2009 18:06:58 +0100
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin
To: Martti Malmi <sirius-m@users.sourceforge.net>

```
Thanks for starting that topic on ASC, your understanding of bitcoin is
spot on.  Some of their responses were rather Neanderthal, although I
guess they're so used to being anti-fiat-money that anything short of
gold isn't good enough.  They concede that something is flammable, but
argue that it'll never burn because there'll never be a spark.  Once
it's backed with cash, that might change, but I'd probably better
refrain from mentioning that in public anymore until we're closer to
ready to start.  I think we'll get flooded with newbies and we need to
get ready first.

What we need most right now is website writing.  My writing is not that
great, I'm a much better coder.  Maybe you could create the website on
sourceforge, which is currently blank.  If you can write a FAQ, I can
give you a compilation of my replies to questions in e-mail and forums
for facts and details and ideas.

Codewise, there's not much that's easy right now.  One thing that's
needed is an interface for server side scripting languages such as Java,
Python, PHP, ASP, etc.  Bitcoin would be running on the web server, and
server side script could call it to do transactions.  It's Windows, so I
guess OLE/COM is the interface.

One easy thing that really helps is to run a node that can accept
incoming connections (forward port 8333 on your firewall) to make sure
that new users who try it out have someone to connect to.  If they run
it and get no connections, they'll probably just give up.

Satoshi


Martti Malmi wrote:
> Message body follows:
>
> Hello,
>
> I'm Trickstern from the anti-state.com forum, and I would
> like to help with Bitcoin, if there's something I can do.
>
```

> I have a good touch on Java and C languages from school
> courses (I'm studying CS), but not so very much development
> experience yet. I think I could learn the C++ tricks quite
> easily on that basis. I could also do testing or
> documentation.
>
> Best regards,
> Martti Malmi
>
> --
> This message has been sent to you, a registered SourceForge.net user,
> by another site user, through the SourceForge.net site. This message
> has been delivered to your SourceForge.net mail alias. You may reply
> to this message using the "Reply" feature of your email client, or
> using the messaging facility of SourceForge.net at:
> https://sourceforge.net/sendmessage.php?touser=2495503
>

Email #2

Date: Sun, 03 May 2009 08:08:36 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

All right, I can do the website and the FAQ. I'll start writing the
FAQ now with the questions that I can think of.

I have a feature suggestion for the program: a UI tool for creating
password protected private keys and saving them into a custom
location. Backups of the key will be needed to be safe from losing the
control of your coins, and for using the coins on more than one
computers. Password protection would be needed to make using your
money more difficult for someone who happens to find your key file.

Maybe a bug/feature tracker could be set up at the Sourceforge project page?

I'm running a bitcoin node always when my PC is powered on, which
means about 24/7. Bitcoin is a great project, and it's really cool to
participate!

-Martti Malmi

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> Thanks for starting that topic on ASC, your understanding of bitcoin is
> spot on. Some of their responses were rather Neanderthal, although I
> guess they're so used to being anti-fiat-money that anything short of
> gold isn't good enough. They concede that something is flammable, but
> argue that it'll never burn because there'll never be a spark. Once
> it's backed with cash, that might change, but I'd probably better
> refrain from mentioning that in public anymore until we're closer to
> ready to start. I think we'll get flooded with newbies and we need to
> get ready first.
>
> What we need most right now is website writing. My writing is not that
> great, I'm a much better coder. Maybe you could create the website on
> sourceforge, which is currently blank. If you can write a FAQ, I can
> give you a compilation of my replies to questions in e-mail and forums
> for facts and details and ideas.
>

> Codewise, there's not much that's easy right now. One thing that's
> needed is an interface for server side scripting languages such as
> Java, Python, PHP, ASP, etc. Bitcoin would be running on the web
> server, and server side script could call it to do transactions. It's
> Windows, so I guess OLE/COM is the interface.
>
> One easy thing that really helps is to run a node that can accept
> incoming connections (forward port 8333 on your firewall) to make sure
> that new users who try it out have someone to connect to. If they run
> it and get no connections, they'll probably just give up.
>
> Satoshi
>
>
> Martti Malmi wrote:
>> Message body follows:
>>
>> Hello,
>>
>> I'm Trickstern from the anti-state.com forum, and I would like to
>> help with Bitcoin, if there's something I can do.
>>
>> I have a good touch on Java and C languages from school courses
>> (I'm studying CS), but not so very much development experience yet.
>> I think I could learn the C++ tricks quite easily on that basis. I
>> could also do testing or documentation.
>>
>> Best regards,
>> Martti Malmi
>>
>> --
>> This message has been sent to you, a registered SourceForge.net user,
>> by another site user, through the SourceForge.net site. This message
>> has been delivered to your SourceForge.net mail alias. You may reply
>> to this message using the "Reply" feature of your email client, or
>> using the messaging facility of SourceForge.net at:
>> https://sourceforge.net/sendmessage.php?touser=2495503
>>

Email #3

Date: Sun, 03 May 2009 23:32:26 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> All right, I can do the website and the FAQ. I'll start writing the FAQ
> now with the questions that I can think of.

That would be great! I added you (dmp1ce) as a dev to the sourceforge
project and gave you access to edit the web space and everything.

> I have a feature suggestion for the program: a UI tool for creating
> password protected private keys and saving them into a custom location.
> Backups of the key will be needed to be safe from losing the control of
> your coins, and for using the coins on more than one computers. Password
> protection would be needed to make using your money more difficult for
> someone who happens to find your key file.

Definitely. This will be an absolutely essential feature once things get going, making it so you can lock your wealth up with strong encryption and back it up more securely than any physical safe. So far I've been putting it off in favour of other features because it's not crucial yet until bitcoins start to have value.

I plan to work on the escrow feature next, which is needed to make actual trades for physical stuff safer and before backing the currency with fiat money can begin.

> I'm running a bitcoin node always when my PC is powered on, which means
> about 24/7. Bitcoin is a great project, and it's really cool to
> participate!

Thanks! Right now there are a lot of people on the network who can't receive incoming connections, so every node that can really helps. Having more helps keep down the "(not accepted)" issue for now until I reduce the chances of that happening in v0.1.6.

I guess one answer for the FAQ should be how to set up your firewall to forward port 8333 so you can receive incoming connections. The question could be something like "what if I have 0 connections" and that could be the answer that it might be because the nodes you can connect with is limited if you don't set that up.

Here's a compilation of questions I've answered in forums and e-mail that should help you see what questions are frequently asked and some answers I've used. It's not intended to use all or most of the material here, just pick and choose. This is just a dump of everything I've answered.

Some issues that we don't have easy answers for are best not to bring up. Casual users seems content to assume that the system works as stated (which it does), and getting into the design details just opens a can of worms that can't be answered without a deep understanding of the system. The advanced questions I've received have mostly been unique per person and best answered individually.

**** QUESTION AND ANSWER DUMP ****

Any questions used for the FAQ should probably be rephrased.

questions:

 > The bottom of the UI shows:
 >
 > Generating   4 connections   4024 blocks   164 transactions
 >
 > I understand "generating"; I assume I am connected to 4 other nodes; and
 > I know I have recorded 164 transactions (including failed generation
 > attempts). I'm not clear what the "blocks" figure describes. It's much
 > smaller than the total of all the blocks shown against all my
transactions.
 >

It's the total number of blocks in the block chain, meaning the network's block chain, which everyone has a copy of. Every Bitcoin node displays the same number and it goes up about every 10 minutes whenever someone generates a block. When you haven't had it running for a while, once you're connected it spins up rapidly as it downloads what was

generated while you were gone to catch up. I'm not sure exactly how to describe it (that would fit on the status bar in 1 word, maybe 2 words max), any ideas?

The blocks number in the status column next to your transactions is the number of blocks that have come after that transaction. Your transaction is essentially "in" that many blocks.

Satoshi

> My best guess - it
> is the length of the global chain, and the rapid advance at the start
> is as the software downloads and verifies the preceding blocks in the
> chain as being valid.

Right. I'm trying to think of more clear wording for that, maybe "%d network blocks" or "%d block chain".

> I'm having an unusual run of (block not-accepted) failures, and thought I'd let you know in
> case this was of any significance.

What rate of not-accepted did you see? I didn't see anything unusual on my end. If you had more than, say, 4 in a row, that would be abnormal and probably a loss of network communication. If it's scattered and less than 25%, just random bad luck. It's normal and harmless to randomly get some per cent of not-accepted, and of course randomness can sometimes bunch up and look like a pattern.

The idea of an option to View/Hide unaccepted blocks is a good one, as well as View/Hide all generated blocks so you can more easily see incoming transactions. Seeing the unaccepted blocks is just annoying and frustrating. Everyone faces the same rate of unaccepted, it's just a part of the process. It would probably be best to default to hide unaccepted blocks, so as not to show giving and taking away something that never was, and not show new generated blocks at all until they have at least one confirmation. It would only mean finding out you have a generated block 15 minutes later than normal, and then you still have 119 blocks to go before it matures anyway. This is on the to-do list for v0.1.6.

Satoshi

[note: I have some improvements in 0.1.6 to reduce this problem somewhat, and it'll also improve when the network is larger]

> For some reason your transfer to me shows up as "From: unknown" even
> though I added you to my address book.
>
> I have a "Generated (not accepted)" line in my transaction list, it
> seems like an attempt to generate a coin went wrong somehow. Not sure

> what happened here - presumably my node successfully solved a block
> but then I went offline before it was sent to the network?

Transactions sent to a bitcoin address will always say "from: unknown".
  The transaction only tells who it's to. Sending by bitcoin address
has a number of problems, but it's so nice having the fallback option to
be able to send to anyone whether they're online or not. There are a
number of ideas to try to improve things later. For now, if things work
out like the real world where the vast majority of transactions are with
merchants, they'll pretty much always make sure to set up to receive by
IP. The P2P file sharing networks seem fairly successful at getting a
large percentage of their users to set up their firewalls to forward a port.

I badly wanted to find some way to include a comment with indirect
transfers, but there just wasn't a way to do it. Bitcoin uses EC-DSA, which
was essential for making the block chain compact enough to be practical with
today's technology because its signatures are an order of magnitude smaller
than RSA. But EC-DSA can't encrypt messages like RSA, it can only be used
to verify signatures.

The "Generated (not accepted)" normally happens if two nodes find a
block at close to the same time, one of them will not be accepted. It's
normal and unavoidable. I plan in v0.1.6 to hide those, since they're
just confusing and annoying and there's no reason for users to have to
see them. While the network is still small like it is now, if you can't
receive incoming connections you're at more of a disadvantage because
you can't receive block announcements as directly.

> ...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?

Right, the credit field stays 0.00 until it matures, then it'll be
50.00. BTW, you can doubleclick on a line for details.

> ...understand correctly, there is only one (or maybe a few) global
> chain[s] into which all transactions are hashed. If there is only one
> chain recording "the story of the economy" so to speak, how does this
> scale? In an imaginary planet-wide deployment there would be millions
> of even billions of transactions per hour being hashed into the chain...

> ...I found the section on incentives hard to follow. In particular, I'm
> not clear on what triggers the transition from minting new coins as a
> reason to run a node, to charging transaction fees (isn't the point of
> BitCoin largely to zero transaction costs anyway?). Presumably there's
> some human in charge of the system...

> ...How did you decide on the inflation schedule for v1? Where did 21
> million coins come from? What denominations are these coins? You
> mention a way to combine and split value but I'm not clear on how this
> works. For instance are bitcoins always denominated by an integer or
> can you have fractional bitcoins?...

> ...it's rare that I encounter truly
> revolutionary ideas. The last time I was this excited about a new
> monetary scheme was when I discovered Ripple. If you have any thoughts
> on Ripple, I'd also love to hear them.

There is only one global chain.

The existing Visa credit card network processes about 15 million Internet purchases per day worldwide. Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost. It never really hits a scale ceiling. If you're interested, I can go over the ways it would cope with extreme size.

By Moore's Law, we can expect hardware speed to be 10 times faster in 5 years and 100 times faster in 10. Even if Bitcoin grows at crazy adoption rates, I think computer speeds will stay ahead of the number of transactions.

I don't anticipate that fees will be needed anytime soon, but if it becomes too burdensome to run a node, it is possible to run a node that only processes transactions that include a transaction fee. The owner of the node would decide the minimum fee they'll accept. Right now, such a node would get nothing, because nobody includes a fee, but if enough nodes did that, then users would get faster acceptance if they include a fee, or slower if they don't. The fee the market would settle on should be minimal. If a node requires a higher fee, that node would be passing up all transactions with lower fees. It could do more volume and probably make more money by processing as many paying transactions as it can. The transition is not controlled by some human in charge of the system though, just individuals reacting on their own to market forces.

A key aspect of Bitcoin is that the security of the network grows as the size of the network and the amount of value that needs to be protected grows. The down side is that it's vulnerable at the beginning when it's small, although the value that could be stolen should always be smaller than the amount of effort required to steal it. If someone has other motives to prove a point, they'll just be proving a point I already concede.

My choice for the number of coins and distribution schedule was an educated guess. It was a difficult choice, because once the network is going it's locked in and we're stuck with it. I wanted to pick something that would make prices similar to existing currencies, but without knowing the future, that's very hard. I ended up picking something in the middle. If Bitcoin remains a small niche, it'll be worth less per unit than existing currencies. If you imagine it being used for some fraction of world commerce, then there's only going to be 21 million coins for the whole world, so it would be worth much more per unit. Values are 64-bit integers with 8 decimal places, so 1 coin is represented internally as 100000000. There's plenty of granularity if typical prices become small. For example, if 0.001 is worth 1 Euro, then it might be easier to change where the decimal point is displayed, so if you had 1 Bitcoin it's now displayed as 1000, and 0.001 is displayed as 1.

Ripple is interesting in that it's the only other system that does something with trust besides concentrate it into a central server.

Satoshi

> If we assume that 0.1% is a good risk rate, then z=5 thus
> any transaction must wait a bit less than an hour before being
> solidified in the chain. As micropayments for things like web content
> or virtual goods are by definition something that requires low

> overhead, waiting an hour seems like quite a significant hurdle.

For the actual risk, multiply the 0.1% by the probability that the buyer is an attacker with a huge network of computers.

For micropayments, you can safely accept the payment immediately. The size of the payment is too small for the effort to steal it. Micropayments are almost always for intellectual property, where there's no physical loss to the merchant. Anyone trying to steal a micropayment would probably not be a paying customer anyway, and if they want to steal intellectual property they can use the file sharing networks.

Currently, businesses accept a certain chargeoff rate. I believe the risk with 1 or even 0 confirming blocks will be much less than the rate of chargebacks on verified credit card transactions.

The usual scam against a merchant that doesn't wait for confirming blocks would be to send a payment to a merchant, then quickly try to propagate a double-spend to the network before the merchant's copy. What the merchant can do is broadcast his transaction and then monitor the network for any double-spend copies. The thief would not be able to broadcast during the monitoring period or else the merchant's node would receive a copy. The merchant would only have to monitor for a minute or two until most of the network nodes have his version and it's too late for the thief's version to catch up and reach many nodes. With just a minute or two delay, the chance of getting away without paying could be made much too low to scam. A thief usually needs a high probability of getting an item for free to make it worthwhile. Using a lot of CPU power to do the brute force attack discussed in the paper in addition to the above scam would not increase the thief's chances very much.

Anything that grants access to something, like something that takes a while to download, access to a website, web hosting, a subscription or service, can be cancelled a few minutes later if the transaction is rejected.

> How is the required difficulty of each block communicated through the
> network and agreed upon?

It's not communicated. The formula is hardcoded in the program and every node does the same calculation to know what difficulty is required for the next block. If someone diverged from the formula, their block would not be accepted by the majority.

> Is the code free/open source or just open source?

It's free open source. It's the MIT license, which just requires some disclaimer text be kept with the source code, other than that you can do just about anything you want with it. The source is included in the main download.

Satoshi

> Is there a way to be told of new versions? Does the app auto update
> itself? Some kind of mailing list would be excellent.

The list is:
bitcoin-list@lists.sourceforge.net
Subscribe/unsubscribe page:
http://lists.sourceforge.net/mailman/listinfo/bitcoin-list
Archives:
http://sourceforge.net/mailarchive/forum.php?forum_name=bitcoin-list

I'll always announce new versions there. Automatic update, or at least notification of new versions, is definitely on the list.

[this inflation discussion was before the transaction fee mechanism and fixed plan of 21 million coins was posted, so it may not be as applicable anymore]

> Since they can be created for free (or at the cost
> of computer power people have anyway for other reasons),
> monetizing them means simply giving away money.

You're still thinking as if the difficulty level will be so easy that people will be able to generate all the bitcoins they want.

Imagine you have to run your computer 24/7 for a month to generate 1 cent. After a year, you could generate 12 cents. That's not going to make it so people can just generate all the bitcoin they want for spending.

The value of bitcoins would be relative to the electricity consumed to produce them. All modern CPUs save power when they're idle. If you run a computational task 24/7, not letting it idle, it uses significantly more power, and you'll notice it generates more heat. The extra wattage consumed goes straight to your power bill, and the value of the bitcoins you produce would be something less than that.

> Why would they, when they make money by generating
> new ones

No, they can't make money that way. It would cost them more in electricity than they'd be selling the bitcoins for.

Historically, people have taken up scarce commodities as money, if necessary taking up whatever is at hand, such as shells or stones. Each has a kernel of usefulness that helped bootstrap the process, but the monetary value ends up being much more than the functional value alone.
  Most of the value comes from the value that others place in it. Gold, for instance, is pretty, non-corrosive and easily malleable, but most of its value is clearly not from that. Brass is shiny and similar in colour. The vast majority of gold sits unused in vaults, owned by governments that could care less about its prettiness.

Until now, no scarce commodity that can be traded over a communications channel without a trusted third party has been available. If there is a desire to take up a form of money that can be traded over the Internet without a TTP, then now that is possible.

Satoshi

> As more capable
> computer hardware comes out, the natural supply per user
> doubles at every cycle of Moore's law.

Actually, that is handled. There's a moving average that compensates for the total effort being expended so that the total production is a constant. As computers get more powerful, the difficulty increases to compensate.

> I do not recall any economic history of a commodity subject
> to natural inflation ever being used as money

There's gold for one. The supply of gold increases by about 2%-3% per year. Any fiat currency typically averages more inflation than that.

> Won't there be massive inflation as computers get faster and are able to solve the proof-of-work problem faster?

The difficulty is controlled by a moving average that compensates for the total effort being expended to keep the total production constant. As computers get more powerful, the difficulty increases to compensate.

> If someone double spends, then the transaction record
> can be unblinded revealing the identity of the cheater?

Identities are not used, and there's no reliance on recourse. It's all prevention.

> ...You're saying
> there's no effort to identify and exclude nodes that don't
> cooperate? I suspect this will lead to trouble and possible DOS
> attacks.

There is no reliance on identifying anyone. As you've said, it's futile and can be trivially defeated with sock puppets.

The credential that establishes someone as real is the ability to supply CPU power.

> But in the absence of identity, there's no downside to them

> if spends become invalid, if they've already received the
> goods they double-spent for (access to website, download,
> whatever). The merchants are left holding the bag with
> "invalid" coins, unless they wait that magical "few blocks"
> (and how can they know how many?) before treating the spender
> as having paid.
>
> The consumers won't do this if they spend their coin and it takes
> an hour to clear before they can do what they spent their coin on.
> The merchants won't do it if there's no way to charge back a
> customer when they find the that their coin is invalid because
> the customer has doublespent.

This is a version 2 problem that I believe can be solved fairly satisfactorily for most applications.

The race is to spread your transaction on the network first. Think 6 degrees of freedom -- it spreads exponentially. It would only take something like 2 minutes for a transaction to spread widely enough that a competitor starting late would have little chance of grabbing very many nodes before the first one is overtaking the whole network. During those 2 minutes, the merchant's nodes can be watching for a double-spent transaction. The double-spender would not be able to blast his alternate transaction out to the world without the merchant getting it, so he has to wait before starting.

If the real transaction reaches 90% and the double-spent tx reaches 10%, the double-spender only gets a 10% chance of not paying, and 90% chance his money gets spent. For almost any type of goods, that's not going to be worth it for the scammer.

Information based goods like access to website or downloads are non-fencible. Nobody is going to be able to make a living off stealing access to websites or downloads. They can go to the file sharing networks to steal that. Most instant-access products aren't going to have a huge incentive to steal.

If a merchant actually has a problem with theft, they can make the customer wait 2 minutes, or wait for something in e-mail, which many already do. If they really want to optimize, and it's a large download, they could cancel the download in the middle if the transaction comes back double-spent. If it's website access, typically it wouldn't be a big deal to let the customer have access for 5 minutes and then cut off access if it's rejected. Many such sites have a free trial anyway.

Satoshi

[in response to a question about scale]

100,000 block generating nodes is a good ballpark large-scale size to think about. Propagating a transaction across the whole network twice would consume a total of US$ 0.02 of bandwidth at today's prices. In practice, many would be burning off excess allocated bandwidth or unlimited plans with one of the cheaper backbones. There could be millions of SPV clients. They only matter in how many transactions they generate. If they pay 1 or 2 cents transaction fees, they pay for themselves. I've coded it so you can pay any optional amount of transaction fees you want. When the

incentive subsidy eventually tapers off, it may be necessary to put a market-determined transaction fee on your transactions to make sure nodes process them promptly.

To think about what a really huge transaction load would look like, I look at the existing credit card network. I found some more estimates about how many transactions are online purchases. It's about 15 million tx per day for the entire e-commerce load of the Internet worldwide. At 1KB per transaction, that would be 15GB of bandwidth for each block generating node per day, or about two DVD movies worth. Seems do-able even with today's technology.

Important to remember, even if Bitcoin caught on at dot-com rates of growth, it would still take years to become any substantial fraction of all transactions. I believe hardware has already recently become strong enough to handle large scale, but if there's any doubt about that, bandwidth speeds, prices, disk space and computing power will be much greater by the time it's needed.

Satoshi

> One other question I had... What prevents the single node with the most
> CPU power from generating and retaining the majority of the BitCoins?
> If every node is working independently of all others, if one is
> significantly more powerful than the others, isn't it probable that this
> node will reach the proper conclusion before other nodes? An
> underpowered node may get lucky once in a while, but if they are at a
> significant horsepower advantage I would expect the majority of BitCoins
> to be generated by the most powerful node.

It's not like a race where if one car is twice as fast, it'll always win. It's an SHA-256 that takes less than a microsecond, and each guess has an independent chance of success. Each computer's chance of finding a hash collision is linearly proportional to it's CPU power. A computer that's half as fast would get half as many coins.

[question about what to backup]

The files are in "%appdata%\Bitcoin", that's the directory to backup.

%appdata% is per-user access privilege. Most new programs like Firefox store their settings files there, despite the headwind of Microsoft changing the directory name with every Windows release and being full of spaces and so long it runs off the screen.

[question about what to backup]

The directory is "%appdata%\Bitcoin"
It has spaces in it so you need the quotes

cd "%appdata%\bitcoin"

On XP it would typically be:
C:\Documents and Settings\[username]\Application Data\Bitcoin

Backup that whole directory. All data files are in that
directory. There are no temporary files.

[question about what to backup]

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

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

> > You know, I think there were a lot more people interested in the 90's,
> > but after more than a decade of failed Trusted Third Party based
systems
> > (Digicash, etc), they see it as a lost cause. I hope they can make the
> > distinction that this is the first time I know of that we're trying a
> > non-trust-based system.
>
> Yea, that was the primary feature that caught my eye. The real trick
> will be to get people to actually value the Bitcoins so that they become
> currency.

Hal sort of alluded to the possibility that it could be seen as a
long-odds investment. I would be surprised if 10 years from now
we're not using electronic currency in some way, now that we know
a way to do it that won't inevitably get dumbed down when the
trusted third party gets cold feet.

Once it gets bootstrapped, there are so many applications if you
could effortlessly pay a few cents to a website as easily as dropping
coins in a vending machine.

[this next bit turned out to be very controversial. there is extreme
prejudice against spam solutions, especially proof-of-work.]

It can already be used for pay-to-send e-mail. The send dialog is
resizeable and you can enter as long of a message as you like.
It's sent directly when it connects. The recipient doubleclicks
on the transaction to see the full message. If someone famous is
getting more e-mail than they can read, but would still like to
have a way for fans to contact them, they could set up Bitcoin and
give out the IP address on their website. "Send X bitcoins to my

priority hotline at this IP and I'll read the message personally."

Subscription sites that need some extra proof-of-work for their free trial so it doesn't cannibalize subscriptions could charge bitcoins for the trial.

[again, I don't know why I'm including this, as it's best to stay away from claims about spam. people automatically react violently against any suggestion of a spam solution.]

> Spammer botnets could burn through pay-per-send email filters
> trivially (as usual, the costs would fall on people other than the
> botnet herders & spammers).

Then you could earn a nice profit by setting up pay-per-send e-mail addresses and collecting all the spam money. You could sell it back to spammers who don't have big enough botnets to generate their own, helping bootstrap the currency's value. As more people catch on, they'll set up more and more phony addresses to harvest it. By the time the book "How I got rich exploiting spammers and you can too" is coming out, there'll be too many fake addresses and the spammers will have to give up.

> > * Spammer botnets could burn through pay-per-send email filters
> > trivially
> If POW tokens do become useful, and especially if they become money,
> machines will no longer sit idle. Users will expect their computers to
> be earning them money (assuming the reward is greater than the cost to
> operate). A computer whose earnings are being stolen by a botnet will
> be more noticeable to its owner than is the case today, hence we might
> expect that in that world, users will work harder to maintain their
> computers and clean them of botnet infestations.

One more factor that would mitigate spam if POW tokens have value: there would be a profit motive for people to set up massive quantities of fake e-mail accounts to harvest POW tokens from spam. They'd essentially be reverse-spamming the spammers with automated mailboxes that collect their POW and don't read the message. The ratio of fake mailboxes to real people could become too high for spam to be cost effective.

The process has the potential to establish the POW token's value in the first place, since spammers that don't have a botnet could buy tokens from harvesters. While the buying back would temporarily let more spam through, it would only hasten the self-defeating cycle leading to too many harvesters exploiting the spammers.

Interestingly, one of the e-gold systems already has a form of spam called "dusting". Spammers send a tiny amount of gold dust in order to put a spam message in the transaction's comment field.
If the system let users configure the minimum payment they're willing to receive, or at least the minimum that can have a message with it, users could set how much they're willing to get paid to receive spam.

> The last thing we need is to deploy a system designed to burn all
> available cycles, consuming electricity and generating carbon dioxide,
> all over the Internet, in order to produce small amounts of bitbux to
> get emails or spams through.
>
> Can't we just convert actual money in a bank account into bitbux --
> cheaply and without a carbon tax? Please?

Ironic if we end up having to choose between economic liberty and conservation.

Unfortunately, proof of work is the only solution I've found to make p2p e-cash work without a trusted third party. Even if I wasn't using it secondarily as a way to allocate the initial distribution of currency, PoW is fundamental to coordinating the network and preventing double-spending.

If it did grow to consume significant energy, I think it would still be less wasteful than the labour and resource intensive conventional banking activity it would replace. The cost would be an order of magnitude less than the billions in banking fees that pay for all those brick and mortar buildings, skyscrapers and junk mail credit card offers.

Satoshi

> BTW I don't remember if we talked about this, but the other day some
> people were mentioning secure timestamping. You want to be able to
> prove that a certain document existed at a certain time in the past.
> Seems to me that bitcoin's stack of blocks would be perfect for this.

Indeed, Bitcoin is a distributed secure timestamp server for transactions. A few lines of code could create a transaction with an extra hash in it of anything that needs to be timestamped. I should add a command to timestamp a file that way.

From a thread on p2presearch which starts with my rant about trust being the root weakness of all conventional financial systems. http://listcultures.org/pipermail/p2presearch_listcultures.org/2009-February/thread.html

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and

transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible.

A generation ago, multi-user time-sharing computer systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what.

It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.

One of the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at http://www.bitcoin.org/bitcoin.pdf

The result is a distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending.

Satoshi Nakamoto
http://www.bitcoin.org

Martien van Steenbergen Martien at AardRock.COM
Thu Feb 12 08:40:53 CET 2009

Very interesting. Is this akin to David Chaum's anonymous digital money? His concept makes sure money is anonymous unless it is compromised, i.e. the same money spent more than once. As soon as it's compromised, the ‘counterfeiter’ is immediately publicly exposed.

Also, in bitcoin, is there a limited supply of money (that must be managed)? Or is money created exaclty at the moment of transaction?

Succes en plezier,

Martien.

Martien van Steenbergen wrote:
> Very interesting. Is this akin to David Chaum's anonymous digital money?
> His concept makes sure money is anonymous unless it is compromised, i.e.
> the same money spent more than once. As soon as it's compromised, the
> ‘counterfeiter’ is immediately publicly exposed.

It's similar in that it uses digital signatures for coins, but different in the approach to privacy and preventing double-spending. The recipient of a Bitcoin payment is able to check whether it is the first spend or not, and second-spends are not accepted. There isn't an off-line mode where double-spenders are caught and shamed after the fact, because that would require participants to have identities.

To protect privacy, key pairs are used only once, with a new one for every transaction. The owner of a coin is just whoever has its private key.

Of course, the biggest difference is the lack of a central server. That was the Achilles heel of Chaumian systems; when the central company shut down, so did the currency.

> Also, in bitcoin, is there a limited supply of money (that must be
> managed)? Or is money created exaclty at the moment of transaction?

There is a limited supply of money. Circulation will be 21,000,000 coins. Transactions only transfer ownership.

Thank you for your questions,

Satoshi

Martien van Steenbergen wrote:
> Reminds me of:
>
> * AardRock » Wizard Rabbit Treasurer
> <http://wiki.aardrock.com/Wizard_Rabbit_Treasurer>; and
> * AardRock » Pekunio <http://wiki.aardrock.com/Pekunio>

Indeed, it is much like Pekunio in the concept of spraying redundant copies of every transaction to a number of peers on the network, but the implementation is not a reputation network like Wizard Rabbit Treasurer.
In fact, Bitcoin does not use reputation at all. It sees the network as just a big crowd and doesn't much care who it talks to or who tells it something, as long as at least one of them relays the information being broadcast around the network. It doesn't care because there's no way to lie to it. Either you tell it crypto proof of something, or it ignores you.

> Are you familiar with Ripple?

As trust systems go, Ripple is unique in spreading trust around rather than concentrating it.

[I've been asked at least 4 other times "have you heard of Ripple?"]

Michel Bauwens wrote:
 > how operational is your project? how soon do you think people will be
 > able to use it in real life?

It's fully operational and the network is growing. If you try the
software, e-mail me your Bitcoin address and I'll send you a few coins.

We just need to spread the word and keep getting more people interested.

Here's a link to the original introduction of the paper on the
Cryptography mailing list. (Inflation issues were superseded by changes
I made later to support transaction fees and the limited circulation
plan. This link is a moving target, this archive page is just a certain
number of days back and the discussion will keep scrolling off to the
next page.)
http://www.mail-archive.com/cryptography@metzdowd.com/mail3.html

A little follow up when the software was released.
http://www.mail-archive.com/cryptography@metzdowd.com/mail2.html

My description of how Bitcoin solves the Byzantine Generals' problem:
http://www.bitcoin.org/byzantine.html

Email #4

Date: Mon, 04 May 2009 03:17:22 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> That would be great! I added you (dmp1ce) as a dev to the sourceforge
> project and gave you access to edit the web space and everything.

Oh, that's not me but another guy who wanted to help. I've seen him on
the Freedomain Radio forum. My name is Martti Malmi and my Sourceforge
account is sirius-m. No problem!

Thanks for your answered questions, I'll add them to the faq. Here's
what I've done so far:

**** Bitcoin FAQ ****

General Questions

1 What is bitcoin?

Bitcoin is a peer-to-peer network based anonymous digital
currency. Peer-to-peer (P2P) means that there is no central
authority to issue new money or to keep track of the
transactions. Instead, those tasks are managed collectively by
the nodes of the network. Anonymity means that the real world
identity of the parties of a transaction can be kept hidden from
the public or even from the parties themselves.

2 How does bitcoin work?

Bitcoin utilizes public/private key cryptography. When a coin is transfered from user A to user B, A adds B's public key to the coin and signs it with his own private key. Now B owns the coin and can transfer it further. To prevent A from transfering the already used coin to another user C, a public list of all the previous transactions is collectively maintained by the network of bitcoin nodes, and before each transaction the coin's unusedness will be checked.

For details, see chapter Advanced Questions.

3 What is bitcoin's value backed by?

Bitcoin is valued for the things it can be exchanged to, just like all the traditional paper currencies are.

When the first user publicly announces that he will make a pizza for anyone who gives him a hundred bitcoins, then he can use bitcoins as payment to some extent - as much as people want pizza and trust his announcement. A pizza-eating hairdresser who trusts him as a friend might then announce that she starts accepting bitcoins as payment for fancy haircuts, and the value of the bitcoin would be higher - now you could buy pizzas and haircuts with them. When bitcoins have become accepted widely enough, he could retire from his pizza business and still be able to use his bitcoin-savings.

4 How are new bitcoins created?

New coins are generated by a network node each time it finds the solution to a certain calculational problem. In the first 4 years of the bitcoin network, amount X of coins will be created. The amount is halved each 4 years, so it will be X/2 after 4 years, X/4 after 8 years and so on. Thus the total number of coins will approach 2X.

5 Is bitcoin safe?

Yes, as long as you make backups of your coin keys, protect them with strong passwords and keep keyloggers away from your computer. If you lose your key or if some unknown attacker manages to unlock it, there's no way to get your coins back. If you have a large amount of coins, it is recommended to distribute them under several keys. You propably wouldn't either keep all your dollars or euros as paper in a single wallet and leave it unguarded.

6 Why should I use bitcoin?

- Transfer money easily through the internet, without having to trust third parties.
- Third parties can't prevent or control your transactions.
- Be safe from the unfair monetary policies of the monopolistic central banks and the other risks of centralized power over a money supply. The limited inflation of the bitcoin system's money supply is distributed evenly (by CPU power) throughout the network, not monopolized to a banking elite.
- Bitcoin's value is likely to increase as the growth of the bitcoin economy exceeds the inflation rate - consider bitcoin

an investment and start running a node today!

7 Where can I get bitcoins?

Find a bitcoin owner and sell her something - MMORPG equipement,
IT support, lawn mowing, dollars or whatever you can trade with
her. You can also generate new bitcoins for yourself by running a
bitcoin network node.

Email #5

Date: Mon, 04 May 2009 16:51:00 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

Oh crap, I got your sourceforge usernames mixed up, sorry about that. I
clicked on the wrong e-mail when I was looking for your username. You
now have access.

Your FAQ looks good so far!

You can create whatever you want on bitcoin.sourceforge.net. Something
to get new users up to speed on what Bitcoin is and how to use it and
why, and clean and professional looking would help make it look well
established. The site at bitcoin.org was designed in a more
professorial style when I was presenting the design paper on the
Cryptography list, but we're moving on from that phase.

You should probably change the part about "distribute them under several
keys". When the paper says that it means for the software to do it, and
it does. For privacy reasons, the software already uses a different key
for every transaction, so every piece of money in your wallet is already
on a different key. The exception is when using a bitcoin address,
everything sent to the same bitcoin address is on the same key, which is
a privacy risk if you're trying to be anonymous. The EC-DSA key size is
very strong (sized for the future), we don't practically have to worry
about a key getting broken, but if we did there's the advantage that
someone expending the massive computing resources would only break one
single transaction's worth of money, not someone's whole account. The
details about how to backup your wallet files is in the Q&A dump and
also it's explained in readme.txt and definitely belongs in the FAQ.

Oh I see, you're trying to address byronm's concern on freedomainradio.
I see what you mean about the password feature being useful to address
that argument. Banks let anyone who has your name and account number
drain your account, and you're not going to get it back from Nigeria.
If someone installs a keylogger on your computer, they could just as
easily get your bank password and transfer money out of your account.
Once we password encrypt the wallet, we'll be able to make a clearer
case that we're much more secure than banks. We use strong encryption,
while banks still let anyone who has your account info draw money from
your account.

mmalmi@cc.hut.fi wrote:
> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>
>> That would be great! I added you (dmp1ce) as a dev to the sourceforge
>> project and gave you access to edit the web space and everything.
>
> Oh, that's not me but another guy who wanted to help. I've seen him on

> the Freedomain Radio forum. My name is Martti Malmi and my Sourceforge
> account is sirius-m. No problem!
>
> Thanks for your answered questions, I'll add them to the faq. Here's
> what I've done so far:
>
> **** Bitcoin FAQ ****
>
> General Questions
>
> 1 What is bitcoin?
>
> Bitcoin is a peer-to-peer network based anonymous digital
> currency. Peer-to-peer (P2P) means that there is no central
> authority to issue new money or to keep track of the
> transactions. Instead, those tasks are managed collectively by
> the nodes of the network. Anonymity means that the real world
> identity of the parties of a transaction can be kept hidden from
> the public or even from the parties themselves.
>
> 2 How does bitcoin work?
>
> Bitcoin utilizes public/private key cryptography. When a coin is
> transfered from user A to user B, A adds B's public key to the
> coin and signs it with his own private key. Now B owns the coin
> and can transfer it further. To prevent A from transfering the
> already used coin to another user C, a public list of all the
> previous transactions is collectively maintained by the network
> of bitcoin nodes, and before each transaction the coin's
> unusedness will be checked.
>
> For details, see chapter Advanced Questions.
>
> 3 What is bitcoin's value backed by?
>
> Bitcoin is valued for the things it can be exchanged to, just
> like all the traditional paper currencies are.
>
> When the first user publicly announces that he will make a pizza
> for anyone who gives him a hundred bitcoins, then he can use
> bitcoins as payment to some extent - as much as people want pizza
> and trust his announcement. A pizza-eating hairdresser who trusts
> him as a friend might then announce that she starts accepting
> bitcoins as payment for fancy haircuts, and the value of the
> bitcoin would be higher - now you could buy pizzas and haircuts
> with them. When bitcoins have become accepted widely enough, he
> could retire from his pizza business and still be able to use his
> bitcoin-savings.
>
> 4 How are new bitcoins created?
>
> New coins are generated by a network node each time it finds the
> solution to a certain calculational problem. In the first 4 years
> of the bitcoin network, amount X of coins will be created. The
> amount is halved each 4 years, so it will be X/2 after 4 years,
> X/4 after 8 years and so on. Thus the total number of coins will
> approach 2X.
>
> 5 Is bitcoin safe?
>
> Yes, as long as you make backups of your coin keys, protect them
> with strong passwords and keep keyloggers away from your
> computer. If you lose your key or if some unknown attacker
> manages to unlock it, there's no way to get your coins back. If

> you have a large amount of coins, it is recommended to distribute
> them under several keys. You propably wouldn't either keep all
> your dollars or euros as paper in a single wallet and leave it
> unguarded.
>
> 6 Why should I use bitcoin?
>
> • Transfer money easily through the internet, without having to
>   trust third parties.
>
> • Third parties can't prevent or control your transactions.
>
> • Be safe from the unfair monetary policies of the monopolistic
>   central banks and the other risks of centralized power over a
>   money supply. The limited inflation of the bitcoin system's
>   money supply is distributed evenly (by CPU power) throughout
>   the network, not monopolized to a banking elite.
>
> • Bitcoin's value is likely to increase as the growth of the
>   bitcoin economy exceeds the inflation rate - consider bitcoin
>   an investment and start running a node today!
>
> 7 Where can I get bitcoins?
>
> Find a bitcoin owner and sell her something - MMORPG equipement,
> IT support, lawn mowing, dollars or whatever you can trade with
> her. You can also generate new bitcoins for yourself by running a
> bitcoin network node.
>

Email #6

Date: Tue, 05 May 2009 04:00:00 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> You can create whatever you want on bitcoin.sourceforge.net. Something
> to get new users up to speed on what Bitcoin is and how to use it and
> why, and clean and professional looking would help make it look well
> established. The site at bitcoin.org was designed in a more
> professorial style when I was presenting the design paper on the
> Cryptography list, but we're moving on from that phase.

Ok. Could you set the project MySQL database passwords so that I can
set up a CMS on the site? I was thinking about WordPress, as it seems
simple and well maintained. I need a password for the read/write
account and one database (or the database admin pass to create it
myself). This can be done somewhere in the project admin pages, I think.

> You should probably change the part about "distribute them under
> several keys". When the paper says that it means for the software to
> do it, and it does. For privacy reasons, the software already uses a
> different key for every transaction, so every piece of money in your
> wallet is already on a different key. The exception is when using a
> bitcoin address, everything sent to the same bitcoin address is on the
> same key, which is a privacy risk if you're trying to be anonymous.
> The EC-DSA key size is very strong (sized for the future), we don't
> practically have to worry about a key getting broken, but if we did
> there's the advantage that someone expending the massive computing

> resources would only break one single transaction's worth of money, not
> someone's whole account. The details about how to backup your wallet
> files is in the Q&A dump and also it's explained in readme.txt and
> definitely belongs in the FAQ.

Ok, that's good to know.

> Oh I see, you're trying to address byronm's concern on freedomainradio.
> I see what you mean about the password feature being useful to address
> that argument. Banks let anyone who has your name and account number
> drain your account, and you're not going to get it back from Nigeria.
> If someone installs a keylogger on your computer, they could just as
> easily get your bank password and transfer money out of your account.
> Once we password encrypt the wallet, we'll be able to make a clearer
> case that we're much more secure than banks. We use strong encryption,
> while banks still let anyone who has your account info draw money from
> your account.

Well, I guess that's true after all.

Email #7

Date: Tue, 05 May 2009 04:07:41 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting mmalmi@cc.hut.fi:

>> Oh I see, you're trying to address byronm's concern on freedomainradio.
>> I see what you mean about the password feature being useful to address
>> that argument. Banks let anyone who has your name and account number
>> drain your account, and you're not going to get it back from Nigeria.
>> If someone installs a keylogger on your computer, they could just as
>> easily get your bank password and transfer money out of your account.
>> Once we password encrypt the wallet, we'll be able to make a clearer
>> case that we're much more secure than banks. We use strong encryption,
>> while banks still let anyone who has your account info draw money from
>> your account.
>
> Well, I guess that's true after all.

...the difference being, though, that not everyone can easily transfer
their regular bank money into an uncontrollable location. In bitcoin
anyone can do it.

Email #8

Date: Tue, 05 May 2009 18:39:44 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
>> You can create whatever you want on bitcoin.sourceforge.net. Something
>> to get new users up to speed on what Bitcoin is and how to use it and
>> why, and clean and professional looking would help make it look well
>> established. The site at bitcoin.org was designed in a more
>> professorial style when I was presenting the design paper on the
>> Cryptography list, but we're moving on from that phase.

>
> Ok. Could you set the project MySQL database passwords so that I can set
> up a CMS on the site? I was thinking about WordPress, as it seems simple
> and well maintained. I need a password for the read/write account and
> one database (or the database admin pass to create it myself). This can
> be done somewhere in the project admin pages, I think.

They have Wordpress built in, you might not need to set up any database stuff manually. I enabled the Wordpress feature and added you as an admin, account sirius-m, e-mail sirius-m@users.sourceforge.net. I'm not sure how it works out the password for access, maybe it's just based on being logged in to sourceforge.

https://apps.sourceforge.net/wordpress/bitcoin/wp-admin/

They also have support for MediaWiki if you want it.

In case you still need it, here's the accounts and passwords for mysql.

Access this project's databases over the Internet
https://apps.sourceforge.net/admin/Bitcoin
Documentation: Guide to MySQL Database Services
http://p.sf.net/sourceforge/mysql
Hostname: mysql-b   (exactly as shown, with no domain suffix)
Database name prefix: b244765_ -- i.e. "CREATE DATABASE b244765_myapp"
as your ADMIN user.
RO user: b244765ro (SELECT)
RW user: b244765rw (SELECT, INSERT, DELETE, UPDATE)
ADMIN user: b244765admin (has RW account privileges, and CREATE, DROP,
ALTER, INDEX, LOCK TABLES)
web-access URL: https://mysql-b.sourceforge.net/
passwords:
b244765ro   EaG3nHLL
b244765rw   sNKgyt4W
b244765admin   Mz589ZKf

> ...the difference being, though, that not everyone can easily
> transfer their regular bank money into an uncontrollable location. In
> bitcoin anyone can do it.

That's true.

We shouldn't try to use security against identity theft as a selling point, since it leads into these counter arguments. The current banking model is already tested and the actual loss percentage is known. Even if ours is probably better, it's an unknown, so people can imagine anything. The uncertainty about what the average loss percentage will be is greater than the likely loss percentage itself.

Email #9

Date: Wed, 06 May 2009 08:31:41 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> They have Wordpress built in, you might not need to set up any database
> stuff manually.
>

> They also have support for MediaWiki if you want it.

The built-in Wordpress comes with ads, and new plugins and themes need
to be installed by the Sourceforge staff, so I installed Wordpress at
http://bitcoin.sourceforge.net/. The admin page is at .../wp-admin/,
with admin/Wubreches3eS as login. If there's something to add or
change, feel free to.

The current layout is just a quickly applied free theme, but I'll see
if I can do something more visual myself.

The MediaWiki might be quite useful for maintaining the FAQ, which
could be retrieved from there to the main site somehow. The wiki says
I need to be an editor or admin to create a new page, which is funny,
because
https://apps.sourceforge.net/mediawiki/bitcoin/index.php?
title=Special:ListGroupRights says that users can create
pages.

Email #10

Date: Wed, 06 May 2009 08:41:43 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Lainaus mmalmi@cc.hut.fi:

> The current layout is just a quickly applied free theme, but I'll see
> if I can do something more visual myself.

And of course I'll continue improving the contents also.

Email #11

Date: Thu, 07 May 2009 03:35:50 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

It's already an improvement, and like you say, there must be better
themes to choose from.

It would be good to make the download link go directly to the download area:
https://sourceforge.net/project/showfiles.php?group_id=244765

I haven't found any way to gain admin control over the mediawiki
feature. It thinks I'm a different S_nakamoto from the one that has
admin access:

```
     User list
     * S nakamoto  <- it thinks I'm this one
     * S nakamoto (admin, editor)
     * Sirius-m
```

I tried deleting and re-enabling the feature, no help. Oh well.

mmalmi@cc.hut.fi wrote:
> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>
>> They have Wordpress built in, you might not need to set up any database

```
>> stuff manually.
>>
>> They also have support for MediaWiki if you want it.
>
> The built-in Wordpress comes with ads, and new plugins and themes need
> to be installed by the Sourceforge staff, so I installed Wordpress at
> http://bitcoin.sourceforge.net/. The admin page is at .../wp-admin/,
> with admin/Wubreches3eS as login. If there's something to add or change,
> feel free to.
>
> The current layout is just a quickly applied free theme, but I'll see if
> I can do something more visual myself.
>
> The MediaWiki might be quite useful for maintaining the FAQ, which could
> be retrieved from there to the main site somehow. The wiki says I need
> to be an editor or admin to create a new page, which is funny, because
> https://apps.sourceforge.net/mediawiki/bitcoin/index.php?
title=Special:ListGroupRights
> says that users can create pages.
```

Email #12

Date: Fri, 22 May 2009 11:05:56 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
Quoting Satoshi Nakamoto <satoshin@gmx.com>:

> I haven't found any way to gain admin control over the mediawiki
> feature.  It thinks I'm a different S_nakamoto from the one that has
> admin access:
>     User list
>     * S nakamoto  <- it thinks I'm this one
>     * S nakamoto (admin, editor)
>     * Sirius-m
>
> I tried deleting and re-enabling the feature, no help.  Oh well.

I think this has something to do with the underscore character in your
username; MediaWiki handles them as spaces. I could ask SF Support
about this.
```

Email #13

Date: Fri, 22 May 2009 11:08:43 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
Quoting mmalmi@cc.hut.fi:

> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>
>> I haven't found any way to gain admin control over the mediawiki
>> feature.  It thinks I'm a different S_nakamoto from the one that has
>> admin access:
>>    User list
```

```
>>    * S nakamoto  <- it thinks I'm this one
>>    * S nakamoto (admin, editor)
>>    * Sirius-m
>>
>> I tried deleting and re-enabling the feature, no help.  Oh well.
>
> I think this has something to do with the underscore character in your
> username; MediaWiki handles them as spaces. I could ask SF Support
> about this.

Or could you control the MediaWiki with your account nakamoto2?
```

Email #14

Date: Fri, 22 May 2009 11:12:41 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
Quoting mmalmi@cc.hut.fi:

> Quoting mmalmi@cc.hut.fi:
>
>> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>>
>>> I haven't found any way to gain admin control over the mediawiki
>>> feature.  It thinks I'm a different S_nakamoto from the one that has
>>> admin access:
>>>   User list
>>>   * S nakamoto  <- it thinks I'm this one
>>>   * S nakamoto (admin, editor)
>>>   * Sirius-m
>>>
>>> I tried deleting and re-enabling the feature, no help.  Oh well.
>>
>> I think this has something to do with the underscore character in your
>> username; MediaWiki handles them as spaces. I could ask SF Support
>> about this.
>
> Or could you control the MediaWiki with your account nakamoto2?

Oh, sorry for spamming with emails, but the problem is indeed with the
underscore character:
http://apps.sourceforge.net/trac/sourceforge/ticket/300
```

Email #15

Date: Sun, 24 May 2009 23:03:38 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

```
You're right, that was it.  I went in and granted us access using the
alternate account.

I like your idea of at least moving the FAQ into the wiki.  I've seen
other projects that use the wiki for the FAQ or even the whole site.  If
you can figure out how to make it so regular users can edit things, then
anyone who wants to can help.
```

```
mmalmi@cc.hut.fi wrote:
> Quoting mmalmi@cc.hut.fi:
>
>> Quoting mmalmi@cc.hut.fi:
>>
>>> Quoting Satoshi Nakamoto <satoshin@gmx.com>:
>>>
>>>> I haven't found any way to gain admin control over the mediawiki
>>>> feature.  It thinks I'm a different S_nakamoto from the one that has
>>>> admin access:
>>>>   User list
>>>>   * S nakamoto  <- it thinks I'm this one
>>>>   * S nakamoto (admin, editor)
>>>>   * Sirius-m
>>>>
>>>> I tried deleting and re-enabling the feature, no help.  Oh well.
>>>
>>> I think this has something to do with the underscore character in your
>>> username; MediaWiki handles them as spaces. I could ask SF Support
>>> about this.
>>
>> Or could you control the MediaWiki with your account nakamoto2?
>
> Oh, sorry for spamming with emails, but the problem is indeed with the
> underscore character:
> http://apps.sourceforge.net/trac/sourceforge/ticket/300
>
```

Email #16

Date: Sun, 07 Jun 2009 08:34:29 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
> I like your idea of at least moving the FAQ into the wiki.  I've seen
> other projects that use the wiki for the FAQ or even the whole site.
> If you can figure out how to make it so regular users can edit things,
> then anyone who wants to can help.

The user group privileges seemingly can't be changed without changing
the wiki source files, which can only be done by the SF admins as a
hosted app is concerned. The hosted apps are also otherwise quite
inflexible: you can only login with a SF account, you can't change
themes by yourself and of course there's the ad-bar above the pages.

I think that replacing the current Wordpress installation at
bitcoin.sourceforge.net with TikiWiki could be a great solution.
TikiWiki supports CMS features, forums, wikis, bug trackers, and many
other features also if needed. Perhaps the best looking example of a
TikiWiki installation is at http://support.mozilla.com/.

I'll take backup of the current site and see if TikiWiki can be
installed at SF. If it doesn't work, I'll see how wiki/forum features
can be integrated with Wordpress or think of something else.
```

Email #17

Date: Tue, 09 Jun 2009 09:55:26 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
I couldn't get TikiWiki to work, so I installed Bitweaver, which is a
lightweight TikiWiki derivative. Its functionality looks good for the
purpose and it's easy to customize.

The admin account password is Wubreches3eS again. New users can
register to the site and write to the wiki and the forums. Next I'm
going to look into how custom menus and custom layouts are made.
```

Email #18

Date: Thu, 11 Jun 2009 07:34:20 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
Now that the project web is up and running, do you think that setting
up a custom VHOST for the bitcoin.org domain would be a good idea?
Instructions:
http://apps.sourceforge.net/trac/sourceforge/wiki/Custom%20VHOSTs

Also, could you please send me a link to a SF Logo for statistics, as
instructed at:
http://apps.sourceforge.net/trac/sourceforge/wiki/Use%20of%20sflogo%20for
%20statistics%20tracking
```

Email #19

Date: Thu, 11 Jun 2009 22:24:25 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

```
The site layout is looking nicer.  More impressive looking.

There are a lot of things you can say on the sourceforge site that I
can't say on my own site.  Even so, I'm uncomfortable with explicitly
saying "consider it an investment".  That's a dangerous thing to say and
you should delete that bullet point.  It's OK if they come to that
conclusion on their own, but we can't pitch it as that.

A few details: the FAQ says "see section 2.3", but the sections aren't
numbered.  Also, could you delete the last sentence on the FAQ "They are
planned to be hidden in v0.1.6, since they're just confusing and
annoying and there's no reason for users to have to see them." -- that's
not really something I meant to say publicly.

The links to sites to help set up 8333 port forwarding is great.
favicon is a nice touch.

Someone came up with the word "cryptocurrency"... maybe it's a word we
should use when describing Bitcoin, do you like it?

Sourceforge is so slow right now I can't even get the login page to
load.  Maybe due to the site reorg they just did.  I'll keep trying and
try to get you that logo stats thing.

mmalmi@cc.hut.fi wrote:
```

> Now that the project web is up and running, do you think that setting up
> a custom VHOST for the bitcoin.org domain would be a good idea?
> Instructions:
> http://apps.sourceforge.net/trac/sourceforge/wiki/Custom%20VHOSTs
>
> Also, could you please send me a link to a SF Logo for statistics, as
> instructed at:
> http://apps.sourceforge.net/trac/sourceforge/wiki/Use%20of%20sflogo%20for
%20statistics%20tracking
>
>

Email #20

Date: Fri, 12 Jun 2009 12:22:34 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> There are a lot of things you can say on the sourceforge site that I
> can't say on my own site. Even so, I'm uncomfortable with explicitly
> saying "consider it an investment". That's a dangerous thing to say
> and you should delete that bullet point. It's OK if they come to that
> conclusion on their own, but we can't pitch it as that.
>
> A few details: the FAQ says "see section 2.3", but the sections aren't
> numbered. Also, could you delete the last sentence on the FAQ "They
> are planned to be hidden in v0.1.6, since they're just confusing and
> annoying and there's no reason for users to have to see them." --
> that's not really something I meant to say publicly.

I made the changes. You could also register to the site or use the
admin account to make necessary changes yourself, since the pages are
located in the wiki.

> Someone came up with the word "cryptocurrency"... maybe it's a word we
> should use when describing Bitcoin, do you like it?

It sounds good. "The P2P Cryptocurrency" could be considered as the
slogan, even if it's a bit more difficult to say than "The Digital P2P
Cash". It still describes the system better and sounds more
interesting, I think.

I could notify the mailing list about the new site and invite them to
write on the forums and to the wiki.

Email #21

Date: Sun, 14 Jun 2009 21:30:58 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> I made the changes. You could also register to the site or use the admin
> account to make necessary changes yourself, since the pages are located
> in the wiki.

Thanks, I've been really busy lately.

I registered username "satoshi". Since there's no SSL login, I want to
mainly use that account with sub-admin powers and use the admin account
as little as possible. I created a "Moderators" group to give my
satoshi account as much editing control as possible without the ability
to overthrow everything.

There's something weird with the download bar on the right covering
things up, like on the new account registration it covers up the entry
fields unless you make the browser really wide, and the homepage it
covers up the screenshots. (with Firefox)

Email #22

Date: Mon, 22 Jun 2009 19:27:11 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> There's something weird with the download bar on the right covering
> things up, like on the new account registration it covers up the entry
> fields unless you make the browser really wide, and the homepage it
> covers up the screenshots. (with Firefox)

Problem fixed. I switched to a fixed width layout, which is also
easier to read as the lines are shorter.

Email #23

Date: Tue, 21 Jul 2009 03:43:34 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Hi,

I made a post on the Bitcoin developer's forum at SF about a month ago
and sent you, David and Hal a notification about it to your
users.sourceforge.net emails. A few days ago I wondered why no one had
replied, and tried if the SF mail aliases even work - and they didn't,
at least in the case of my account. So could you please forward this
message to the others?

Best regards,
sirius-m

Email #24

Date: Tue, 21 Jul 2009 04:14:43 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

I know this sounds really retarded, but I still haven't been able to get
the sourceforge login page to load, so I haven't been able to read it
either. https://sourceforge.net/account/login.php

Hal isn't currently actively involved. He helped me a lot defending the
design on the Cryptography list, and with initial testing when it was
first released. He carried this torch years ago with his Reusable Proof

Of Work (RPOW).

I'm not going to be much help right now either, pretty busy with work,
and need a break from it after 18 months development.

It would help if there was something for people to use it for. We need
an application to bootstrap it. Any ideas?

There are donors I can tap if we come up with something that needs
funding, but they want to be anonymous, which makes it hard to actually
do anything with it.

mmalmi@cc.hut.fi wrote:
> Hi,
>
> I made a post on the Bitcoin developer's forum at SF about a month ago
> and sent you, David and Hal a notification about it to your
> users.sourceforge.net emails. A few days ago I wondered why no one had
> replied, and tried if the SF mail aliases even work - and they didn't,
> at least in the case of my account. So could you please forward this
> message to the others?
>
> Best regards,
> sirius-m
>

Email #25

Date: Wed, 22 Jul 2009 13:10:02 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> I know this sounds really retarded, but I still haven't been able to
> get the sourceforge login page to load, so I haven't been able to read
> it either. https://sourceforge.net/account/login.php

That's strange, I haven't had any problems with that. Clearly the
banking establishment got scared and banned your account (and founded
www.bitcoin.com in attempt to fetch the trademark), eh. You could ask
if the SF staff at sfnet_ops@corp.sourceforge.com can help you.

> I'm not going to be much help right now either, pretty busy with work,
> and need a break from it after 18 months development.

Oh, that sounds tough. Take your time.

> It would help if there was something for people to use it for. We need
> an application to bootstrap it. Any ideas?

I've been thinking about a currency exchange service that sells and
buys bitcoins for euros and other currencies. Direct exchangeability
to an existing currency would give bitcoin the best possible initial
liquidity and thus the best adoptability for new users. Everyone
accepts payment in coins that are easily exchangeable for common
money, but not everyone accepts payment in coins that are only
guaranteed to buy a specific kind of a product.

The instructional formula for stable pricing in euros would be something like:

(The amount of euros that you're ready to trade for bc + the
euro-value of goods that other people are selling for bc) /

(Total number of bc in circulation - own bc assets).

So if there's a total of 1M bitcoins of which you own 100K, you have 1000 eur and no one else trades with bitcoin yet, you can safely offer the exchange rate of 1 eur / 900 bc, without having to devaluate even if everyone sold their coins to you. This could be guaranteed as the minimal exchange rate, but the rate could be also higher when demand is high.

Initially, when others aren't yet offering anything for bitcoins, you can increase your bitcoin assets cheaply - for the minimum price that people bother to do the transaction for. If you had all the existing coins for yourself, you could set the price to whatever you want, because you wouldn't face the risk of having to buy even a single coin with that price (not counting the new money created by others). So it's best to get as much coins as possible before backing bitcoin with all your available euros.

Profit can be gained, as usually in trading, by having a margin between the buying and selling prices. Making Bitcoin as usable as possible will make the business run better, as people do not only want to sell all their coins to you, but also want to buy them and use them as a medium of exchange.

At its simplest this exchange service could be a website where traders, who can be individual persons, can post their rates, and random users can leave trade requests. Some kind of an average rate estimate could be shown on the site. Small-scale trading by individuals would be outside legal hassle in most countries, and putting all the eggs in the same basket would be avoided.

Another idea, which could be additional to the previous one, would be an automated exchange service. The service would automatically calculate the exchange rate and perform the transactions. This would be nicer to the user: completion of the transaction request would be certain and instantaneous. Making this service might actually be quite easy if there was a command line interface to Bitcoin: just take any web application framework and use PayPal back-end integration to automatically send euros when Bitcoins are received, and vice versa. This kind of business would also work great on larger scale if you set up a company and take care of all the bureaucracy needed to practice currency exchange. (I actually have a registered company that I've used for billing of some IT work, I could use that as a base.)

This exchange business thing is something that I'd be interested in doing, and I also have the sufficient technical skills to do it. Although, before this can be done, there should be a non-alpha version of Bitcoin (and the command line interface / API).

> There are donors I can tap if we come up with something that needs
> funding, but they want to be anonymous, which makes it hard to actually
> do anything with it.

If this gets started, donors / high-risk investors would be very welcome to bring capital for the currency's backup.

So, what do you think about the idea? Note that this is not something that I'm asking you to do (unless you want to) if you're busy with other things. I can do it myself, if I get positive reviews about the plan.

Date: Wed, 29 Jul 2009 18:14:51 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
I've had quite a few errors coming up when trying to build the
third-party libraries and adding them to the Bitcoin build. Do you
happen to have a ready-to-build package that you could upload to the
CVS or somewhere else? I use mingw + msys, but I guess I could try
Visual C++ also, if it's easier that way.
```

Email #27

Date: Mon, 24 Aug 2009 06:38:13 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

```
I got it compile with MinGW + MSYS when I used wxPack instead of just
wxWidgets. Maybe wxAdditions was required. The bitcoin.exe filesize
was 52MB though, I should see how that can be fixed.

Next I'm going to implement the "minimize to tray" feature and the
option to autostart Bitcoin with Windows, so the number of nodes
online would stay higher. After that I could see if I can do a Linux
port or the command line interface needed for web app frameworks.

Drop by at #bitcoin-dev on FreeNode some time if you use IRC.

And again, thanks for the great work you've done with Bitcoin.

Quote mmalmi@cc.hut.fi:

> I've had quite a few errors coming up when trying to build the
> third-party libraries and adding them to the Bitcoin build. Do you
> happen to have a ready-to-build package that you could upload to the
> CVS or somewhere else? I use mingw + msys, but I guess I could try
> Visual C++ also, if it's easier that way.
```

Email #28

Date: Mon, 24 Aug 2009 23:00:35 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

```
That's a good point that since you know how many coins exist and how
fast new ones are created, you could set a support price based on the
amount of legacy currency you have and be sure you'll have enough to
meet all demands.  I had imagined an auction, but it would be far
simpler and more confidence inspiring to back it at a specific exchange
rate.

Offering currency to back bitcoins would attract freebie seekers, with
the benefit of attracting a lot of publicity.  At first it would mostly
be seen as a way to get free money for your computer's idle time.  Maybe
pitched like help support the future of e-commerce and get a little
```

money for your computer's spare cycles. As people cash in and actually get paid, word would spread exponentially.

It might help to keep the minimum transaction size above an amount which a typical user would be able to accumulate with one computer, so that users have to trade with each other for someone to collect enough to cash in. Aggregators would set up shop to buy bitcoins in smaller increments, which would add confidence in users ability to sell bitcoins if there are more available buyers than just you.

People would obviously be sceptical at first that the backing will hold up against an onslaught of people trying to get the free money, but as the competition raises the proof-of-work difficulty, it should become clear that bitcoins stay scarce. People will see that they can't just get all the bitcoins they want. It would establish a minimum value under bitcoins enabling them to be used for other purposes if, hopefully, other purposes are waiting for something to use.

>> It would help if there was something for people to use it for. We need
>> an application to bootstrap it. Any ideas?
>
> I've been thinking about a currency exchange service that sells and
> buys bitcoins for euros and other currencies. Direct exchangeability
> to an existing currency would give bitcoin the best possible initial
> liquidity and thus the best adoptability for new users. Everyone
> accepts payment in coins that are easily exchangeable for common
> money, but not everyone accepts payment in coins that are only
> guaranteed to buy a specific kind of a product.

That would be more powerful if there was also some narrow product market to use it for. Some virtual currencies like Tencent's Q coin have made headway with virtual goods. It would be sweet if there was some way to horn in on a market like that as the official virtual currency gets clamped down on with limitations. Not saying it can't work without something, but a ready specific transaction need that it fills would increase the certainty of success.

> At its simplest this exchange service could be a website where
> traders, who can be individual persons, can post their rates, and
> random users can leave trade requests. Some kind of an average rate
> estimate could be shown on the site. Small-scale trading by
> individuals would be outside legal hassle in most countries, and
> putting all the eggs in the same basket would be avoided.

Basically like an eBay site with user reviews to try to establish which sellers can be trusted. The escrow feature will help but not solve everything. It would be far more work to set up such a site than just to set up a single exchange site of your own, and there won't be enough users to make it go until later. I'm thinking it wouldn't make sense to make an eBay type site until later.

> Another idea, which could be additional to the previous one, would be
> an automated exchange service. The service would automatically
> calculate the exchange rate and perform the transactions. This would
> be nicer to the user: completion of the transaction request would be
> certain and instantaneous. Making this service might actually be quite
> easy if there was a command line interface to Bitcoin: just take any
> web application framework and use PayPal back-end integration to
> automatically send euros when Bitcoins are received, and vice versa.
> This kind of business would also work great on larger scale if you set
> up a company and take care of all the bureaucracy needed to practice
> currency exchange. (I actually have a registered company that I've
> used for billing of some IT work, I could use that as a base.)

Even if you had automation, you'd probably want to review orders manually before processing them anyway. It wouldn't be hard to process orders by hand, especially at first. You could always set a minimum order size to keep orders more infrequent.

> This exchange business thing is something that I'd be interested in
> doing, and I also have the sufficient technical skills to do it.
> Although, before this can be done, there should be a non-alpha version
> of Bitcoin (and the command line interface / API).
>
> If this gets started, donors / high-risk investors would be very
> welcome to bring capital for the currency's backup.
>
> So, what do you think about the idea? Note that this is not something
> that I'm asking you to do (unless you want to) if you're busy with
> other things. I can do it myself, if I get positive reviews about the
> plan.

That's great, I could probably get a donor to send currency to you which you convert to euros and pay out through methods that are convenient for users. I don't want to do an exchange business myself, but it can be done independently of me. Like you say, there is more software development to be done first, and also I'd like to keep trying for a while to think of a bootstrap application to use bitcoins for. I've had some ideas that could only be done before an exchange exists.

BTW, I tried to buy bitcoin.com before I started but there was no chance, it's owned by a professional domain speculator. It's normal for open source projects to have .org so it's not so bad.

Email #29

Date: Mon, 24 Aug 2009 23:04:25 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

Glad that worked, it's a pain that the dependencies are so big and hard to build. Some of them give little attention to the Windows build. Next time I update to the latest versions, maybe I'll lay everything out in one directory tree and bundle the whole thing up into a giant archive.

I'm not sure they had wxPack before. I'm glad they got that so everyone doesn't have to build wxWidgets themselves. OpenSSL is the harder one to build.

I reduced the EXE size by running strip.exe on it to take out the debug symbols. That's with mingw. That's the better compiler, I only used VC for debugging.

mmalmi@cc.hut.fi wrote:
> I got it compile with MinGW + MSYS when I used wxPack instead of just
> wxWidgets. Maybe wxAdditions was required. The bitcoin.exe filesize was
> 52MB though, I should see how that can be fixed.
>
> Next I'm going to implement the "minimize to tray" feature and the
> option to autostart Bitcoin with Windows, so the number of nodes online
> would stay higher. After that I could see if I can do a Linux port or
> the command line interface needed for web app frameworks.
>
> Drop by at #bitcoin-dev on FreeNode some time if you use IRC.
>

> And again, thanks for the great work you've done with Bitcoin.
>
> Quote mmalmi@cc.hut.fi:
>
>> I've had quite a few errors coming up when trying to build the
>> third-party libraries and adding them to the Bitcoin build. Do you
>> happen to have a ready-to-build package that you could upload to the
>> CVS or somewhere else? I use mingw + msys, but I guess I could try
>> Visual C++ also, if it's easier that way.
>
>
>

Email #30

Date: Fri, 28 Aug 2009 07:10:06 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

> It might help to keep the minimum transaction size above an amount
> which a typical user would be able to accumulate with one computer, so
> that users have to trade with each other for someone to collect enough
> to cash in. Aggregators would set up shop to buy bitcoins in smaller
> increments, which would add confidence in users ability to sell
> bitcoins if there are more available buyers than just you.

That might be a good idea.

> That would be more powerful if there was also some narrow product
> market to use it for. Some virtual currencies like Tencent's Q coin
> have made headway with virtual goods. It would be sweet if there was
> some way to horn in on a market like that as the official virtual
> currency gets clamped down on with limitations. Not saying it can't
> work without something, but a ready specific transaction need that it
> fills would increase the certainty of success.

Bitcoin could be promoted to the users of virtual communities like
World of Warcraft and Second Life, which both have millions of users.
It would be great if not only peer-to-peer item traders, but also
providers of some existing virtual services that already have a lot of
customers, were to adopt the currency early on.

A programming question: What do you think about using the Boost's
program_options to write settings like the transaction fee into a file
bitcoin.config? Or is it better to save them in the database as it is
now? Having a config file would make it easier to change the settings
when running the program on a remote server with a console access only.

Email #31

Date: Sat, 29 Aug 2009 18:31:05 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

> Next I'm going to implement the "minimize to tray" feature and the
> option to autostart Bitcoin with Windows, so the number of nodes online
> would stay higher.

Now that I think about it, you've put your finger on the most important missing feature right now that would make an order of magnitude difference in the number of nodes. Without auto-run, we'll almost never retain nodes after an initial tryout interest. Auto-running as a minimized tray icon by default was the key to success for the early file sharing networks. It wouldn't have been appropriate for v0.1.0 when stability wasn't a given yet, but now it's good and stable. This is a must-have feature for the next release so any users that come back to try the new version we hopefully retain this time.

I think the most user friendly way of doing auto-run is putting an icon in the Startup folder. I see OpenOffice.org and a number of other things on my computer do it that way. The other way, creating a runas registry entry, is not easily visible or editable by users, I've never liked that much. I guess what we want is an auto-run option that's on by default, if the option is changed then it creates or deletes the startup icon.

While it's tempting to do a Linux port, once we do it we have that extra work with every release from then on. I'd rather put it off a while longer. Auto-run might give us 300% more nodes while Linux might give us 3% more. Linux would help server farms, but actually we'd like to favour individual users. Someone reported that it works fine in WinE.

Email #32

Date: Wed, 16 Sep 2009 15:54:42 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

Just for information: I committed my working copy to the svn/branches. There's the minimize to tray feature and some other changes. It's nicer to run in the background now, but it's still incomplete and I'm working on it. The bugs are listed in bugs.txt.

Did you get your Sourceforge account work yet?

Email #33

Date: Wed, 30 Sep 2009 19:12:29 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

To: mmalmi@cc.hut.fi

That's great, that's a good step forward.

Yes, I worked out the sourceforge login problem, it was some tricky thing on the login page that exposed a quirky bug in a browser add-in.

mmalmi@cc.hut.fi wrote:
> Just for information: I committed my working copy to the svn/branches.
> There's the minimize to tray feature and some other changes. It's nicer
> to run in the background now, but it's still incomplete and I'm working
> on it. The bugs are listed in bugs.txt.
>
> Did you get your Sourceforge account work yet?
>

Email #34

Date: Thu, 08 Oct 2009 20:44:49 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin

I made a Windows installer for the latest version of Bitcoin, which includes the autostart and minimize to tray features. The installer makes a start menu shortcut and a startup registry entry. I first implemented the autostart with a shortcut to the startup folder, but I found out that it doesn't always work by default and ended up doing it with a registry entry. The registry entry is removed by the uninstaller and can be also disabled from the options menu, so I don't think it's such a big menace to the user after all.

I made the installer with NSIS, and the nsi script can be found in the SVN.

Could you add the installer to the SF download page? Here's the file: http://bitcoin.sourceforge.net/uploads/Bitcoin_setup.exe

There are some new users registered to the bitcoin.sf.net site. One of them just announced that he's trading Bitcoins for dollars. Here's his site: http://newlibertystandard.wetpaint.com/. Making an exchange service first seemed a bit premature for the time being, but on the other hand it's good that people show interest towards the project, and this might attract even more interested people (and hopefully more developers). I just sent the guy an email.

Email #35

Date: Fri, 16 Oct 2009 19:41:40 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: mmalmi@cc.hut.fi

Thanks for that. I'm still merging in some changes I had that need to go in before any next release. Some things based on questions and feedback I've received that'll reduce confusion. I'll probably enable multi-proc generating support, and hopefully make it safe to just backup wallet.dat to backup your money. It's good to be coding again!

I'm going to hide the transaction fee setting, which is completely not needed and only serves to confuse people. It was only there for testing and demonstration of a technical detail that can only be needed in the far away future, if ever, but was necessary to implement at the beginning to make it possible later.

What was the problem with the shortcut in the startup folder? If you could send me the code, I'd like to take another look and see if I can see what the problem was. The first strcat in the registry code should be strcpy, otherwise it would fail intermittently. If the same code was in the shortcut one, maybe that was the problem.

It's encouraging to see more people taking an interest such as that NewLibertyStandard site. I like his approach to estimating the value based on electricity. It's educational to see what explanations people adopt. They may help discover a simplified way of understanding it that makes it more accessible to the masses. Many complex concepts in the world have a simplistic explanation that satisfies 80% of people, and a complete explanation that satisfies the other 20% who see the flaws in the simplistic explanation.

```
mmalmi@cc.hut.fi wrote:
> I made a Windows installer for the latest version of Bitcoin, which
> includes the autostart and minimize to tray features. The installer
> makes a start menu shortcut and a startup registry entry. I first
> implemented the autostart with a shortcut to the startup folder, but I
> found out that it doesn't always work by default and ended up doing it
> with a registry entry. The registry entry is removed by the uninstaller
> and can be also disabled from the options menu, so I don't think it's
> such a big menace to the user after all.
>
> I made the installer with NSIS, and the nsi script can be found in the SVN.
>
> Could you add the installer to the SF download page? Here's the file:
> http://bitcoin.sourceforge.net/uploads/Bitcoin_setup.exe
>
> There are some new users registered to the bitcoin.sf.net site. One of
> them just announced that he's trading Bitcoins for dollars. Here's his
> site: http://newlibertystandard.wetpaint.com/. Making an exchange
> service first seemed a bit premature for the time being, but on the
> other hand it's good that people show interest towards the project, and
> this might attract even more interested people (and hopefully more
> developers). I just sent the guy an email.
>
```

Email #36

Date: Sun, 18 Oct 2009 18:59:42 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: Martti Malmi <mmalmi@cc.hut.fi>

```
I got it, I see you checked in the startup folder code before changing
it to registry.  I don't see any visible problems in the code.  I guess
it depends what exactly the problem was with it not always working by
default.  Was there a Vista/UAC security problem?

Satoshi Nakamoto wrote:
> What was the problem with the shortcut in the startup folder?  If you
> could send me the code, I'd like to take another look and see if I can
> see what the problem was.  The first strcat in the registry code should
> be strcpy, otherwise it would fail intermittently.  If the same code was
> in the shortcut one, maybe that was the problem.
>
> mmalmi@cc.hut.fi wrote:
>> I made a Windows installer for the latest version of Bitcoin, which
>> includes the autostart and minimize to tray features. The installer
>> makes a start menu shortcut and a startup registry entry. I first
>> implemented the autostart with a shortcut to the startup folder, but I
>> found out that it doesn't always work by default and ended up doing it
>> with a registry entry. The registry entry is removed by the
>> uninstaller and can be also disabled from the options menu, so I don't
>> think it's such a big menace to the user after all.
```

Email #37

Date: Mon, 19 Oct 2009 00:02:28 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

Well, the code worked and made a shortcut in the startup folder. For some reason it didn't automatically start when booting, but worked fine when you clicked on it in the menu. Now I tried making a shortcut manually, and this time it works on autostart, don't know why. I could try again with the older code.

> I got it, I see you checked in the startup folder code before changing
> it to registry. I don't see any visible problems in the code. I guess
> it depends what exactly the problem was with it not always working by
> default. Was there a Vista/UAC security problem?
>
> Satoshi Nakamoto wrote:
>> What was the problem with the shortcut in the startup folder? If
>> you could send me the code, I'd like to take another look and see
>> if I can see what the problem was. The first strcat in the
>> registry code should be strcpy, otherwise it would fail
>> intermittently. If the same code was in the shortcut one, maybe
>> that was the problem.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I made a Windows installer for the latest version of Bitcoin,
>>> which includes the autostart and minimize to tray features. The
>>> installer makes a start menu shortcut and a startup registry
>>> entry. I first implemented the autostart with a shortcut to the
>>> startup folder, but I found out that it doesn't always work by
>>> default and ended up doing it with a registry entry. The registry
>>> entry is removed by the uninstaller and can be also disabled from
>>>   the options menu, so I don't think it's such a big menace to the
>>>   user after all.

Email #38

Date: Mon, 19 Oct 2009 00:11:50 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: mmalmi@cc.hut.fi

It's possible Bitcoin ran and bailed out because something was wrong. debug.log should tell something if that was the case. What OS are you using? I wonder if we need Admin privilege and don't realize it. Stuff that requires Admin can't start on startup on Vista.

Program shortcuts have multiple tabs of settings with lots of little details. I'll try the startup folder code and see if I can reproduce the problem. Every other systray icon on my computer is in the startup folder, and it makes it easy for users to manage all their autoruns in one place. The things in the registry key tend to be devious hidden bloatware.

I implemented the code to flush wallet.dat whenever it's closed so we'll be able to tell users they only need to backup wallet.dat. You can restore just wallet.dat and it'll re-download the rest. I'll have to do another stress test before release.

mmalmi@cc.hut.fi wrote:
> Well, the code worked and made a shortcut in the startup folder. For
> some reason it didn't automatically start when booting, but worked fine
> when you clicked on it in the menu. Now I tried making a shortcut
> manually, and this time it works on autostart, don't know why. I could

> try again with the older code.
>
>> I got it, I see you checked in the startup folder code before changing
>> it to registry. I don't see any visible problems in the code. I guess
>> it depends what exactly the problem was with it not always working by
>> default. Was there a Vista/UAC security problem?
>>
>> Satoshi Nakamoto wrote:
>>> What was the problem with the shortcut in the startup folder? If
>>> you could send me the code, I'd like to take another look and see
>>> if I can see what the problem was. The first strcat in the
>>> registry code should be strcpy, otherwise it would fail
>>> intermittently. If the same code was in the shortcut one, maybe
>>> that was the problem.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I made a Windows installer for the latest version of Bitcoin,
>>>> which includes the autostart and minimize to tray features. The
>>>> installer makes a start menu shortcut and a startup registry
>>>> entry. I first implemented the autostart with a shortcut to the
>>>> startup folder, but I found out that it doesn't always work by
>>>> default and ended up doing it with a registry entry. The registry
>>>> entry is removed by the uninstaller and can be also disabled from
>>>> the options menu, so I don't think it's such a big menace to the
>>>> user after all.
>
>
>
>

Email #39

Date: Tue, 20 Oct 2009 21:38:56 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

> It's possible Bitcoin ran and bailed out because something was wrong.
> debug.log should tell something if that was the case. What OS are you
> using? I wonder if we need Admin privilege and don't realize it.
> Stuff that requires Admin can't start on startup on Vista.

I'm using XP. I recompiled the older revision and this time the
startup shortcut works. It also works when testing on Vista
(non-admin). Maybe I just missed something the previous time.

> Program shortcuts have multiple tabs of settings with lots of little
> details. I'll try the startup folder code and see if I can reproduce
> the problem. Every other systray icon on my computer is in the startup
> folder, and it makes it easy for users to manage all their autoruns in
> one place. The things in the registry key tend to be devious hidden
> bloatware.

Here it's the other way around, I have all my startup programs in the
registry. But maybe the shortcut method is nicer for the user, if it
works just as well

Email #40

Date: Wed, 21 Oct 2009 18:58:49 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Setup, Autorun, v0.1.6

To: mmalmi@cc.hut.fi

```
Yeah, I put back your startup folder shortcut code and it started fine
for me too on XP and Vista.  For good measure, I changed it to make the
shortcut settings look identical to one I manually created.  I set the
working directory to where the EXE is since that's where debug.log is
created, otherwise windows puts it in some weird directory.  I didn't
change the setup script yet.

I checked everything in to SVN (thanks for setting that up)
- multi-proc generate
- flush wallet.dat after every change so the DB doesn't leave that stuff
in the transaction logs
- view menu checkbox to hide all generated coins so you can see just
your payment transactions
- disabled transaction fee option
- made the minimize to tray options similar to Firefox's MinimizeToTray
- bunch of other misc changes since the 0.1.5 release

I made it not show non-accepted generated coins.  It won't show
generated coins until they have at least one confirmation (one block
linked after it), so usually they'll just never be seen.  Occasionally a
generated coin that was displayed might disappear because it became not
accepted later.  I don't think anyone would notice the occasional
non-accepteds if we didn't point them out in the UI.  People have told
me they find it annoying to have to look at them, as they're permanently
displayed in the transaction record.

I still have more testing to do.  I guess we gotta test Windows 7 now.

mmalmi@cc.hut.fi wrote:
>> It's possible Bitcoin ran and bailed out because something was wrong.
>> debug.log should tell something if that was the case.  What OS are you
>> using?  I wonder if we need Admin privilege and don't realize it.
>> Stuff that requires Admin can't start on startup on Vista.
>
> I'm using XP. I recompiled the older revision and this time the startup
> shortcut works. It also works when testing on Vista (non-admin). Maybe I
> just missed something the previous time.
>
>> Program shortcuts have multiple tabs of settings with lots of little
>> details.  I'll try the startup folder code and see if I can reproduce
>> the problem.  Every other systray icon on my computer is in the startup
>> folder, and it makes it easy for users to manage all their autoruns in
>> one place.  The things in the registry key tend to be devious hidden
>> bloatware.
>
> Here it's the other way around, I have all my startup programs in the
> registry. But maybe the shortcut method is nicer for the user, if it
> works just as well
>
```

Email #41

Date: Sat, 24 Oct 2009 00:55:06 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: [bitcoin-list] Does Bitcoin Crash in Windows?

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: bitcoin-list@lists.sourceforge.net

Liberty Standard wrote:
> Do you Windows users experience occasional Bitcoin crashes?
> Lately Bitcoin running in wine-1.0.1 has been crashing frequently. I was
> just wondering whether this is a Wine issue or a Bitcoin issue.

I haven't had any reports of crashes in v0.1.5. It's been rock solid
for me on Windows. I think it must be Wine related. If you get another
crash in Wine and it prints anything on the terminal, e-mail me and I
may be able to figure out what happened, maybe something I can work
around. Martti and I have been working on a new version to release soon
and it would be nice to get any Wine fixes in there.

> The following four lines print from the terminal when I start Bitcoin.
> fixme:toolhelp:CreateToolhelp32Snapshot Unimplemented: heap list snapshot
> fixme:toolhelp:Heap32ListFirst : stub
> fixme:toolhelp:CreateToolhelp32Snapshot Unimplemented: heap list snapshot
> fixme:toolhelp:Heap32ListFirst : stub

Those don't look like anything to worry about. Probably functions
unimplemented by Wine that are harmlessly stubbed out.

> I previously wasn't starting Bitcoin from the terminal, so I don't know what
> gets printed out when it crashes, but I'll reply with the results the next
> time it crashes.
>
> While Bitcoin first downloads previously completed blocks, the file
> debug.log grows grows to 17.4 MB and then stops growing. I imagine it will
> continue to grow as more bitcoins are completed.

You can delete debug.log occasionally if you don't want to take the disk
space. It's just status messages that help with debugging.

bitcoin.sourceforge.net looks fine now. Maybe sourceforge was doing
some maintenance.

Satoshi

Email #42

Date: Mon, 26 Oct 2009 17:50:10 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Fw: bitcoin.sourceforge.net

To: Martti Malmi <mmalmi@cc.hut.fi>

Any idea what's going on with it? Every time I look, it's fine.

Eugen Leitl wrote:
On Sat, Oct 24, 2009 at 12:55:06AM +0100, Satoshi Nakamoto wrote:
> > bitcoin.sourceforge.net looks fine now. Maybe sourceforge was doing

Doesn't work right now.

```
 > > some maintenance.


Liberty Standard wrote:
 > In case you weren't aware, the Bitcoin website is down.
 >
 > http://bitcoin.sourceforge.net/
 >
 > -----
 > You are running bitweaver in TEST mode
 >
 >     * Click here to log a bug, if this appears to be an error with the
 > application.
 >     * Go here to begin the installation process, if you haven't done so
 > already.
 >     * To hide this message, please set the IS_LIVE constant to TRUE
in your
 > kernel/config_inc.php file.
```

Email #43

Date: Tue, 27 Oct 2009 05:02:49 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

```
IS_LIVE option was indeed set to false, but it only affects the
visibility of error messages to user. I've noticed the site being slow
at times, sometimes taking up to 30 seconds to load. I think it's
related to the Sourceforge hosting. Bitweaver should be among the
lightest PHP CMS'es, but I can check out if there are any issues to it.

Off the topic, do you think that we could use Boost's thread and
socket libraries instead of the Windows-specific ones? Are there other
windows-only-functions used in the code?

> Any idea what's going on with it?  Every time I look, it's fine.
>
>
> Eugen Leitl wrote:
> On Sat, Oct 24, 2009 at 12:55:06AM +0100, Satoshi Nakamoto wrote:
>> > bitcoin.sourceforge.net looks fine now.  Maybe sourceforge was doing
>
> Doesn't work right now.
>
>> > some maintenance.
>
>
> Liberty Standard wrote:
>> In case you weren't aware, the Bitcoin website is down.
>>
>> http://bitcoin.sourceforge.net/
>>
>> -----
>> You are running bitweaver in TEST mode
>>
>>     * Click here to log a bug, if this appears to be an error with the
>> application.
>>     * Go here to begin the installation process, if you haven't done so
>> already.
>>     * To hide this message, please set the IS_LIVE constant to TRUE in your
>> kernel/config_inc.php file.
```

Email #44

Date: Tue, 27 Oct 2009 04:45:47 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

To: mmalmi@cc.hut.fi

```
Sourceforge is just so darn slow.  I don't know what else to do though.
  It's such a standard, more often than not any given project has a
projectname.sourceforge.net site.  When I see whatever.sourceforge.net
in a google search, I assume that's the official site.

Is there a way to make Bitweaver allow users to edit (and maybe delete)
their own messages in the forum?

Getting antsy to port to Linux?  It's not a decision to be taken lightly
because once it's done, it doubles my testing and building workload.
Although I am worried about Liberty's Wine crashes.

I've tried to be as portable as possible and use standard C stuff
instead of Windows calls.  The threading is _beginthread which is part
of the standard C library.  wxWidgets has wxCriticalSection stuff we can
use.  The sockets code is send/recv stuff which I think is the same as
unix because Microsoft ported sockets from BSD.  We need direct control
over sockets, it wouldn't be a good idea to get behind an abstraction
layer.  wxWidgets is a good place to look for cross-platform support
functions.  I want to avoid #ifdefing up the code if we can.  Anything
that's used more than once probably becomes a function in util.cpp that
has the #ifdef in it.

BTW, I have a lot of uncommitted changes right now because it includes
some crucial protocol transitions that can't be unleashed on the network
until I've tested the heck out of it.  It shouldn't be too much longer.

Can you make the setup uninstall the Startup folder icon?  I figure it
should install and uninstall an icon in a regular program group, and
just uninstall the Startup folder one.  I guess it doesn't matter that
much whether it installs and uninstalls the Startup folder icon or just
uninstalls it.

mmalmi@cc.hut.fi wrote:
> IS_LIVE option was indeed set to false, but it only affects the
> visibility of error messages to user. I've noticed the site being slow
> at times, sometimes taking up to 30 seconds to load. I think it's
> related to the Sourceforge hosting. Bitweaver should be among the
> lightest PHP CMS'es, but I can check out if there are any issues to it.
>
> Off the topic, do you think that we could use Boost's thread and socket
> libraries instead of the Windows-specific ones? Are there other
> windows-only-functions used in the code?
>
>> Any idea what's going on with it?  Every time I look, it's fine.
>>
>>
>> Eugen Leitl wrote:
>> On Sat, Oct 24, 2009 at 12:55:06AM +0100, Satoshi Nakamoto wrote:
>>> > bitcoin.sourceforge.net looks fine now.  Maybe sourceforge was doing
>>
>> Doesn't work right now.
```

```
>>
>>> > some maintenance.
>>
>>
>> Liberty Standard wrote:
>>> In case you weren't aware, the Bitcoin website is down.
>>>
>>> http://bitcoin.sourceforge.net/
>>>
>>> -----
>>> You are running bitweaver in TEST mode
>>>
>>>     * Click here to log a bug, if this appears to be an error with the
>>> application.
>>>     * Go here to begin the installation process, if you haven't done so
>>> already.
>>>     * To hide this message, please set the IS_LIVE constant to TRUE
>>> in your
>>> kernel/config_inc.php file.
>
>
>
```

Email #45

Date: Wed, 28 Oct 2009 23:27:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

```
> Sourceforge is just so darn slow.  I don't know what else to do though.
>  It's such a standard, more often than not any given project has a
> projectname.sourceforge.net site.  When I see whatever.sourceforge.net
> in a google search, I assume that's the official site.
>
> Is there a way to make Bitweaver allow users to edit (and maybe delete)
> their own messages in the forum?

It's not possible with the current version of Bitweaver. Bitweaver's
wiki and forum packages aren't so very highly advanced. SF hosting
also has its disadvantages, like the occasional slowness and lack of
e-mailer and user IP retrieving. I've been considering to buy web
hosting from prq.se (the host of Wikileaks and Pirate Bay, among
others) to be used later for the exchange service. I could maybe host
the project site there as well, under a separate user account for
better security. There I could set up Drupal or TikiWiki, which are
more advanced and have quite a lot bigger and more active
developer/user communities than Bitweaver.

> Getting antsy to port to Linux?  It's not a decision to be taken
> lightly because once it's done, it doubles my testing and building
> workload. Although I am worried about Liberty's Wine crashes.
>
> I've tried to be as portable as possible and use standard C stuff
> instead of Windows calls.  The threading is _beginthread which is part
> of the standard C library.  wxWidgets has wxCriticalSection stuff we
> can use.  The sockets code is send/recv stuff which I think is the same
> as unix because Microsoft ported sockets from BSD.  We need direct
> control over sockets, it wouldn't be a good idea to get behind an
> abstraction layer.  wxWidgets is a good place to look for
> cross-platform support functions.  I want to avoid #ifdefing up the
> code if we can.  Anything that's used more than once probably becomes a
```

```
> function in util.cpp that has the #ifdef in it.

Ok. I replaced the Windows thread and socket library includes with
their POSIX equivalents, and now it only gives a few errors, mostly
svn/branches, it doesn't need to be an official release yet.

> Can you make the setup uninstall the Startup folder icon?  I figure it
> should install and uninstall an icon in a regular program group, and
> just uninstall the Startup folder one.  I guess it doesn't matter that
> much whether it installs and uninstalls the Startup folder icon or just
> uninstalls it.

I'll do it.
```

Email #46

Date: Thu, 29 Oct 2009 02:05:30 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

To: mmalmi@cc.hut.fi

```
I'll convert the CriticalSection code to wxCriticalSection and upload it
to SVN (it's a little tricky).  I don't know what to do for
TryEnterCriticalSection though.  I think I'm almost ready to check
everything in.

You're probably right, it's about time to do a linux build.  I've been
working on getting my linux machine set up and building the dependencies.

> Ok. I replaced the Windows thread and socket library includes with their
> POSIX equivalents, and now it only gives a few errors, mostly from the
> CriticalSections. If I make it work, I'll put it into svn/branches, it
> doesn't need to be an official release yet.
```

Email #47

Date: Thu, 29 Oct 2009 06:08:10 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fw: bitcoin.sourceforge.net

```
> I'll convert the CriticalSection code to wxCriticalSection and upload
> it to SVN (it's a little tricky).  I don't know what to do for
> TryEnterCriticalSection though.  I think I'm almost ready to check
> everything in.

Would the Boost mutex be of any help here?

http://www.boost.org/doc/libs/1_40_0/doc/html/thread/
synchronization.html#thread.synchronization.mutex_concepts
```

Email #48

Date: Thu, 29 Oct 2009 06:38:30 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

```
The easy solution I took was to look at the wxWidgets source code and
see how they did it.  They just mapped it to wxMutex on non-MSW, which
does have TryEnter, so that mapped in perfectly.

I checked in all my backlog of changes to SVN, including the overhaul of
CCriticalSection in util.h and OpenSSL's mutex callback in util.cpp to
do everything with wxWidgets when not on Windows.

If we get it working on Linux, I'll run my test suite against it here
off-network first, then we can give an unreleased build to
LibertyStandard to test for a while before going public.

mmalmi@cc.hut.fi wrote:
>> I'll convert the CriticalSection code to wxCriticalSection and upload
>> it to SVN (it's a little tricky).  I don't know what to do for
>> TryEnterCriticalSection though.  I think I'm almost ready to check
>> everything in.
>
> Would the Boost mutex be of any help here?
>
>
http://www.boost.org/doc/libs/1_40_0/doc/html/thread/synchronization.html#thread
.synchronization.mutex_concepts
>
>
```

Email #49

Date: Fri, 30 Oct 2009 01:05:45 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: Martti Malmi <mmalmi@cc.hut.fi>

```
I fixed some non-portable stuff I came across:
QueryPerformanceCounter
%I64d in printf format strings
Sleep
CheckDiskSpace

If there's any other unportable stuff you know of I should fix, let me know.

I think I'll move debug.log and db.log into the same directory as the
data files (%appdata%\Bitcoin), rather than whatever the current
directory happens to be.
```

Email #50

Date: Sat, 31 Oct 2009 11:21:50 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

```
I made an #ifdef to replace QueryPerformanceCounter with Linux's
gettimeofday in util.h. Some Unicode/ANSI errors were resolved without
code changes when I updated to wxWidgets 2.9. The only compile error
I'm getting in Linux at the moment is from heapchk() in util.h.

> I fixed some non-portable stuff I came across:
> QueryPerformanceCounter
> %I64d in printf format strings
```

```
> Sleep
> CheckDiskSpace
>
> If there's any other unportable stuff you know of I should fix, let me know.
>
> I think I'll move debug.log and db.log into the same directory as the
> data files (%appdata%\Bitcoin), rather than whatever the current
> directory happens to be.
```

Email #51

Date: Sat, 31 Oct 2009 20:09:58 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

```
heapchk() is just a MSVCRT debugging thing that's not being used.  It
can be a no-op on Linux.  OpenSSL automatically uses /dev/urandom to
seed on Linux, so RandAddSeedPerfmon can also be a no-op.

Don't let it connect to the network before we've tested it thoroughly
off-net.  If you have two computers, unplug the internet and use
"bitcoin -connect=<ip>" to connect to each other, one windows and one
linux.  -connect will allow you to connect to non-routable addresses
like 192.168.x.x.  We don't want to reflect badly on the reliability of
the network if it throws off some malformed crud we hadn't thought to
check for yet, or discovers something else anti-social to do on the network.

I have time that I can do some testing when you've got something
buildable to test.  I can include it in the stress test I'm currently
running on the changes so far.

mmalmi@cc.hut.fi wrote:
> I made an #ifdef to replace QueryPerformanceCounter with Linux's
> gettimeofday in util.h. Some Unicode/ANSI errors were resolved without
> code changes when I updated to wxWidgets 2.9. The only compile error I'm
> getting in Linux at the moment is from heapchk() in util.h.
>
>> I fixed some non-portable stuff I came across:
>> QueryPerformanceCounter
>> %I64d in printf format strings
>> Sleep
>> CheckDiskSpace
>>
>> If there's any other unportable stuff you know of I should fix, let me
>> know.
>>
>> I think I'll move debug.log and db.log into the same directory as the
>> data files (%appdata%\Bitcoin), rather than whatever the current
>> directory happens to be.
>
>
>
```

Email #52

Date: Tue, 03 Nov 2009 09:31:41 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

```
I uploaded what I've ported so far to the svn/branches. Util, script,
db and the headers compile fully now and net.cpp partially, so there's
still work to do.

_beginthread doesn't have a direct Linux equivalent, so I used Boost
threads instead.

I couldn't get connected using the Tor SOCKS proxy. That might be
because of the Freenode Tor policy which requires connecting to their
hidden service: http://freenode.net/irc_servers.shtml#tor

> heapchk() is just a MSVCRT debugging thing that's not being used.  It
> can be a no-op on Linux.  OpenSSL automatically uses /dev/urandom to
> seed on Linux, so RandAddSeedPerfmon can also be a no-op.
>
> Don't let it connect to the network before we've tested it thoroughly
> off-net.  If you have two computers, unplug the internet and use
> "bitcoin -connect=<ip>" to connect to each other, one windows and one
> linux.  -connect will allow you to connect to non-routable addresses
> like 192.168.x.x.  We don't want to reflect badly on the reliability of
> the network if it throws off some malformed crud we hadn't thought to
> check for yet, or discovers something else anti-social to do on the
> network.
>
> I have time that I can do some testing when you've got something
> buildable to test.  I can include it in the stress test I'm currently
> running on the changes so far.
>
> mmalmi@cc.hut.fi wrote:
>> I made an #ifdef to replace QueryPerformanceCounter with Linux's
>> gettimeofday in util.h. Some Unicode/ANSI errors were resolved
>> without code changes when I updated to wxWidgets 2.9. The only
>> compile error I'm getting in Linux at the moment is from heapchk()
>> in util.h.
>>
>>> I fixed some non-portable stuff I came across:
>>> QueryPerformanceCounter
>>> %I64d in printf format strings
>>> Sleep
>>> CheckDiskSpace
>>>
>>> If there's any other unportable stuff you know of I should fix,
>>> let me know.
>>>
>>> I think I'll move debug.log and db.log into the same directory as the
>>> data files (%appdata%\Bitcoin), rather than whatever the current
>>> directory happens to be.
>>
>>
>>
```

Email #53

Date: Tue, 03 Nov 2009 15:53:25 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build, proxy

To: mmalmi@cc.hut.fi

Great, I've been looking forward to working on the Linux build.

If you connect to Freenode's hidden service, then they tell you they've also banned TOR from that due to abuse and it kicks you off. There's a several step procedure you can do to run a password utility on unix and e-mail request an account that you could login with, but that's getting pretty complicated. I wonder if we could get away with applying for one account and then everyone use the same account? I suppose the IRC server probably limits accounts to one login, or some admin might not like to see a dozen logins on the same account.

Besides the IRC part, how did your test of proxy go? Since you've been connected before, your addr.dat contains known node addresses, but without IRC to know which ones are online, it takes a long time to find them. There are normally 1 to 3 other nodes besides you that can accept incoming connections, and existing nodes that already know you would eventually connect to you. How many connections did you get, and how long did it take? I guess to know whether it successfully connected outbound through TOR you'd need to search debug.log for "connected".

To originally connect with TOR without connecting normally once to get seeded, you'd have to know the address of an existing node that can accept incoming connections and seed it like this:
bitcoin -proxy=127.0.0.1:9050 -addnode=<ip of a node>

If some nodes that accept incoming connects were willing to have their IP coded into the program, it could seed automatically. Or some IP seed addresses posted on a Wiki page with the instructions.

Another option is to search the world again for an IRC server that doesn't ban TOR nodes. Or if we could get someone to set one up. IRC servers ban TOR because they have actual text chat on them... if there was one with just bots and junk then it wouldn't care. Probably should post a question on the forum or the mailing list and see if anyone knows one.

Another problem is that TOR users can't accept incoming connections, and we have so few that can. If everyone goes to TOR, there won't be any nodes to connect to.

We have a shortage of nodes that can accept incoming connections. It generally ranges from 2 to 4 lately. We need to emphasize the importance to people of setting up port forwarding on their router. Every P2P file sharing program has instructions how to do it. We should have a paragraph on the bitcoin.sourceforge.net homepage urging people to set up port forwarding to accept incoming connections, and a link to a site that describes how to do it for each router.

mmalmi@cc.hut.fi wrote:
> I uploaded what I've ported so far to the svn/branches. Util, script, db
> and the headers compile fully now and net.cpp partially, so there's
> still work to do.
>
> _beginthread doesn't have a direct Linux equivalent, so I used Boost
> threads instead.
>
> I couldn't get connected using the Tor SOCKS proxy. That might be
> because of the Freenode Tor policy which requires connecting to their
> hidden service: http://freenode.net/irc_servers.shtml#tor
>
>> heapchk() is just a MSVCRT debugging thing that's not being used. It
>> can be a no-op on Linux. OpenSSL automatically uses /dev/urandom to

```
>> seed on Linux, so RandAddSeedPerfmon can also be a no-op.
>>
>> Don't let it connect to the network before we've tested it thoroughly
>> off-net.  If you have two computers, unplug the internet and use
>> "bitcoin -connect=<ip>" to connect to each other, one windows and one
>> linux.  -connect will allow you to connect to non-routable addresses
>> like 192.168.x.x.  We don't want to reflect badly on the reliability of
>> the network if it throws off some malformed crud we hadn't thought to
>> check for yet, or discovers something else anti-social to do on the
>> network.
>>
>> I have time that I can do some testing when you've got something
>> buildable to test.  I can include it in the stress test I'm currently
>> running on the changes so far.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I made an #ifdef to replace QueryPerformanceCounter with Linux's
>>> gettimeofday in util.h. Some Unicode/ANSI errors were resolved
>>> without code changes when I updated to wxWidgets 2.9. The only
>>> compile error I'm getting in Linux at the moment is from heapchk()
>>> in util.h.
>>>
>>>> I fixed some non-portable stuff I came across:
>>>> QueryPerformanceCounter
>>>> %I64d in printf format strings
>>>> Sleep
>>>> CheckDiskSpace
>>>>
>>>> If there's any other unportable stuff you know of I should fix,  let
>>>> me know.
>>>>
>>>> I think I'll move debug.log and db.log into the same directory as the
>>>> data files (%appdata%\Bitcoin), rather than whatever the current
>>>> directory happens to be.
>>>
>>>
>>>
>
>
>
```

Email #54

Date: Wed, 04 Nov 2009 05:38:17 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

```
It was almost there.  I fixed a few things and got it to finish
compiling but I don't know the system libraries to link to so there's
undefined references galore.

I changed the makefile to look for things under /usr/local and in their
default "make install" locations.  I wrote what I did and switches I
used in build-unix.txt.  I'm currently using wxWidgets 2.8.9 for now
because it's the same version as on Windows and I don't want to wonder
if there's version change issues at the same time as platform change.
2.8.10 or 2.9.0 are probably fine though.  I went with the
single-library compile of wxWidgets since we're linking to almost every
library anyway.

I added xpm files, which is what they use everywhere else but Windows
```

instead of RC files. They're clever C files that define graphics in static arrays. The bitcoin icon has 5 different versions but I couldn't figure out how that works in xpm so I only put the biggest one. Maybe on GTK it scales it for you. I don't know if these are right or what, but they compile.

mmalmi@cc.hut.fi wrote:
> I uploaded what I've ported so far to the svn/branches. Util, script, db
> and the headers compile fully now and net.cpp partially, so there's
> still work to do.
>
> _beginthread doesn't have a direct Linux equivalent, so I used Boost
> threads instead.
>

Email #55

Date: Wed, 04 Nov 2009 20:38:03 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: mmalmi@cc.hut.fi

Just letting you know I'm still working on the Linux build so we don't duplicate work. I got it linked and ran it and working through runtime issues like getting it switched to load bitmaps from xpm instead of resources.

There are debian packages available for some of the dependencies instead of having to compile them ourselves:
apt-get install build-essential
apt-get install libgtk2.0-dev
apt-get install libssl-dev

I need to see if Berkeley DB or Boost have packages.

We'll shared-link OpenSSL, I'm pretty sure it's always preinstalled on Linux. GTK has to be shared linked. I'm not completely sure if it's preinstalled by default.

Email #56

Date: Wed, 04 Nov 2009 23:42:44 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

> Besides the IRC part, how did your test of proxy go? Since you've been
> connected before, your addr.dat contains known node addresses, but
> without IRC to know which ones are online, it takes a long time to find
> them. There are normally 1 to 3 other nodes besides you that can
> accept incoming connections, and existing nodes that already know you
> would eventually connect to you. How many connections did you get, and
> how long did it take? I guess to know whether it successfully
> connected outbound through TOR you'd need to search debug.log for
> "connected".

Enabling the proxy setting and restarting Bitcoin I got the first connections in less than a minute and ultimately even 8 connections. I wonder if they're all really through TOR. Netstat shows only 2 connections to localhost:9050 and 7 connections from local port 8333 to elsewhere. (Some of the shown connections may be already

```
disconnected ones.) For some reason there's no debug.log in the folder
where I'm running it.

> If some nodes that accept incoming connects were willing to have their
> IP coded into the program, it could seed automatically.  Or some IP
> seed addresses posted on a Wiki page with the instructions.

The wiki page sounds like a good and quickly applicable solution. I
could keep my ip updated there and we could ask others to do the same.
When the Linux build works, it's easier to set up nodes on servers
that are online most of the time and have a static IP. A static ip
list shipped with Bitcoin and a peer exchange protocol would be cool.
That way there'd be no need for an IRC server.

> Just letting you know I'm still working on the Linux build so we don't
> duplicate work.  I got it linked and ran it and working through runtime
> issues like getting it switched to load bitmaps from xpm instead of
> resources.

Ok. I didn't get it linked on the first attempt, but I didn't look
further into the dependencies yet.
```

Email #57

Date: Thu, 05 Nov 2009 05:31:03 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: Martti Malmi <mmalmi@cc.hut.fi>

```
I merged the linux changes into the main trunk on SVN.  It compiles and
runs now.  I think all the problems are in the UI.  The menus quickly
quit working and it doesn't repaint when it's supposed to unless I
resize it, and the UI is getting some segfaults.  Shouldn't be too hard
to debug with gdb.  I haven't tested if it plays nice with other nodes
yet so keep it off-net.

build-unix.txt and makefile.unix added
```

Email #58

Date: Thu, 05 Nov 2009 15:25:27 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Proxy

To: mmalmi@cc.hut.fi

```
mmalmi@cc.hut.fi wrote:
> Enabling the proxy setting and restarting Bitcoin I got the first
> connections in less than a minute and ultimately even 8 connections. I
> wonder if they're all really through TOR. Netstat shows only 2
> connections to localhost:9050 and 7 connections from local port 8333 to
> elsewhere. (Some of the shown connections may be already disconnected
> ones.) For some reason there's no debug.log in the folder where I'm
> running it.

debug.log moved to the data directory "%appdata%/bitcoin/debug.log"

7 inbound and 2 outbound sounds about as expected.

My last SVN commit included an overhaul of the code that selects the
order of addresses to connect to, trying them in the order of most
recently seen online, so it should get connected in a more reasonable
```

amount of time if IRC is unavailable. IRC is really only needed to seed
the first connection, but we've been using it as a crutch to get
connected faster.

>> If some nodes that accept incoming connects were willing to have their
>> IP coded into the program, it could seed automatically. Or some IP
>> seed addresses posted on a Wiki page with the instructions.
>
> The wiki page sounds like a good and quickly applicable solution. I
> could keep my ip updated there and we could ask others to do the same.
> When the Linux build works, it's easier to set up nodes on servers that
> are online most of the time and have a static IP. A static ip list
> shipped with Bitcoin and a peer exchange protocol would be cool. That
> way there'd be no need for an IRC server.

That would be great. It's only TOR users that need it, so in the
instructions saying "bitcoin -proxy=127.0.0.1:9050 -addnode=<someip>",
someip could be an actual static IP, with the wiki free-for-all
add-your-ip list nearby or a link to it. There should be a link to that
optional step, add your IP to this list now that you can accept incoming
if you're static.

Do you think anonymous people are looking to be completely stealth, as
in never connect once without TOR so nobody knows they use bitcoin, or
just want to switch to TOR before doing any transactions? It's just if
you want to be completely stealth that you'd have to go through the
-proxy -addnode manual seeding. It would be very easy to fumble that
up; if you run bitcoin normally to begin with it immediately
automatically starts connecting.

Email #59

Date: Thu, 05 Nov 2009 17:33:58 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Forum

To: Martti Malmi <mmalmi@cc.hut.fi>

Now that the forum on bitcoin.sourceforge.net is catching on, we really
should look for somewhere that freehosts full blown forum software. The
bitweaver forum feature is just too lightweight. I assume the "Forum"
tab on the homepage can link out to wherever the forum is hosted.

I've seen projects that have major following just from forum talk and
pie-in-the-sky planning without even having any code yet. Having a lot
of forum talk gives a project more presence on the net, more search
hits, makes it look big, draws new users in, helps solve support
questions, hashes out what features are most of wanted.

It would be a big plus if it could support SSL, at least for the login
page if not sitewide. Multiple people on the forum have expressed
interest in TOR/I2P, and those users need SSL because a lot of TOR exit
nodes are probably password scrapers run by identity thieves. A lot of
the core interest in Bitcoin is going to be from the privacy crowd.

Any ideas where we can get a free forum? Maybe we should look at where
some other projects have their forums hosted for ideas where to look.

Email #60

Date: Fri, 06 Nov 2009 06:20:15 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build

To: Martti Malmi <mmalmi@cc.hut.fi>

```
It works reliably on Linux now, except if it uses wxMessageBox() outside
the GUI thread, it'll crash because non-GUI threads can't open a window
on Linux.  I haven't got to fixing that yet.  I've been running my
stress test on it and it's functioning normally.

Most of wxWidgets is not thread-safe to use in threads other than the UI
thread, but as a rule of thumb on Windows anything not UI related is OK.
  It turns out its more thread-unsafe on GTK.  I replaced a bunch of
stuff at once so I don't know if it was just one thing (probably
Repaint), but I have to assume even any wx function that uses wxString
is not safe to use outside the UI thread.  So dang, there goes all the
nice wxWidgets portability support functions.  I left a few simple
things like wxThread::GetCPUCount() that I checked the source and it's
all numerical, and wxMutex has to be safe or it'd be useless.

There's an issue that if you exit and run it again right away, it can't
bind port 8333.  The port frees up after about a minute.  Unless I'm
missing something, I am closing the socket before exit, so I don't know
what else I can do.  Maybe this is just something about Linux that it
takes a minute to free up a port you had bound.  Possibly a security
feature so some trojan doesn't kill the web server and quickly jump into
its place and pick up all the client retries.

Still gotta figure out how to do the xpm version of the icon correctly.

I wonder if the database dat files are interchangeable with Windows.
```

Email #61

Date: Sat, 07 Nov 2009 12:13:45 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

```
> Do you think anonymous people are looking to be completely stealth, as
> in never connect once without TOR so nobody knows they use bitcoin, or
> just want to switch to TOR before doing any transactions?  It's just if
> you want to be completely stealth that you'd have to go through the
> -proxy -addnode manual seeding.  It would be very easy to fumble that
> up; if you run bitcoin normally to begin with it immediately
> automatically starts connecting.

The people who are interested in being stealthy tend to be more
technically able, and they probably don't have a problem following the
instructions to get perfect secrecy. Of course there could be a
connect-button in the UI that needs to be clicked before use, but the
tradeoff is that the UI becomes less straightforward for the average
user.

> It would be a big plus if it could support SSL, at least for the login
> page if not sitewide.  Multiple people on the forum have expressed
> interest in TOR/I2P, and those users need SSL because a lot of TOR exit
> nodes are probably password scrapers run by identity thieves.  A lot of
> the core interest in Bitcoin is going to be from the privacy crowd.
>
> Any ideas where we can get a free forum?  Maybe we should look at where
> some other projects have their forums hosted for ideas where to look.
```

```
One option would be ning.com. Ning.com is a popular community site and
many users who already have an account wouldn't need to register a new
account. Example: http://p2pfoundation.ning.com/. This seems to
support SSL.

Another option would be to relocate the whole site to some place where
we can run Drupal or TikiWiki. I've been thinking of buying virtual
server or web hosting for the exchange service sometime soon, and if
the platform allows for two separate accounts, we could run the site
there too. The CMS and its database can be always copied and relocated
to a new web host if needed.
```

Email #62

Date: Sun, 08 Nov 2009 05:23:13 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux build ready for testing (attached)

To: Martti Malmi <mmalmi@cc.hut.fi>, Liberty Standard <newlibertystandard@gmail.com>

```
bitcoin-linux-0.1.6-test1.tar.bz2 attached
```

Email #63

Date: Sun, 08 Nov 2009 05:52:11 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux build ready for testing

To: Martti Malmi <mmalmi@cc.hut.fi>, Liberty Standard <newlibertystandard@gmail.com>

```
The Linux build is ready for testing on the network.  It seems solid.  I
sent the executable as an attachment in the previous e-mail, but if the
mail server didn't let it through (it's 12MB), you can download it here:
http://rapidshare.com/files/303914158/linux-0.1.6-test1.tar.bz2.html
```

Email #64

Date: Sun, 08 Nov 2009 11:50:44 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Cc: Liberty Standard <newlibertystandard@gmail.com>

Subject: Re: Linux build ready for testing

```
That's great! A major waypoint reached. Seems to work fine here.

> The Linux build is ready for testing on the network.  It seems solid.
> I sent the executable as an attachment in the previous e-mail, but if
> the mail server didn't let it through (it's 12MB), you can download it
> here:
> http://rapidshare.com/files/303914158/linux-0.1.6-test1.tar.bz2.html
```

Email #65

Date: Sun, 08 Nov 2009 18:48:27 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

```
I made a ning.com site for testing: bitcoin.ning.com. At least it's
there to get Google hits, even if we didn't use it.

> Now that the forum on bitcoin.sourceforge.net is catching on, we really
> should look for somewhere that freehosts full blown forum software.
> The bitweaver forum feature is just too lightweight.  I assume the
> "Forum" tab on the homepage can link out to wherever the forum is
> hosted.
>
> I've seen projects that have major following just from forum talk and
> pie-in-the-sky planning without even having any code yet.  Having a lot
> of forum talk gives a project more presence on the net, more search
> hits, makes it look big, draws new users in, helps solve support
> questions, hashes out what features are most of wanted.
>
> It would be a big plus if it could support SSL, at least for the login
> page if not sitewide.  Multiple people on the forum have expressed
> interest in TOR/I2P, and those users need SSL because a lot of TOR exit
> nodes are probably password scrapers run by identity thieves.  A lot of
> the core interest in Bitcoin is going to be from the privacy crowd.
>
> Any ideas where we can get a free forum?  Maybe we should look at where
> some other projects have their forums hosted for ideas where to look.
```

Email #66

Date: Sun, 08 Nov 2009 17:39:39 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
In the debug.log, it requests the block list, receives the block list,
then begins uploading the list of blocks requested.  It doesn't receive
the blocks, but it didn't run long enough for me to be sure it would
have had time yet.  Everything else looks normal.

How long did you run it?  It could take a few minutes to start
downloading the blocks.  Especially if you're on a cable modem, the
uplink can be much lower bandwidth so it would take some time to upload
the block request list.

If you run it again and it still doesn't download blocks, keep it
running for several hours at least and then send me the debug.log.  That
should give it time for my node to connect to you and I could see what
it says on my side and correlate it with your debug.log.

You're right about the minimize on close option, there's no reason that
can't be separate.  Martti originally had it separate and I made it a
sub-option, my bad.  I'll change it back.

Liberty Standard wrote:
> That is what I meant. The blocks displayed in the status bar did not
> increase at all while i ran the program. I have attached my debug.log.
>
> A good way for you to test the tray icon in Gnome is to remove the
> notification area and then add it back. If the icon is still displayed
```

> after adding the notification back, then it's working correctly.
>
> I generally set application preferences to not minimize to the tray, but
> to close to the tray. And I keep the application minimized. That way I
> don't accidentally close the program and still have the convenience of
> being able to open the application from the tray. (I don't display open
> windows in the 'task bar' but I have an icon that if clicked displays
> open windows as sub-menu items.) Then if the tray icon disappears, I go
> into the settings disable and re-enable the tray icon setting to get it
> to reappear. That's currently not possible with the bitcoin preferences
> because the close to tray check mark can not be enabled without the
> minimize to tray check box being enabled.
>
>
> On Sun, Nov 8, 2009 at 9:08 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
>   Liberty Standard wrote:
>
>   I downloaded it and it runs. It and it is using plenty of CPU,
>   so I think it's working properly. It has not downloaded
>   previously generated blocks. Is that a bug or a new feature?
>
>
>   If you mean the blocks count in the status bar isn't working its way
>   up to around 26600, then that's a bug, you should send me your
>   debug.log. (which is at ~/.bitcoin/debug.log)
>
>
>   The system tray in Gnome is not very reliable. Sometimes an icon
>   will disappear leaving no way to get back to the program. I have
>   verified that this can happen with bitcoin. It would be nice if
>   starting bitcoin while it's already running would just bring up
>   the GUI of the already running bitcoin process.
>
>
>   We haven't figured out how to find and bring up the existing running
>   program yet on Linux like it does on Windows. Given what you say, I
>   should at least turn off the minimize to tray option initially by
>   default.
>
>

Email #67

Date: Sun, 08 Nov 2009 18:48:38 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

I'm not really a fan of that type of forum layout. The thread list only fits about 4 threads on a page, posts are treated like news articles or blog posts with reply comments at the bottom. It's more of a social networking site, not really conducive to technical discussion.

I'm thinking phpBB or IPB or similar. One line of text per thread, small fonts, efficient use of vertical space. Most people are already familiar with the interface.

mmalmi@cc.hut.fi wrote:
> I made a ning.com site for testing: bitcoin.ning.com. At least it's
> there to get Google hits, even if we didn't use it.

>
>> Now that the forum on bitcoin.sourceforge.net is catching on, we really
>> should look for somewhere that freehosts full blown forum software.
>> The bitweaver forum feature is just too lightweight. I assume the
>> "Forum" tab on the homepage can link out to wherever the forum is
>> hosted.
>>
>> I've seen projects that have major following just from forum talk and
>> pie-in-the-sky planning without even having any code yet. Having a lot
>> of forum talk gives a project more presence on the net, more search
>> hits, makes it look big, draws new users in, helps solve support
>> questions, hashes out what features are most of wanted.
>>
>> It would be a big plus if it could support SSL, at least for the login
>> page if not sitewide. Multiple people on the forum have expressed
>> interest in TOR/I2P, and those users need SSL because a lot of TOR exit
>> nodes are probably password scrapers run by identity thieves. A lot of
>> the core interest in Bitcoin is going to be from the privacy crowd.
>>
>> Any ideas where we can get a free forum? Maybe we should look at where
>> some other projects have their forums hosted for ideas where to look.
>
>
>

Email #68

Date: Mon, 09 Nov 2009 01:23:59 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

Liberty Standard wrote:
> Ok, blocks have now started to increase. It definitely takes longer for
> them to start increasing than with the Windows version. Also, I think
> they might be increasing at a slower rate than in with the Windows
> version. Is there perhaps debugging enabled in the Linux build that you
> sent me? Block are increasing at about 15 blocks per second (eyeball
> estimate while looking at a clock). I didn't time how fast they
> increased in the Windows version, but it seems like it was much faster.

About how long did it take to start? It could be the node that you
happened to request from is slow. The slow start is consistent with the
slow download speed.

I'd like to look at your current debug.log file and try to understand
what's going. It might just be a really slow connection on the other
side, or maybe something's wrong and failed and retried. Taking too
long could confuse other users.

Martti, how long did it take to start downloading blocks when you ran
it, and how fast did it download?

>   When I launch bitcoin and the bitcoin port is not available, I get
>   the following messages to the command line. I don't get those
>   messages when the bitcoin port is available. Would it be possible
>   for bitcoin to pick another port if the default port is taken? The
>   same think sometimes happens to me with my BitTorrent client. When I
>   restart it, my previously open port is closed. All I have to do is
>   change the port and it starts working again.

```
>
>     /usr/lib/gio/modules/libgvfsdbus.so: wrong ELF class: ELFCLASS64
>     Failed to load module: /usr/lib/gio/modules/libgvfsdbus.so
>     /usr/lib/gio/modules/libgioremote-volume-monitor.so: wrong ELF
>     class: ELFCLASS64
>     Failed to load module:
>     /usr/lib/gio/modules/libgioremote-volume-monitor.so
>     /usr/lib/gio/modules/libgiogconf.so: wrong ELF class: ELFCLASS64
>     Failed to load module: /usr/lib/gio/modules/libgiogconf.so

It already uses SO_REUSEADDR so it can bind to the port if it's in
TIME_WAIT state after being closed.  The only time it should fail to
bind is when the program really is already running.  It's important that
two copies of Bitcoin not run on the same machine at once because they
would be modifying the database at the same time.  There is never any
need to run two on one machine as coin generation will now use multiple
processors automatically.

I'm not sure what those lib errors are, I'll do some searching.
```

Email #69

Date: Mon, 09 Nov 2009 05:42:59 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
Thanks for that, I see what happened.  Because the first one was slow,
it ended up requesting the blocks from everybody else, which only bogged
everything down.  I can fix this, I just need to think a while about the
right way.

There's no risk in shutting down while there are unconfirmed.  When you
make a transaction or new block, it immediately broadcasts it to the
network.  After that, the increasing #/confirmed number is just
monitoring the outcome.  There's nothing your node does during that time
to promote the acceptance.

Now that I think about it, when you close Bitcoin, it closes the main
window immediately but in the background continues running to finish an
orderly flush and shutdown of the database.  Before I implemented that,
it was annoying having a dead hung unresponsive window hanging around.
Until it finishes the orderly shutdown in the background, the port would
be locked, and this is an important protection to make sure another copy
can't touch the database until it's done.  I haven't seen the shutdown
take more than a few seconds.

In Wine, there's no way for the Windows version to do SO_REUSEADDR, so
that would add 60 seconds (on my system) of TIME_WAIT after the port is
closed.

If you need to transfer between two copies, you could send it to the
other's bitcoin address.  The receiving copy doesn't have to be online
at the time.

The command line to use a different data directory is
bitcoin -datadir=<directory>

For example, on Linux, the default directory is (don't use ~)
bitcoin -datadir=/home/yourusername/.bitcoin
```

You shouldn't normally have any need to use this switch. It still won't
let you run two instances at once.

Liberty Standard wrote:
> On Mon, Nov 9, 2009 at 3:23 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
>   Liberty Standard wrote:
>
>   Ok, blocks have now started to increase. It definitely takes
>   longer for them to start increasing than with the Windows
>   version. Also, I think they might be increasing at a slower rate
>   than in with the Windows version. Is there perhaps debugging
>   enabled in the Linux build that you sent me? Block are
>   increasing at about 15 blocks per second (eyeball estimate while
>   looking at a clock). I didn't time how fast they increased in
>   the Windows version, but it seems like it was much faster.
>
>
>   About how long did it take to start? It could be the node that you
>   happened to request from is slow. The slow start is consistent with
>   the slow download speed.
>
>
> It took about a half hour for it to start incrementing quickly.
> Interestingly, the CPU usage increased before it started to increment
> steadily and then lowered when it started to increment steadily.
> Although this time the block incremented to 2 within the first few
> minutes. I have not yet generated any bitcoins. I'll wait for as long as
> I have patience to generate a bitcoin, but if none are created by the
> time I lose patience, I'm going to move back to the wine version.
>
>   I'd like to look at your current debug.log file and try to
>   understand what's going. It might just be a really slow connection
>   on the other side, or maybe something's wrong and failed and
>   retried. Taking too long could confuse other users.
>
>
> I've included my current debug.log.
>
>
>   Martti, how long did it take to start downloading blocks when you
>   ran it, and how fast did it download?
>
>
>   When I launch bitcoin and the bitcoin port is not available,
>   I get
>   the following messages to the command line. I don't get those
>   messages when the bitcoin port is available. Would it be possible
>   for bitcoin to pick another port if the default port is
>   taken? The
>   same think sometimes happens to me with my BitTorrent client.
>   When I
>   restart it, my previously open port is closed. All I have to
>   do is
>   change the port and it starts working again.
>
>   /usr/lib/gio/modules/libgvfsdbus.so: wrong ELF class: ELFCLASS64
>   Failed to load module: /usr/lib/gio/modules/libgvfsdbus.so
>   /usr/lib/gio/modules/libgioremote-volume-monitor.so: wrong ELF
>   class: ELFCLASS64
>   Failed to load module:
>   /usr/lib/gio/modules/libgioremote-volume-monitor.so
>   /usr/lib/gio/modules/libgiogconf.so: wrong ELF class: ELFCLASS64

```
>            Failed to load module: /usr/lib/gio/modules/libgiogconf.so
>
>
>     It already uses SO_REUSEADDR so it can bind to the port if it's in
>     TIME_WAIT state after being closed.  The only time it should fail to
>     bind is when the program really is already running.  It's important
>     that two copies of Bitcoin not run on the same machine at once
>     because they would be modifying the database at the same time.
>      There is never any need to run two on one machine as coin
>     generation will now use multiple processors automatically.
>
>
> The reason I run two instances at the same time is to transfer bitcoins
> from one bitcoin instance to another. They of course would need to be
> accessing different data directories. Perhaps that could be specified as
> a command line argument. I currently have to move my bitcoin data folder
> to a virtual machine to do this. Shutting down bitcoin and restarting it
> with a different data directory is a poor solution because shutting down
> bitcoin while there are unconfirmed bitcoins risks losing those bitcoins.
>
> Bitcoin was definitely not running when i get the busy port error. The
> process closes quickly and reliably from my experience, but it takes
> anywhere from 30 seconds to 3 minutes (estimation from memory) for the
> port to become available again. It occurred while switching from bitcoin
> 0.1.5 in Wine to the Linux build and again while switching from the
> Linux build to bitcoin 0.1.5 in Wine.
>
> Another thing that I noticed is that the about dialog text does not fit
> correctly and it cannot be resized.
>
>     I'm not sure what those lib errors are, I'll do some searching.
>
>
```

Email #70

Date: Mon, 09 Nov 2009 10:32:08 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Cc: Liberty Standard <newlibertystandard@gmail.com>

Subject: Re: Linux build ready for testing

```
> Martti, how long did it take to start downloading blocks when you ran
> it, and how fast did it download?

Started very quickly when I got connected and downloaded quicker than
my Windows PC, which has a slower CPU.

I'll have to focus on a school project (coincidentally C++ coding) for
about a month now, so I don't have that much time for active
developing until December. Let's keep contact anyway.

> Liberty Standard wrote:
>> Ok, blocks have now started to increase. It definitely takes longer
>>  for them to start increasing than with the Windows version. Also,
>> I  think they might be increasing at a slower rate than in with the
>>  Windows version. Is there perhaps debugging enabled in the Linux
>> build that you sent me? Block are increasing at about 15 blocks per
>>  second (eyeball estimate while looking at a clock). I didn't time
>> how fast they increased in the Windows version, but it seems like
>> it was much faster.
```

>
> About how long did it take to start? It could be the node that you
> happened to request from is slow. The slow start is consistent with
> the slow download speed.
>
> I'd like to look at your current debug.log file and try to understand
> what's going. It might just be a really slow connection on the other
> side, or maybe something's wrong and failed and retried. Taking too
> long could confuse other users.
>
> Martti, how long did it take to start downloading blocks when you ran
> it, and how fast did it download?
>
>>   When I launch bitcoin and the bitcoin port is not available, I get
>>   the following messages to the command line. I don't get those
>>   messages when the bitcoin port is available. Would it be possible
>>   for bitcoin to pick another port if the default port is taken? The
>>   same think sometimes happens to me with my BitTorrent client. When I
>>   restart it, my previously open port is closed. All I have to do is
>>   change the port and it starts working again.
>>
>>   /usr/lib/gio/modules/libgvfsdbus.so: wrong ELF class: ELFCLASS64
>>   Failed to load module: /usr/lib/gio/modules/libgvfsdbus.so
>>   /usr/lib/gio/modules/libgioremote-volume-monitor.so: wrong ELF
>>   class: ELFCLASS64
>>   Failed to load module:
>>   /usr/lib/gio/modules/libgioremote-volume-monitor.so
>>   /usr/lib/gio/modules/libgiogconf.so: wrong ELF class: ELFCLASS64
>>   Failed to load module: /usr/lib/gio/modules/libgiogconf.so
>
> It already uses SO_REUSEADDR so it can bind to the port if it's in
> TIME_WAIT state after being closed. The only time it should fail to
> bind is when the program really is already running. It's important
> that two copies of Bitcoin not run on the same machine at once because
> they would be modifying the database at the same time. There is never
> any need to run two on one machine as coin generation will now use
> multiple processors automatically.
>
> I'm not sure what those lib errors are, I'll do some searching.

Email #71

Date: Mon, 09 Nov 2009 19:30:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

You really don't want to keep running in Wine, you're getting database
errors (db.log). You probably developed these rituals of transferring
to a fresh install to cope with database corruption. If there is a way
to lose unconfirmed blocks, it would have to be the database errors.
Any problems you find in the Linux build can be fixed. The Wine
incompatibility deep inside Berkeley DB is unfixable.

I think GCC 4.3.3 on the Linux build optimized the SHA-256 code better
than the old GCC 3.4.5 on Windows. When I was looking for the best
SHA-256 code, there was a lot of hand tuned highly optimized SHA1 code
available, but not so much for SHA-256 yet. I should see if I can

```
upgrade MinGW to 4.3.x to get them on a level playing field.

Liberty Standard wrote:
> Everyone that contributed to making this Linux build really did a great
> job! Thanks for the hard work. It has started maturing some bitcoins, so
> I'm going to continue to run the Linux client for the time being until I
> decide whether it's at least as good or better at generating coins than
> the Windows version running in Wine.
>
>
> On Mon, Nov 9, 2009 at 8:59 AM, Liberty Standard
> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>> wrote:
>
>     Another instance when I would like to run multiple instances is when
>     I upgrade bitcoin. I will uncheck the generate coin check box in the
>     outdated bitcoin, launch and start generating coins in the new
>     bitcoin using a separate data directory, then when the old
>     application's coins have matured I will send them to the new
>     application and then close the old application. I prefer do do clean
>     installs rather than upgrading while maintaining old data.
>
>
>
>     On Mon, Nov 9, 2009 at 7:42 AM, Satoshi Nakamoto <satoshin@gmx.com
>     <mailto:satoshin@gmx.com>> wrote:
>
>         Thanks for that, I see what happened.  Because the first one was
>         slow, it ended up requesting the blocks from everybody else,
>         which only bogged everything down.  I can fix this, I just need
>         to think a while about the right way.
>
>         There's no risk in shutting down while there are unconfirmed.
>          When you make a transaction or new block, it immediately
>         broadcasts it to the network.  After that, the increasing
>         #/confirmed number is just monitoring the outcome.  There's
>         nothing your node does during that time to promote the acceptance.
>
```

Email #72

Date: Mon, 09 Nov 2009 19:41:11 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux build ready for testing

To: mmalmi@cc.hut.fi

Cc: Liberty Standard <newlibertystandard@gmail.com>

```
You got a lot done with the Linux build, autostart, minimize to tray,
setup and everything, it's really appreciated.  Good luck on your C++
project.

mmalmi@cc.hut.fi wrote:
> I'll have to focus on a school project (coincidentally C++ coding) for
> about a month now, so I don't have that much time for active developing
> until December. Let's keep contact anyway.
>
```

Email #73

Date: Tue, 10 Nov 2009 16:46:04 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux - dead sockets problem

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

I see what happened. All your sockets went dead somehow. You had no communication with the network, but because you had 8 zombie connections, it thought it was still online and kept generating blocks.

  You can tell this is happening when your blocks are numbered sequentially, without other people's blocks interspersed, like:

2/unconfirmed
3/unconfirmed
4/unconfirmed
5/unconfirmed
6 blocks
7 blocks

It's implausible that you would be the only one to find blocks for 6 blocks in a row like that.

When you exited and restarted, it connected and downloaded 45 blocks that the network found in your absence. Since your blocks were not broadcast to the network immediately, the network went on without them.

It sounds like you had exactly the same problem on Wine. There's clearly something about socket handling on Linux that's effecting it either way.

I'll start researching this. Ultimately if I can't find the root of the problem, I'll have to make some kind of mechanism to watch for an absence of messages and disconnect. The only workaround for you right now would be to exit and restart more often.

All but one of your node connections went dead at the same time, one shortly after. IRC was still working, so it wasn't that you were offline from the internet.

I wonder if the status of blocks should say "#/unconfirmed" all the way up to maturity (119/unconfirmed then 120 blocks) instead. The meaning of the number isn't as strong for blocks as for transactions.

I think it would be an improvement not to count one's own blocks as confirmations. A drawback would be that the status numbers shown by different nodes would not match. The status number would no longer be coordinated with the maturity countdown on blocks either. A lighter option would be a special case only if all confirmations are your own.

Liberty Standard wrote:

> I just lost 6 sets of maturing coins! I had 10 sets of bitcoins
> maturing. The last set was generated at about 0:22. It got to
> 2/unconfirmed before bitcoin got stuck. At 10:10, the bitcoin which was
> generated at 0:22 was still only at 2/unconfirmed. Since you had told me
> that I wasn't going to lose coins, I shutdown and restarted bitcoin. On
> the bright side, it shutdown and started up very smoothly. But
> unfortunately, when the blocks updated, I lost 6 sets of bitcoins. Four
> sets were still unconfirmed, but two sets were confirmed. And there's no
> trace of them now. Perhaps now that you have the 'Show Generated Coins'
> option available, you can put back in failed bitcoin generations. I just
> don't like that those bitcoins just disappeared into thin air. I'm still
> running the Linux build at the moment, but the Wine version is suddenly
> looking much more attractive now that 6 out of the 10 sets of bitcoins I
> generated in the past 24 hours just vanished. I've included my debug.log.
>
>
> On Tue, Nov 10, 2009 at 1:45 AM, Liberty Standard

```
> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>> wrote:
>
>     The Linux build has generated a decent amount of bitcoins within the
>     past 20 hours and I trust what you're telling me about database
>     errors, so all signs point toward me running the Linux build from
>     now on. The only half annoying thing about the Linux build is that
>     my computer's fan has gone from 50% to 100%. :-P I know I can limit
>     the CPU, so if it gets on my nerves too much and if I can live with
>     less bitcoins being generated, perhaps I'll do that. Or maybe I just
>     need to start listening to more music...
>
...
>
>                    There's no risk in shutting down while there are
>             unconfirmed.
>                     When you make a transaction or new block, it immediately
>                    broadcasts it to the network.  After that, the increasing
>                    #/confirmed number is just monitoring the outcome.
>              There's
>                    nothing your node does during that time to promote
>             the acceptance.
>
>
>
```

Email #74

Date: Wed, 11 Nov 2009 00:39:19 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux - linux-0.1.6-test2

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
I fixed a few places I found where it was possible for a socket to get
an error and not get disconnected.  If your connections go dead again,
it should disconnect and reconnect them.  I also implemented an
inactivity timeout as a fallback.

This also includes a partial fix for the slow initial block download.

You should run with the "-debug" switch to get some additional debug.log
information I added that'll help if there are more problems.

linux-0.1.6-test2.tar.bz2  12,134,012 bytes
Download:
http://rapidshare.com/files/305231818/linux-0.1.6-test2.tar.bz2.html


Satoshi Nakamoto wrote:
> I see what happened.  All your sockets went dead somehow.  You had no
> communication with the network, but because you had 8 zombie
> connections, it thought it was still online and kept generating blocks.
>  You can tell this is happening when your blocks are numbered
> sequentially, without other people's blocks interspersed, like:
> 2/unconfirmed
> 3/unconfirmed
> 4/unconfirmed
> 5/unconfirmed
> 6 blocks
> 7 blocks
>
```

> It's implausible that you would be the only one to find blocks for 6
> blocks in a row like that.
>
> When you exited and restarted, it connected and downloaded 45 blocks
> that the network found in your absence. Since your blocks were not
> broadcast to the network immediately, the network went on without them.
>
> It sounds like you had exactly the same problem on Wine. There's
> clearly something about socket handling on Linux that's effecting it
> either way.
>
> I'll start researching this. Ultimately if I can't find the root of the
> problem, I'll have to make some kind of mechanism to watch for an
> absence of messages and disconnect. The only workaround for you right
> now would be to exit and restart more often.
>
> All but one of your node connections went dead at the same time, one
> shortly after. IRC was still working, so it wasn't that you were
> offline from the internet.
>
> I wonder if the status of blocks should say "#/unconfirmed" all the way
> up to maturity (119/unconfirmed then 120 blocks) instead. The meaning
> of the number isn't as strong for blocks as for transactions.
>
> I think it would be an improvement not to count one's own blocks as
> confirmations. A drawback would be that the status numbers shown by
> different nodes would not match. The status number would no longer be
> coordinated with the maturity countdown on blocks either. A lighter
> option would be a special case only if all confirmations are your own.
>
> Liberty Standard wrote:
>> I just lost 6 sets of maturing coins! I had 10 sets of bitcoins
>> maturing. The last set was generated at about 0:22. It got to
>> 2/unconfirmed before bitcoin got stuck. At 10:10, the bitcoin which
>> was generated at 0:22 was still only at 2/unconfirmed. Since you had
>> told me that I wasn't going to lose coins, I shutdown and restarted
>> bitcoin. On the bright side, it shutdown and started up very smoothly.
>> But unfortunately, when the blocks updated, I lost 6 sets of bitcoins.
>> Four sets were still unconfirmed, but two sets were confirmed. And
>> there's no trace of them now. Perhaps now that you have the 'Show
>> Generated Coins' option available, you can put back in failed bitcoin
>> generations. I just don't like that those bitcoins just disappeared
>> into thin air. I'm still running the Linux build at the moment, but
>> the Wine version is suddenly looking much more attractive now that 6
>> out of the 10 sets of bitcoins I generated in the past 24 hours just
>> vanished. I've included my debug.log.
>>
>>
>> On Tue, Nov 10, 2009 at 1:45 AM, Liberty Standard
>> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>>
>> wrote:
>>
>>   The Linux build has generated a decent amount of bitcoins within the
>>   past 20 hours and I trust what you're telling me about database
>>   errors, so all signs point toward me running the Linux build from
>>   now on. The only half annoying thing about the Linux build is that
>>   my computer's fan has gone from 50% to 100%. :-P I know I can limit
>>   the CPU, so if it gets on my nerves too much and if I can live with
>>   less bitcoins being generated, perhaps I'll do that. Or maybe I just
>>   need to start listening to more music...
>>
> ...
>>
>>   There's no risk in shutting down while there are

```
>>             unconfirmed.
>>                     When you make a transaction or new block, it
>> immediately
>>                     broadcasts it to the network.  After that, the
>> increasing
>>                     #/confirmed number is just monitoring the outcome.
>>              There's
>>                     nothing your node does during that time to promote
>>             the acceptance.
>>
>>
>>
>
>
```

Email #75

Date: Wed, 11 Nov 2009 00:41:06 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux - linux-0.1.6-test2 attachment

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
linux-0.1.6-test2.tar.bz2 attached
```

Email #76

Date: Thu, 12 Nov 2009 05:36:06 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux - linux-0.1.6-test3

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
Right now (04:50 GMT) my node is connecting to yours and getting zombie
connections each time.  The socket isn't returning an error, just zombie
without notice.  If you're running the linux build right now, it would
be interesting to see what the log says on your side.

test3:

I've added specific code to detect zombie sockets.  It'll detect if the
socket hasn't sent or received any data within 60 seconds of connecting,
and detect if data is queued to send and hasn't sent for 3 minutes.

I think I may have weakened the reconnect speed in test2.  In test3 I'm
making it more determined to reconnect quickly.

I added checking to track whether other nodes received your generated
blocks.  If none did, it'll warn you in the description:
"Generated - Warning: This block was not received by any other nodes and
will probably not be accepted!"

The status can go to "#/offline?" for blocks or transactions you create
if they don't get out to any other nodes.

With all this, it should be impossible not to notice as soon as it
screws up.  It should hopefully disconnect all the zombie sockets.
After that, whether it's able to make some good connections, or sockets
is completely hosed and it stays at 0 connections, I don't know.
```

If this doesn't work, I guess I'll look at the sourcecode of some other P2P apps like BitTorrent and see how they deal with this stuff. Maybe there's some magic flag or procedure to bash the sockets system back to life.

File linux-0.1.6-test3.tar.bz2 attached in the next message.

Liberty Standard wrote:
> On Wed, Nov 11, 2009 at 8:08 AM, Liberty Standard
> <newlibertystandard@gmail.com <mailto:newlibertystandard@gmail.com>> wrote:
>
> My network connection is direct to my computer. My ISP requires that
> I run VPN to connect to the Internet. I then have a second NIC that
> shares my Internet with other devices. My IP address while using my
> computer is my actual IP address, but the devices connected through
> my second NIC use NAT. When I connect through a virtual machine,
> that also uses NAT. All this requires very little configuration.
> NetworkManager in Ubuntu has an option to share my Internet
> connection through the second NIC and VirtualBox has the option to
> use NAT.
>
> I lost a couple packs of bitcoins again, so that problem is not yet
> fixed. It's a bit more bearable now that I have an idea of what is
> going on. I figure for now I'll just restart bitcoin whenever I see
> a pack of bitcoins starting to mature. I may go back and forth a bit
> between Linux and Wine, but I'll definitely test every new version
> that comes out. At the moment I'm still running the Linux build.
>
>
>
> On Wed, Nov 11, 2009 at 7:49 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
> Thanks. The log didn't stop on anything special, just simple
> message passing. Chances are it's UI related. Most of the
> initial bugs were all UI.
>
> What brand/model of firewall do you have? It's possible for
> BitTorrent to overwhelm the number of connections some models
> can handle. Most are underpowered and flaky under load.
>
> NewLibertyStandard wrote:
>
> I have been getting your attachments just fine. I just
> thought I'd spare Martti the large attachment.
>
> I am not able to reproduce the bug. I don't know whether the
> paste, the blocks finishing, a combination of the two or
> something else entirely caused the fault.
>
> ...
>
> But after they started
> downloading, I took a look a look at my BitTorrent
> client, and
> sure enough, I had forgotten about a torrent and my
> upload was
> quite high, at the limit I had set for it.
>
>
>
>
>
>

Email #77

Date: Thu, 12 Nov 2009 05:37:58 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: linux-0.1.6-test3.tar.bz2 attached
To: Liberty Standard <newlibertystandard@gmail.com>
Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
File linux-0.1.6-test3.tar.bz2 attached

linux-0.1.6-test3.tar.bz2   12,143,473 bytes
```

Email #78

Date: Thu, 12 Nov 2009 23:39:44 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: linux-0.1.6-test5 fix for zombie sockets
To: Liberty Standard <newlibertystandard@gmail.com>
Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
test 5:

I added MSG_DONTWAIT to the send and recv calls in case they forgot the
socket is non-blocking.  If that doesn't work, there's now the catch-all
solution: another thread monitors the send/recv thread and terminates
and restarts it if it stops.  It prints "*** Restarting
ThreadSocketHandler ***" in debug.log, and an error message displays on
the status bar for a while.

Before terminating, it tries closing the socket that's hung.  If that
works, it doesn't have to resort to terminating.

I ran a test where it terminated the thread about 1000 times without
trouble, so it should be safe.  The terminate on linux is
pthread_cancel, which throws it into C++'s exception handler.

The thread calls we were using didn't have terminate, so I created our
own wrappers in util.h to use CreateThread on windows and pthread_create
on linux, instead of:
   _beginthread is windows only and lacks terminate
   boost::thread is really attractive, but lacks terminate
   wxThread requires you to create a class for every function you might
call (yuck)

File attached in the next e-mail
```

Email #79

Date: Thu, 12 Nov 2009 23:42:29 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: linux-0.1.6-test5.tar.bz2 attached
To: Liberty Standard <newlibertystandard@gmail.com>
Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
12,033,918 linux-0.1.6-test5.tar.bz2
```

Email #80

Date: Sat, 14 Nov 2009 05:46:22 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Zetaboards forum

To: Martti Malmi <mmalmi@cc.hut.fi>

```
I created a forum on Zetaboards, InvisionFree's new site that they're
migrating to.

http://s1.zetaboards.com/Bitcoin/index/

I made an admin account you can use to upgrade your own account to admin:
u: admin
pw: B98VzUUA

BTW, the admin pages have a huge blank space at the top, you have to
scroll down.

It doesn't support SSL, but none of them do.  I replaced the ugly
default orange and blue theme with the Frostee theme, which was the only
decent looking theme I could find after extensive searching.  Searching
for themes is futile, there are thousands of rubbish themes.  It turns
out the solution is to look at button sets instead
(http://resources.zetaboards.com/forum/1000328/)

I only created two subforums to begin with.  I'll create new ones as the
need arises.  I like to start with a flat namespace until there's enough
items to justify subsections.  Technical Support makes sense as a
separate section to get that stuff out of the main spotlight so our
dirty laundry isn't in everyone's face, and to make people feel more
free to report bugs there.  Mostly only devs and people checking on a
bug need read the Technical Support section.
```

Email #81

Date: Sun, 15 Nov 2009 15:40:29 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Linux update

To: Martti Malmi <mmalmi@cc.hut.fi>

```
linux-0.1.6-test5 solved Liberty's zombie socket problem.  The
MSG_DONTWAIT fixed the root cause, it's not having to terminate and
restart the thread.  The sockets are marked non-blocking already, so I
don't understand why.  Maybe it forgot.  I suppose if a socket fails and
the OS closes it then there's nothing left to remember it was
non-blocking, but then accessing a closed handle should return
immediately with an error.  There's no MSG_DONTWAIT on Windows, marking
the socket as nonblocking is the only way, so if anyone runs the Windows
version in Wine it will have to rely on terminating the thread.

The only problem now is the DB exceptions he's getting.
**********
EXCEPTION: 11DbException
Db::open: Bad file descriptor
bitcoin in ThreadMessageHandler()
**********
EXCEPTION: 11DbException
Db::close: Bad file descriptor
bitcoin in ThreadMessageHandler()
```

I had expected those to be a Wine problem, but he's getting them on
Linux just the same. He tried moving the datadir to a different drive,
no help. I've never gotten them. I'm running a stress test that
continuously generates a lot of activity and DB access and never got it.

He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
difference. Is your Linux machine 64-bit or 32-bit? Have you ever had
a DB exception? (see db.log also) Now that the zombie problem is fixed
in test5, could you start running it on your Linux machine? We could
use a 3rd vote to get a better idea of what we're dealing with here.
The DB exception is uncaught, so it'll stop the program if you get it.

BTW, zetaboards insists on displaying "Member #", so you better sign up
soon and grab a good account number.

Email #82

Date: Sun, 15 Nov 2009 19:55:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux update

The program terminated a few times with the same error in debug.log
close: Bad file descriptor
blkindex.dat: Bad file descriptor

I'm running a 64-bit Ubuntu distribution.

> The only problem now is the DB exceptions he's getting.
> ************************
> EXCEPTION: 11DbException
> Db::open: Bad file descriptor
> bitcoin in ThreadMessageHandler()
> ************************
> EXCEPTION: 11DbException
> Db::close: Bad file descriptor
> bitcoin in ThreadMessageHandler()
>
> I had expected those to be a Wine problem, but he's getting them on
> Linux just the same. He tried moving the datadir to a different drive,
> no help. I've never gotten them. I'm running a stress test that
> continuously generates a lot of activity and DB access and never got it.
>
> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
> difference. Is your Linux machine 64-bit or 32-bit? Have you ever had
> a DB exception? (see db.log also) Now that the zombie problem is fixed
> in test5, could you start running it on your Linux machine? We could
> use a 3rd vote to get a better idea of what we're dealing with here.
> The DB exception is uncaught, so it'll stop the program if you get it.
>
> BTW, zetaboards insists on displaying "Member #", so you better sign up
> soon and grab a good account number.

Email #83

Date: Sun, 15 Nov 2009 19:15:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux update

To: mmalmi@cc.hut.fi

I'd better install 64-bit then. I imagine it's something about the

```
32-bit version of Berkeley DB on 64-bit Linux.

BTW, in things like the feature list credits, do you want me to refer to
you as sirius-m or Martti Malmi?  I think most projects go by real names
for consistency.

mmalmi@cc.hut.fi wrote:
> The program terminated a few times with the same error in debug.log from
> Db::close. Db.log has:
>
> close: Bad file descriptor
> blkindex.dat: Bad file descriptor
>
> I'm running a 64-bit Ubuntu distribution.
>
>> The only problem now is the DB exceptions he's getting.
>> ************************
>> EXCEPTION: 11DbException
>> Db::open: Bad file descriptor
>> bitcoin in ThreadMessageHandler()
>> ************************
>> EXCEPTION: 11DbException
>> Db::close: Bad file descriptor
>> bitcoin in ThreadMessageHandler()
>>
>> I had expected those to be a Wine problem, but he's getting them on
>> Linux just the same.  He tried moving the datadir to a different drive,
>> no help.  I've never gotten them.  I'm running a stress test that
>> continuously generates a lot of activity and DB access and never got it.
>>
>> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
>> difference.  Is your Linux machine 64-bit or 32-bit?  Have you ever had
>> a DB exception? (see db.log also)  Now that the zombie problem is fixed
>> in test5, could you start running it on your Linux machine?  We could
>> use a 3rd vote to get a better idea of what we're dealing with here.
>> The DB exception is uncaught, so it'll stop the program if you get it.
>>
>> BTW, zetaboards insists on displaying "Member #", so you better sign up
>> soon and grab a good account number.
>
```

Email #84

Date: Sun, 15 Nov 2009 22:05:50 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux update

```
Perhaps the real name is better.

Another name question: I've been thinking of a name for the exchange
service, and I came up with Bitcoin X (bitcoinx.com) and Bitcoin Shop
(bitcoinshop.com). Which one do you find better?

> I'd better install 64-bit then.  I imagine it's something about the
> 32-bit version of Berkeley DB on 64-bit Linux.
>
> BTW, in things like the feature list credits, do you want me to refer
> to you as sirius-m or Martti Malmi?  I think most projects go by real
> names for consistency.
>
> mmalmi@cc.hut.fi wrote:
```

```
>> The program terminated a few times with the same error in debug.log
>>  from Db::close. Db.log has:
>>
>> close: Bad file descriptor
>> blkindex.dat: Bad file descriptor
>>
>> I'm running a 64-bit Ubuntu distribution.
>>
>>> The only problem now is the DB exceptions he's getting.
>>> ************************
>>> EXCEPTION: 11DbException
>>> Db::open: Bad file descriptor
>>> bitcoin in ThreadMessageHandler()
>>> ************************
>>> EXCEPTION: 11DbException
>>> Db::close: Bad file descriptor
>>> bitcoin in ThreadMessageHandler()
>>>
>>> I had expected those to be a Wine problem, but he's getting them on
>>> Linux just the same.  He tried moving the datadir to a different drive,
>>> no help.  I've never gotten them.  I'm running a stress test that
>>> continuously generates a lot of activity and DB access and never got it.
>>>
>>> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
>>> difference.  Is your Linux machine 64-bit or 32-bit?  Have you ever had
>>> a DB exception? (see db.log also)  Now that the zombie problem is fixed
>>> in test5, could you start running it on your Linux machine?  We could
>>> use a 3rd vote to get a better idea of what we're dealing with here.
>>> The DB exception is uncaught, so it'll stop the program if you get it.
>>>
>>> BTW, zetaboards insists on displaying "Member #", so you better sign up
>>> soon and grab a good account number.
>>
```

Email #85

Date: Sun, 15 Nov 2009 20:25:26 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Linux update

To: mmalmi@cc.hut.fi

```
At first glance, bitcoinshop.com looks better.  bitcoinexchange.com
might be better than bitcoinx.com.

Be careful where you search domain names, many will front-run you.  Even
network solutions, although they've said they won't if you use their
whois page not the homepage.  The only safe place is
http://www.internic.com/whois.html

mmalmi@cc.hut.fi wrote:
> Perhaps the real name is better.
>
> Another name question: I've been thinking of a name for the exchange
> service, and I came up with Bitcoin X (bitcoinx.com) and Bitcoin Shop
> (bitcoinshop.com). Which one do you find better?
>
>> I'd better install 64-bit then.  I imagine it's something about the
>> 32-bit version of Berkeley DB on 64-bit Linux.
>>
>> BTW, in things like the feature list credits, do you want me to refer
```

```
>> to you as sirius-m or Martti Malmi?  I think most projects go by real
>> names for consistency.
>>
>> mmalmi@cc.hut.fi wrote:
>>> The program terminated a few times with the same error in debug.log
>>>  from Db::close. Db.log has:
>>>
>>> close: Bad file descriptor
>>> blkindex.dat: Bad file descriptor
>>>
>>> I'm running a 64-bit Ubuntu distribution.
>>>
>>>> The only problem now is the DB exceptions he's getting.
>>>> ************************
>>>> EXCEPTION: 11DbException
>>>> Db::open: Bad file descriptor
>>>> bitcoin in ThreadMessageHandler()
>>>> ************************
>>>> EXCEPTION: 11DbException
>>>> Db::close: Bad file descriptor
>>>> bitcoin in ThreadMessageHandler()
>>>>
>>>> I had expected those to be a Wine problem, but he's getting them on
>>>> Linux just the same.  He tried moving the datadir to a different drive,
>>>> no help.  I've never gotten them.  I'm running a stress test that
>>>> continuously generates a lot of activity and DB access and never got
>>>> it.
>>>>
>>>> He has Ubuntu 64-bit and I have 32-bit, so I'm assuming that's the
>>>> difference.  Is your Linux machine 64-bit or 32-bit?  Have you ever had
>>>> a DB exception? (see db.log also)  Now that the zombie problem is fixed
>>>> in test5, could you start running it on your Linux machine?  We could
>>>> use a 3rd vote to get a better idea of what we're dealing with here.
>>>> The DB exception is uncaught, so it'll stop the program if you get it.
>>>>
>>>> BTW, zetaboards insists on displaying "Member #", so you better sign up
>>>> soon and grab a good account number.
>>>
>
>
>
```

Email #86

Date: Mon, 16 Nov 2009 06:20:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Db::open/Db::close "Bad file descriptor" exception

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
I have an idea for a workaround, but it depends on what files the errors
are on.  If you've accumulated several errors in db.log, could you send
it to me? (even if it's rather simple and boring)  Is the file listed
always blkindex.dat, or does it include addr.dat or wallet.dat too?

Liberty Standard wrote:
> I moved the data directory back to my SSD card and started bitcoin test
> 6. It encountered a segmentation fault today with Db::open in the log. I
> had changed the settings to only use one processor/core while I watched
> a 720p mkv movie. I noticed the segmentation fault after the film had ended.
>
```

```
> On Sun, Nov 15, 2009 at 12:45 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
>     Here's one where I linked Berkeley DB a different way.  It's worth a
>     try.  Otherwise identical to test5.
>
>     (Keep the datadir on the hard drive at least until you get it to
>     fail the same way there.  That has a fair chance of success.)
>
>
```

Email #87

Date: Mon, 16 Nov 2009 19:19:26 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Forum

```
I installed a TikiWiki on my VPS at 174.143.149.98. SSL is currently
enabled with a self-signed certificate. Admin password is the same as
in the Bitweaver. How about using this as the site platform? Maybe we
can make bitcoin.org or at least bitcoin.sf.net point there?
```

Email #88

Date: Mon, 16 Nov 2009 19:34:56 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

```
mmalmi@cc.hut.fi wrote:
> I installed a TikiWiki on my VPS at 174.143.149.98. SSL is currently
> enabled with a self-signed certificate. Admin password is the same as in
> the Bitweaver. How about using this as the site platform? Maybe we can
> make bitcoin.org or at least bitcoin.sf.net point there?

What do you see as the benefits of switching the wiki?
Some I can think of:
  SSL
  get away from sourceforge's unreliable hosting
  everything not logged by sourceforge

The forum feature is about as weak as bitweaver.  We need a full blown
forum software for that.

My priority right now is to get a forum going, either phpBB or similar.
  What do you think of the zetaboards option?  Should we go ahead with that?
```

Email #89

Date: Mon, 16 Nov 2009 22:11:24 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

```
> What do you see as the benefits of switching the wiki?
> Some I can think of:
>  SSL
```

> get away from sourceforge's unreliable hosting
> everything not logged by sourceforge

I think the biggest advantage is having a single site so you don't need a separate account for the wiki and the forum, and the functionalities are also nicely integrated with the main site itself. Also being ad-free is a plus.

> The forum feature is about as weak as bitweaver. We need a full blown
> forum software for that.

How about Drupal's forum functionality? Address: https://174.143.149.98/drupal/. The CMS in general looks better and simpler than TikiWiki. If the forum's not good enough, then we can of course use a specialized forum software like phpBB.

> My priority right now is to get a forum going, either phpBB or similar.
> What do you think of the zetaboards option? Should we go ahead with
> that?

Otherwise fine, but the ads and the lack of SSL are a minus.

Email #90

Date: Mon, 16 Nov 2009 21:10:22 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

That's a good idea to go in a more web-publishing CMS type direction like Drupal. That's a better fit and can produce a better looking website than a wiki. I think I was wrong about wiki. Only a few specific people will do any website design work and those people can go ahead and have a separate login. In that case, login integration with the forum doesn't matter much. For security, I'd almost rather have a different login than be constantly checking the forum with the same login that could pwn the website.

Drupal's forum is less bad than the wikis, but still a long way from something I would want to use.

zetaboards pros and cons:

pros:
- we don't have to worry about bandwidth
- they handle the backend management and security patches

con:
- lack of SSL
- lack of privacy, everything is logged
- lack of control over the php code for customization
- no CAPTCHA, and if they add one later it might be unacceptable flash
- ads (could pay to get rid of them later if we care enough)
- there's always the risk they abruptly cancel the site for some petty reason

mmalmi@cc.hut.fi wrote:
>> What do you see as the benefits of switching the wiki?
>> Some I can think of:
>> SSL
>> get away from sourceforge's unreliable hosting

```
>>  everything not logged by sourceforge
>
> I think the biggest advantage is having a single site so you don't need
> a separate account for the wiki and the forum, and the functionalities
> are also nicely integrated with the main site itself. Also being ad-free
> is a plus.
>
>> The forum feature is about as weak as bitweaver.  We need a full blown
>> forum software for that.
>
> How about Drupal's forum functionality? Address:
> https://174.143.149.98/drupal/. The CMS in general looks better and
> simpler than TikiWiki. If the forum's not good enough, then we can of
> course use a specialized forum software like phpBB.
>
>> My priority right now is to get a forum going, either phpBB or similar.
>>  What do you think of the zetaboards option?  Should we go ahead with
>> that?
>
> Otherwise fine, but the ads and the lack of SSL are a minus.
>
```

Email #91

Date: Tue, 17 Nov 2009 03:41:26 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: linux-0.1.6-test7

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

```
test 7:

Backup your data directory before running this, just in case.

Workaround for the Db::open/Db::close "Bad file descriptor" exception.
Might also make the initial block download faster.  The workaround is to
open the database handles and keep them open for the duration of the
program, which is actually the more common thing to do anyway.  If we're
not closing and opening all the time, the error shouldn't get a chance
to happen.

The one exception is wallet.dat, which I still close after writing is
finished so I can flush the transaction logs into the dat file, making
the dat file standalone.  That way if someone does a backup while
Bitcoin is running, they'll get a wallet.dat that is valid by itself
without the database transaction logs.

This is a restructuring of the database handling, so we might find some
new deadlocks.  Usually if it deadlocks, either the UI will stop
repainting, or it'll stop using CPU even though it still says Generating.
```

Email #92

Date: Tue, 17 Nov 2009 16:57:26 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

```
mmalmi@cc.hut.fi wrote:
> How about Drupal's forum functionality? Address:
```

> https://174.143.149.98/drupal/. The CMS in general looks better and
> simpler than TikiWiki. If the forum's not good enough, then we can of
> course use a specialized forum software like phpBB.

Another issue I thought of with zetaboards: most free forum sites won't
let you export the user account database if you want to move. I don't
know why I don't see any other software projects using a free forum, but
I have to assume there might be a reason we would discover later.

If you can install phpBB3 on your VPS, that's probably the better option.

 From what I've seen on other forums, if the cost of bandwidth becomes
an issue, a small Google Adwords (text links) at the top generates more
than the cost of bandwidth even for very low value traffic like gaming.
  This would be much higher value traffic well targeted for high paying
gold merchant keywords and VPN hosts. It could eventually be a valuable
revenue stream you wouldn't want to give away to some free site.

I want to pre-announce some of the features in version 0.2 on the forum
and try to get some anticipation going. Even if hardly anyone else is
posting, I have seen project forums where most of the posts are the
author announcing what's going on with the latest changes. Users can
see progress going on, see that it's improving and supported and not
abandonware. It's a little like a blog in that case, but easier for
users to use it as a searchable FAQ and better organized. Whenever I
google search software questions, most of the hits are forum posts.

Email #93

Date: Wed, 18 Nov 2009 03:31:39 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

I installed both phpBB3 and Simple Machines Forum, which are kind of
the market leaders among the open source forums. SMF's interface looks
better on the first look, especially the admin panel. What do you
think, shall we go with SMF or phpBB3?

Email #94

Date: Wed, 18 Nov 2009 03:50:24 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Db::open/Db::close "Bad file descriptor" exception

Here's the logs in case they're still useful.

> I have an idea for a workaround, but it depends on what files the
> errors are on. If you've accumulated several errors in db.log, could
> you send it to me? (even if it's rather simple and boring) Is the file
> listed always blkindex.dat, or does it include addr.dat or wallet.dat
> too?

Email #95

Date: Wed, 18 Nov 2009 04:35:32 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: linux-0.1.6-test7

To: Liberty Standard <newlibertystandard@gmail.com>

Cc: Martti Malmi <mmalmi@cc.hut.fi>

Finally an easy one. I see a way that could happen on a long operation such as the initial download. The TryLock bug is unrelated to the db stuff. Fix will be in test8.

I've been able to reproduce the db::open/close exception 3 times now on 32-bit linux by hitting it with a continuous flood of non-stop requests. It looks like even periodically closing the wallet.dat database to flush it gets the db::close exceptions. I'm disabling the wallet flush feature on Linux. On Linux we'll never close a database handle until we're ready to exit. So far with this disabled, no exceptions.

I'm also implementing the orderly initial block download. Instead of naively requesting all the blocks at once, it'll request batches of 500 at a time. This way, it'll receive the blocks before the retry timeout, so it shouldn't go requesting it from other nodes unless it actually doesn't receive them or it's too slow. The change is in the requestee's side, so this functionality won't be visible until your initial block download is coming from a node that has the new version.

I'm going to test this some more before sending test8.

Liberty Standard wrote:
> I started with a fresh data directory with test7. Blocks started to
> download much faster. It only took about 15 seconds where it took a few
> minutes previously with the Linux build. It crashed once while it was
> downloading blocks with the following message in the terminal.
>
> ../include/wx/thrimpl.cpp(50): assert "m_internal" failed in TryLock():
> wxMutex::TryLock(): not initialized [in child thread]
> Trace/breakpoint trap
>
> I've included my log file, but I forgot to back it up before restarting
> bitcoin, so I'm not sure at what point in the log file the crash occurred.
>
> Fortunately I haven't encountered the segmentation fault yet. The
> frequency of segmentation faults in the previous builds varied quite a
> bit, so I'll keep running it and let you know if i run into any problems.
>
>
>
> On Tue, Nov 17, 2009 at 5:41 AM, Satoshi Nakamoto <satoshin@gmx.com
> <mailto:satoshin@gmx.com>> wrote:
>
>   test 7:
>
>   Backup your data directory before running this, just in case.
>
>   Workaround for the Db::open/Db::close "Bad file descriptor"
>   exception. Might also make the initial block download faster. The
>   workaround is to open the database handles and keep them open for
>   the duration of the program, which is actually the more common thing
>   to do anyway. If we're not closing and opening all the time, the
>   error shouldn't get a chance to happen.
>
>   The one exception is wallet.dat, which I still close after writing
>   is finished so I can flush the transaction logs into the dat file,
>   making the dat file standalone. That way if someone does a backup
>   while Bitcoin is running, they'll get a wallet.dat that is valid by
>   itself without the database transaction logs.

```
>
>     This is a restructuring of the database handling, so we might find
>     some new deadlocks.  Usually if it deadlocks, either the UI will
>     stop repainting, or it'll stop using CPU even though it still says
>     Generating.
>
>
```

Email #96

Date: Wed, 18 Nov 2009 05:14:45 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Db::open/Db::close "Bad file descriptor" exception

To: mmalmi@cc.hut.fi

```
Thanks.  The db::open/close errors confirm the pattern.

More interesting is the zombie sockets activity towards the end, and the
socket thread monitor tripped but didn't get it going again.  Was the
machine disconnected from the net?  MSG_DONTWAIT in test5 solved the
zombie problem for Liberty.  What test version were you running?  (I
should print the test version in the log)

mmalmi@cc.hut.fi wrote:
> Here's the logs in case they're still useful.
>
>> I have an idea for a workaround, but it depends on what files the
>> errors are on.  If you've accumulated several errors in db.log, could
>> you send it to me? (even if it's rather simple and boring)  Is the file
>> listed always blkindex.dat, or does it include addr.dat or wallet.dat
>> too?
>
```

Email #97

Date: Wed, 18 Nov 2009 05:32:22 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Forum

To: mmalmi@cc.hut.fi

```
That's great, this is going to fun!  I'll research what people say about
the two.

mmalmi@cc.hut.fi wrote:
> I installed both phpBB3 and Simple Machines Forum, which are kind of
> the market leaders among the open source forums. SMF's interface looks
> better on the first look, especially the admin panel. What do you
> think, shall we go with SMF or phpBB3?
>
>
```

Email #98

Date: Wed, 18 Nov 2009 21:32:15 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Db::open/Db::close "Bad file descriptor" exception

I think it was test version 5, not completely sure though. I'm running
the Linux version on a laptop which I move between different locations
and use the hibernate-feature instead of powering down.

> Thanks. The db::open/close errors confirm the pattern.
>
> More interesting is the zombie sockets activity towards the end, and
> the socket thread monitor tripped but didn't get it going again. Was
> the machine disconnected from the net? MSG_DONTWAIT in test5 solved
> the zombie problem for Liberty. What test version were you running?
> (I should print the test version in the log)
>
> mmalmi@cc.hut.fi wrote:
>> Here's the logs in case they're still useful.
>>
>>> I have an idea for a workaround, but it depends on what files the
>>> errors are on. If you've accumulated several errors in db.log, could
>>> you send it to me? (even if it's rather simple and boring) Is the file
>>> listed always blkindex.dat, or does it include addr.dat or wallet.dat
>>> too?
>>

Email #99

Date: Fri, 20 Nov 2009 05:14:56 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: SMF forum, need a mod installed

To: Martti Malmi <mmalmi@cc.hut.fi>

I've been configuring the SMF forum. They're saying SMF is better
written than phpBB and more reliable, so if I can get SMF to look right,
that's the preferable choice.

Most forums run vBulletin (big-boards.com lists 1376 vBulletin, 275
Invision, 245 phpBB and 41 SMF), so if you don't look like vBulletin or
Invision, it looks like you compromised because you couldn't afford
vBulletin. SMF's UI started out further away from the standard look,
but I've been able to use CSS to make it look more like the others.

I've done as much as I can with CSS, the rest requires editing PHP files
and uploading images. The forum doesn't have a built in file
upload/edit admin feature, it's added separately as the SMF File Manager
mod. I uploaded the mod but some files need to be chmod 777 so it can
install. If you go to Admin->Packages->Browse Packages and click on
Apply Mod, it offers to do it automatically if you enter an ftp login.

Someone says you might also have to
mkdir /var/www/bitcoin/smf/packages/temp

The error in the error log is:
failed to open stream: Permission denied
File: /var/www/bitcoin/smf/Sources/Subs-Package.php
(I'm sure that's just the first file)

Is it OK to go live with this SMF installation when I'm finished
configuring it? I should be able to point forum.bitcoin.org to it.

Liberty reports that linux-test8 has been running smoothly. My tests
have been running fine as well. The Linux version looks fully
stabilized to me.

Good news: he says he made his first sale of bitcoins. Someone bought
out all he had. I had been wondering whether it would be buyers or sellers.

Email #100

Date: Fri, 20 Nov 2009 09:05:34 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

I don't have the time to configure it today, but I made a temporary
account "maintenance" with password "6648ku5HeK" and full permissions
to /var/www/bitcoin. You can access it via ssh or sftp at port 30000.

It's okay to go live. Are you setting up a redirect or a dns entry? In
case of dns entry I could set up an Apache vhost so that the forum
address would be http://forum.bitcoin.org/.

Great that the Linux build works now. It's exciting to see how things
will start rolling with the new release and the forum. Not too long
until I can set up my own exchange and start promoting the currency to
(web) business people.

NewLibertyStandard should perhaps change his pricing to the market
price (i.e. what people are willing to buy and sell for) so that he
doesn't run out of coins.

> I've been configuring the SMF forum. They're saying SMF is better
> written than phpBB and more reliable, so if I can get SMF to look
> right, that's the preferable choice.
>
> Most forums run vBulletin (big-boards.com lists 1376 vBulletin, 275
> Invision, 245 phpBB and 41 SMF), so if you don't look like vBulletin or
> Invision, it looks like you compromised because you couldn't afford
> vBulletin. SMF's UI started out further away from the standard look,
> but I've been able to use CSS to make it look more like the others.
>
> I've done as much as I can with CSS, the rest requires editing PHP
> files and uploading images. The forum doesn't have a built in file
> upload/edit admin feature, it's added separately as the SMF File
> Manager mod. I uploaded the mod but some files need to be chmod 777 so
> it can install. If you go to Admin->Packages->Browse Packages and
> click on Apply Mod, it offers to do it automatically if you enter an
> ftp login.
>
> Someone says you might also have to
> mkdir /var/www/bitcoin/smf/packages/temp
>
> The error in the error log is:
> failed to open stream: Permission denied
> File: /var/www/bitcoin/smf/Sources/Subs-Package.php
> (I'm sure that's just the first file)
>
> Is it OK to go live with this SMF installation when I'm finished
> configuring it? I should be able to point forum.bitcoin.org to it.
>
> Liberty reports that linux-test8 has been running smoothly. My tests
> have been running fine as well. The Linux version looks fully
> stabilized to me.
>

> Good news: he says he made his first sale of bitcoins. Someone bought
> out all he had. I had been wondering whether it would be buyers or
> sellers.

Email #101

Date: Fri, 20 Nov 2009 09:17:00 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

Oh yes, one more thing. I haven't configured the server's sendmail
yet, so the php mail functionality doesn't work, but it's not needed
yet anyway.

> I don't have the time to configure it today, but I made a temporary
> account "maintenance" with password "6648ku5HeK" and full permissions
> to /var/www/bitcoin. You can access it via ssh or sftp at port 30000.
>
> It's okay to go live. Are you setting up a redirect or a dns entry? In
> case of dns entry I could set up an Apache vhost so that the forum
> address would be http://forum.bitcoin.org/.
>
> Great that the Linux build works now. It's exciting to see how things
> will start rolling with the new release and the forum. Not too long
> until I can set up my own exchange and start promoting the currency to
> (web) business people.
>
> NewLibertyStandard should perhaps change his pricing to the market
> price (i.e. what people are willing to buy and sell for) so that he
> doesn't run out of coins.
>
>> I've been configuring the SMF forum. They're saying SMF is better
>> written than phpBB and more reliable, so if I can get SMF to look
>> right, that's the preferable choice.
>>
>> Most forums run vBulletin (big-boards.com lists 1376 vBulletin, 275
>> Invision, 245 phpBB and 41 SMF), so if you don't look like vBulletin or
>> Invision, it looks like you compromised because you couldn't afford
>> vBulletin. SMF's UI started out further away from the standard look,
>> but I've been able to use CSS to make it look more like the others.
>>
>> I've done as much as I can with CSS, the rest requires editing PHP
>> files and uploading images. The forum doesn't have a built in file
>> upload/edit admin feature, it's added separately as the SMF File
>> Manager mod. I uploaded the mod but some files need to be chmod 777 so
>> it can install. If you go to Admin->Packages->Browse Packages and
>> click on Apply Mod, it offers to do it automatically if you enter an
>> ftp login.
>>
>> Someone says you might also have to
>> mkdir /var/www/bitcoin/smf/packages/temp
>>
>> The error in the error log is:
>> failed to open stream: Permission denied
>> File: /var/www/bitcoin/smf/Sources/Subs-Package.php
>> (I'm sure that's just the first file)
>>
>> Is it OK to go live with this SMF installation when I'm finished
>> configuring it? I should be able to point forum.bitcoin.org to it.

```
>>
>> Liberty reports that linux-test8 has been running smoothly.  My tests
>> have been running fine as well.  The Linux version looks fully
>> stabilized to me.
>>
>> Good news: he says he made his first sale of bitcoins.  Someone bought
>> out all he had.  I had been wondering whether it would be buyers or
>> sellers.
```

Email #102

Date: Fri, 20 Nov 2009 22:09:41 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

To: mmalmi@cc.hut.fi

```
> It's okay to go live. Are you setting up a redirect or a dns entry? In
> case of dns entry I could set up an Apache vhost so that the forum
> address would be http://forum.bitcoin.org/.

DNS entry.

I'm thinking of merging the bitcoin.org information with your site
content so I can switch the whole bitcoin.org domain over.  We need to
replace the current bitcoin.org site with a user-oriented site before
the release.

If the website and forum switch at the same time, then forum.bitcoin.org
isn't necessary unless we want it that way for looks.

Have you decided on the CMS to use?  I should research Drupal and other
CMSes and see what's the most popular.

> Great that the Linux build works now. It's exciting to see how things
> will start rolling with the new release and the forum. Not too long
> until I can set up my own exchange and start promoting the currency to
> (web) business people.

The linux version, setup exe, tor option and better website/forum will
all increase the percentage of visitors who can use it, and the
autostart and minimize to tray will increase how many keep running it.
All those factors multiply together.

> NewLibertyStandard should perhaps change his pricing to the market price
> (i.e. what people are willing to buy and sell for) so that he doesn't
> run out of coins.

It's good to start low and only have the price go up.

I really like that he explains the concept that the cost of electricity
is a minimum floor under the price.  At a minimum you either have to pay
the cost in electricity or pay someone the cost of production to make
them for you.
```

Email #103

Date: Sat, 21 Nov 2009 07:02:20 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

To: mmalmi@cc.hut.fi

```
Thanks, that worked, I got File Manager installed with SSH.  I also
uploaded a few themes into Drupal.  I haven't thoroughly gone through
all the available themes yet.

Looked around at CMSes, Drupal and Joomla are popular.  Consensus is
Joomla has a better selection of themes and is easier to learn, though
Drupal may be more intuitive for programmers and customization.  Joomla
better for CMS, Drupal better for blogs.  Drupal's URLs are search
engine friendly, Joomla not.

Both have SMF bridge modules available.  For future reference, Drupal's
is named "SMFforum Integration".

mmalmi@cc.hut.fi wrote:
> I don't have the time to configure it today, but I made a temporary
> account "" with password "" and full permissions to
> /var/www/bitcoin. You can access it via ssh or sftp at port 30000.
```

Email #104

Date: Sat, 21 Nov 2009 12:50:00 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

```
I've done a Joomla site for a customer, and I must say I like Drupal
better, mostly for the admin interface which is easier to use and
integrated into the main site.

Images aren't loading properly over https, I'll check it out when I can.

It's easier to just change the bitcoin.org DNS entry,
forum.bitcoin.org is not necessary.

We could see if we can get a free SSL certificate somewhere, like
http://www.startssl.com/?app=1, so the users wouldn't get a security
warning from a self-signed certificate. However I don't know if they
give certificates for anonymously registered domains.

> Thanks, that worked, I got File Manager installed with SSH.  I also
> uploaded a few themes into Drupal.  I haven't thoroughly gone through
> all the available themes yet.
>
> Looked around at CMSes, Drupal and Joomla are popular.  Consensus is
> Joomla has a better selection of themes and is easier to learn, though
> Drupal may be more intuitive for programmers and customization.  Joomla
> better for CMS, Drupal better for blogs.  Drupal's URLs are search
> engine friendly, Joomla not.
>
> Both have SMF bridge modules available.  For future reference, Drupal's
> is named "SMFforum Integration".
>
> mmalmi@cc.hut.fi wrote:
>> I don't have the time to configure it today, but I made a temporary
>>  account "" with password "" and full permissions to
>> /var/www/bitcoin. You can access it via ssh or sftp at port 30000.
```

Email #105

Date: Sat, 21 Nov 2009 21:46:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SMF forum, need a mod installed

To: mmalmi@cc.hut.fi

```
I'll go ahead with setting up Drupal then.

I don't think we should make the site https by default.  It's still very
unusual for the public part of sites to be https, probably because it
introduces potential technical complications, delays and greater server
load.  As a user I'm a little annoyed when it takes time to verify the
identity of some no-name site I casually came across.  For me it seems
like https sites fail to load a lot more often.

The important thing is to have SSL available for those who need it.
Those who need SSL I think know to try inserting an "s" after http and
see if it works.  SMF has code that changes all the links to https if
the URL handed in is https.

We could add a note on the registration page that if you want SSL, you
can change http to https at any time and approve the self-signed
certificate, or a link that does it, and the TOR page can mention it too.

We can look into getting a certificate later when things have settled
down.  With Class 1, no changes are allowed for a year, which is a risk
if we find issues with the current host and have to change IP.

mmalmi@cc.hut.fi wrote:
> I've done a Joomla site for a customer, and I must say I like Drupal
> better, mostly for the admin interface which is easier to use and
> integrated into the main site.
>
> Images aren't loading properly over https, I'll check it out when I can.
>
> It's easier to just change the bitcoin.org DNS entry, forum.bitcoin.org
> is not necessary.
>
> We could see if we can get a free SSL certificate somewhere, like
> http://www.startssl.com/?app=1, so the users wouldn't get a security
> warning from a self-signed certificate. However I don't know if they
> give certificates for anonymously registered domains.
>
>> Thanks, that worked, I got File Manager installed with SSH.  I also
>> uploaded a few themes into Drupal.  I haven't thoroughly gone through
>> all the available themes yet.
>>
>> Looked around at CMSes, Drupal and Joomla are popular.  Consensus is
>> Joomla has a better selection of themes and is easier to learn, though
>> Drupal may be more intuitive for programmers and customization.  Joomla
>> better for CMS, Drupal better for blogs.  Drupal's URLs are search
>> engine friendly, Joomla not.
>>
>> Both have SMF bridge modules available.  For future reference, Drupal's
>> is named "SMFforum Integration".
>>
>> mmalmi@cc.hut.fi wrote:
>>> I don't have the time to configure it today, but I made a temporary
>>>  account "" with password "" and full permissions to
>>> /var/www/bitcoin. You can access it via ssh or sftp at port 30000.
>
>
```

>

Email #106

Date: Sun, 22 Nov 2009 19:47:56 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: SEO friendly site transition

To: Martti Malmi <mmalmi@cc.hut.fi>

We need to do a continuity transition with bitcoin.org so the search engines don't think this is a new site and reset the site start date and PR data. Google allows a certain number of properties like IP address or content of the site to change without deleting your site history. To play it safe, when the IP address changes, the content better stay the same and vice versa. Even though not much rank has accumulated yet, the original start date becomes extremely important if the site gets popular later.

Steps:
1) copy the current bitcoin.org index.html to the new server exactly as-is.
2) switch the bitcoin.org DNS entry.
3) keep working on the drupal site behind the scenes.
4) after google has had time to update its records, we can switch over to the drupal site.

The timing works out well because we can switch to the new forum now and release the drupal site later when we're ready.

I'll see if I can figure out how to temporarily move drupal aside to drupal.php or /drupal/ or something where we can still easily get in and work on it.

Email #107

Date: Sun, 22 Nov 2009 22:22:57 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: SEO friendly site transition

That's ok.

I'll be afk 23.-25.11.

> We need to do a continuity transition with bitcoin.org so the search
> engines don't think this is a new site and reset the site start date
> and PR data. Google allows a certain number of properties like IP
> address or content of the site to change without deleting your site
> history. To play it safe, when the IP address changes, the content
> better stay the same and vice versa. Even though not much rank has
> accumulated yet, the original start date becomes extremely important if
> the site gets popular later.
>
> Steps:
> 1) copy the current bitcoin.org index.html to the new server exactly as-is.
> 2) switch the bitcoin.org DNS entry.
> 3) keep working on the drupal site behind the scenes.
> 4) after google has had time to update its records, we can switch over
> to the drupal site.
>
> The timing works out well because we can switch to the new forum now
> and release the drupal site later when we're ready.

```
>
> I'll see if I can figure out how to temporarily move drupal aside to
> drupal.php or /drupal/ or something where we can still easily get in
> and work on it.
```

Email #108

Date: Mon, 23 Nov 2009 05:48:19 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Access permissions required to fix Drupal

To: Martti Malmi <mmalmi@cc.hut.fi>

```
Drupal's .htaccess file which uses mod_rewrite to allow clean URLs
without the ? parameter is not working because its changes are rejected
because Apache is not configured with "AllowOverride All".  This is
needed to make Drupal coexist with the other site the way we want.

I need access to change these files to fix it:
  /etc/apache2/sites-available/default
  /etc/apache2/sites-available/default-ssl
  /etc/apache2/httpd.conf

Here's the planned fix.  If you do it yourself, please still give me
access to httpd.conf in case I need to change it again later.

In /etc/apache2/sites-available/default
change the 2nd instance of "AllowOverride None"
      to "AllowOverride All"

and in /etc/apache2/sites-available/default-ssl
change the 2nd instance of "AllowOverride AuthConfig"
      to "AllowOverride All"

replace
  /etc/apache2/httpd.conf
with
  /home/maintenance/httpd.conf

This probably requires Apache to be restarted after.
(apache2ctl graceful)
```

Email #109

Date: Mon, 23 Nov 2009 08:44:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Access permissions required to fix Drupal

```
Done. I granted you access to all the files.

> Drupal's .htaccess file which uses mod_rewrite to allow clean URLs
> without the ? parameter is not working because its changes are rejected
> because Apache is not configured with "AllowOverride All".  This is
> needed to make Drupal coexist with the other site the way we want.
>
> I need access to change these files to fix it:
>  /etc/apache2/sites-available/default
>  /etc/apache2/sites-available/default-ssl
```

```
>  /etc/apache2/httpd.conf
>
> Here's the planned fix.  If you do it yourself, please still give me
> access to httpd.conf in case I need to change it again later.
>
> In /etc/apache2/sites-available/default
> change the 2nd instance of "AllowOverride None"
>      to "AllowOverride All"
>
> and in /etc/apache2/sites-available/default-ssl
> change the 2nd instance of "AllowOverride AuthConfig"
>      to "AllowOverride All"
>
> replace
>  /etc/apache2/httpd.conf
> with
>  /home/maintenance/httpd.conf
>
> This probably requires Apache to be restarted after.
> (apache2ctl graceful)
```

Email #110

Date: Thu, 26 Nov 2009 00:26:33 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: bitcoin.org DNS change went through

To: Martti Malmi <mmalmi@cc.hut.fi>

```
The bitcoin.org DNS change went through about 12 hours ago.  I'll wait
another 12 hours and then change the Forum tab on
bitcoin.sourceforge.net to go to http://www.bitcoin.org/smf/

For future reference, the changes in SMF to update the base url were:
   server settings->Forum URL
   themes and layout->attempt to reset all themes
   there's a path in smileys and message icons
```

Email #111

Date: Thu, 26 Nov 2009 17:45:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bitweaver menu editor broken

To: Martti Malmi <mmalmi@cc.hut.fi>

```
The Bitweaver menu editor is broken, I can't change the Forum link.  The
"create and edit menu items" page comes up blank for me:

http://bitcoin.sourceforge.net/nexus/menu_items.php?menu_id=2

You try it, I'm stumped.

The Forum link should be changed to:
http://www.bitcoin.org/smf/
```

Email #112

Date: Fri, 27 Nov 2009 02:46:50 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitweaver menu editor broken

```
Fixed. I changed it directly in the database.

> The Bitweaver menu editor is broken, I can't change the Forum link.
> The "create and edit menu items" page comes up blank for me:
>
> http://bitcoin.sourceforge.net/nexus/menu_items.php?menu_id=2
>
> You try it, I'm stumped.
>
> The Forum link should be changed to:
> http://www.bitcoin.org/smf/
```

Email #113

Date: Sun, 29 Nov 2009 09:53:10 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Cc: Liberty Standard <newlibertystandard@gmail.com>

Subject: Google Wave

```
I just watched the Google Wave introduction video at wave.google.com.
It's the Google's open source proposal for a replacement for the
decades old e-mail protocol, and it looked quite cool. A "wave" is a
communication and collaboration unit that can be read and edited by
multiple users in real time and easily shared to new users, unlike
e-mail threads. It combines the functionality of instant messaging,
wikis, conventional e-mail and social networking, and supports
integration with external applications.

If you want invites, you can give me the e-mail addresses where you
want them to. If you already have Wave addresses, please give me them
as well. It would be great to see how the system works in practice.
```

Email #114

Date: Mon, 30 Nov 2009 14:13:04 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bitcoin.org

```
The current site layout looks nice and simple. The logo just should be
changed. If we want to go live quickly, we can just replace it with
the site title and make a better logo later.

If we need help with site administration or contacts to professional
web graphic artists, we can ask Dave. He does Drupal stuff for work.
```

Email #115

Date: Mon, 30 Nov 2009 14:36:51 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

```
It would be also great if you can get the Sourceforge logo from the SF
project admin and add it to the site footer.

> The current site layout looks nice and simple. The logo just should be
> changed. If we want to go live quickly, we can just replace it with the
> site title and make a better logo later.
>
> If we need help with site administration or contacts to professional
> web graphic artists, we can ask Dave. He does Drupal stuff for work.
```

Email #116

Date: Mon, 30 Nov 2009 16:07:13 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

```
I autogenerated the new logo at http://cooltext.com/, it's a good
quick solution. You can try a wide variety of different logo styles
there if you have the patience for the slow user interface.

> It would be also great if you can get the Sourceforge logo from the SF
> project admin and add it to the site footer.
>
>> The current site layout looks nice and simple. The logo just should be
>> changed. If we want to go live quickly, we can just replace it with the
>> site title and make a better logo later.
>>
>> If we need help with site administration or contacts to professional
>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
```

Email #117

Date: Mon, 30 Nov 2009 20:34:20 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

To: mmalmi@cc.hut.fi

```
Thanks, I haven't settled on a theme yet.  My first experiment was to
try something besides yet another blue site.  Another line of thought is
that it should be like a bank website, stately, professional and
official looking to support confidence in financial matters.

The logo's a little too Disco/web-1990's.  I still like your bitweaver
one better, I recreated it with text as a placeholder for now.  When the
theme is more settled, I'll think about a matching logo.

Good idea about the Sourceforge tag, we can use all the graphics we can get.

I have more to do before we go live, and we need to give the search
engines more time.

mmalmi@cc.hut.fi wrote:
> I autogenerated the new logo at http://cooltext.com/, it's a good quick
```

> solution. You can try a wide variety of different logo styles there if
> you have the patience for the slow user interface.
>
>> It would be also great if you can get the Sourceforge logo from the SF
>> project admin and add it to the site footer.
>>
>>> The current site layout looks nice and simple. The logo just should be
>>> changed. If we want to go live quickly, we can just replace it with the
>>> site title and make a better logo later.
>>>
>>> If we need help with site administration or contacts to professional
>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>
>
>

Email #118

Date: Wed, 02 Dec 2009 16:26:42 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

The text logo looks quite good actually, except on Windows when the
font antialiasing doesn't work. I turned it into a png.

I just made a 10,000bc transaction from one account to another, but it
ended up sending 10,000.20bc. Any idea why that could be?

> Thanks, I haven't settled on a theme yet. My first experiment was to
> try something besides yet another blue site. Another line of thought
> is that it should be like a bank website, stately, professional and
> official looking to support confidence in financial matters.
>
> The logo's a little too Disco/web-1990's. I still like your bitweaver
> one better, I recreated it with text as a placeholder for now. When
> the theme is more settled, I'll think about a matching logo.
>
> Good idea about the Sourceforge tag, we can use all the graphics we can get.
>
> I have more to do before we go live, and we need to give the search
> engines more time.
>
> mmalmi@cc.hut.fi wrote:
>> I autogenerated the new logo at http://cooltext.com/, it's a good
>> quick solution. You can try a wide variety of different logo styles
>> there if you have the patience for the slow user interface.
>>
>>> It would be also great if you can get the Sourceforge logo from the SF
>>> project admin and add it to the site footer.
>>>
>>>> The current site layout looks nice and simple. The logo just should be
>>>> changed. If we want to go live quickly, we can just replace it with the
>>>> site title and make a better logo later.
>>>>
>>>> If we need help with site administration or contacts to professional
>>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>
>>
>>

Email #119

Date: Wed, 02 Dec 2009 17:47:48 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

To: mmalmi@cc.hut.fi

```
What Windows version/browser doesn't font anti-aliasing work on?  IE 6
on XP anti-aliases, and versions below that have less than 1% market share.

There's a transaction fee of 0.01 per KB after the first 1KB for
oversized transactions.  The first 1KB is free, small transactions are
typically 250 bytes.  Doubleclick on the transaction.  Think of it like
postage by weight.

The solution is an extra dialog when sending, something like "This is an
oversized transaction and requires a transaction fee of 0.20bc.  Is this
OK?"  (is that text good enough or any improvements?)  I have the code
already, I'll put it in.

Then we wouldn't have to explain the 10,000.20bc transaction, but may
still have to explain who the transaction fee goes to.

mmalmi@cc.hut.fi wrote:
> The text logo looks quite good actually, except on Windows when the font
> antialiasing doesn't work. I turned it into a png.
>
> I just made a 10,000bc transaction from one account to another, but it
> ended up sending 10,000.20bc. Any idea why that could be?
>
>> Thanks, I haven't settled on a theme yet.  My first experiment was to
>> try something besides yet another blue site.  Another line of thought
>> is that it should be like a bank website, stately, professional and
>> official looking to support confidence in financial matters.
>>
>> The logo's a little too Disco/web-1990's.  I still like your bitweaver
>> one better, I recreated it with text as a placeholder for now.  When
>> the theme is more settled, I'll think about a matching logo.
>>
>> Good idea about the Sourceforge tag, we can use all the graphics we
>> can get.
>>
>> I have more to do before we go live, and we need to give the search
>> engines more time.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I autogenerated the new logo at http://cooltext.com/, it's a good
>>> quick solution. You can try a wide variety of different logo styles
>>>  there if you have the patience for the slow user interface.
>>>
>>>> It would be also great if you can get the Sourceforge logo from the SF
>>>> project admin and add it to the site footer.
>>>>
>>>>> The current site layout looks nice and simple. The logo just should be
>>>>> changed. If we want to go live quickly, we can just replace it with
>>>>> the
>>>>> site title and make a better logo later.
>>>>>
>>>>> If we need help with site administration or contacts to professional
>>>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>>
```

>>>
>>>
>
>
>

Email #120

Date: Thu, 03 Dec 2009 09:46:50 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

> What Windows version/browser doesn't font anti-aliasing work on? IE 6
> on XP anti-aliases, and versions below that have less than 1% market
> share.

Firefox on XP doesn't, and IE also doesn't produce as good quality as
I have on Linux. Screenshots from browsershots.org attached.

> There's a transaction fee of 0.01 per KB after the first 1KB for
> oversized transactions. The first 1KB is free, small transactions are
> typically 250 bytes. Doubleclick on the transaction. Think of it like
> postage by weight.

Is there no transaction fee then, if you send the same amount in
multiple small packages?

> The solution is an extra dialog when sending, something like "This is
> an oversized transaction and requires a transaction fee of 0.20bc. Is
> this OK?" (is that text good enough or any improvements?) I have the
> code already, I'll put it in.

Sounds fine.

> Then we wouldn't have to explain the 10,000.20bc transaction, but may
> still have to explain who the transaction fee goes to.

Where should it go btw? Here it went to the receiver along with all
the other coins. Transaction screenshot attached.

> mmalmi@cc.hut.fi wrote:
>> The text logo looks quite good actually, except on Windows when the
>> font antialiasing doesn't work. I turned it into a png.
>>
>> I just made a 10,000bc transaction from one account to another, but
>> it ended up sending 10,000.20bc. Any idea why that could be?
>>
>>> Thanks, I haven't settled on a theme yet. My first experiment was to
>>> try something besides yet another blue site. Another line of thought
>>> is that it should be like a bank website, stately, professional and
>>> official looking to support confidence in financial matters.
>>>
>>> The logo's a little too Disco/web-1990's. I still like your bitweaver
>>> one better, I recreated it with text as a placeholder for now. When
>>> the theme is more settled, I'll think about a matching logo.
>>>
>>> Good idea about the Sourceforge tag, we can use all the graphics
>>> we can get.
>>>
>>> I have more to do before we go live, and we need to give the search
>>> engines more time.

>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I autogenerated the new logo at http://cooltext.com/, it's a good
>>>> quick solution. You can try a wide variety of different logo
>>>> styles there if you have the patience for the slow user interface.
>>>>
>>>>> It would be also great if you can get the Sourceforge logo from the SF
>>>>> project admin and add it to the site footer.
>>>>>
>>>>>> The current site layout looks nice and simple. The logo just should be
>>>>>> changed. If we want to go live quickly, we can just replace it with the
>>>>>> site title and make a better logo later.
>>>>>>
>>>>>> If we need help with site administration or contacts to professional
>>>>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>>>
>>>>
>>>>
>>
>>
>>

Email #121

Date: Fri, 04 Dec 2009 04:24:41 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin.org

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
>> What Windows version/browser doesn't font anti-aliasing work on? IE 6
>> on XP anti-aliases, and versions below that have less than 1% market
>> share.
>
> Firefox on XP doesn't, and IE also doesn't produce as good quality as I
> have on Linux. Screenshots from browsershots.org attached.

That's strange, I've seen Firefox 3.5 on XP anti-alias large fonts.
Well anyway, your way is safer.

I changed it back to text for now though so I can keep tweaking the
colours. Drupal puts the tags and junk in the browser title but
that's fine for testing.

I added some instruction text on the homepage below the screenshots.

> Is there no transaction fee then, if you send the same amount in
> multiple small packages?

True. I suppose the dialog could make it worse by giving people a
chance to experiment with breaking it up.

I'm making some changes. The largest free transaction will be 60KB, or
about 27,000bc if made of 50bc inputs. I hope that's high enough that
the transaction fee should rarely ever come up. v0.2 nodes will take
free transactions until the block size is over 200K, with priority given
to smaller transactions.

It's best if you don't talk about this transaction fee stuff in public.
  It's there for flood control. We don't want to give anyone any ideas.

> Where should it go btw? Here it went to the receiver along with all the
> other coins. Transaction screenshot attached.

You found an infrequent bug in CreateTransaction. It wrote the
transaction for 10000.20 with a fee of 0.22. If you look at the
transaction on the sender's side, it'll be a debit 10000.42 with
transaction fee 0.22. The bug was that it had to make a rare third pass
on calculating the fee, and incorrectly added the first pass' fee to the
amount being sent. Will fix.

Email #122

Date: Sun, 06 Dec 2009 03:21:00 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Sourceforge tracker

To: mmalmi@cc.hut.fi

I added the sourceforge tracker to bitcoin.sourceforge.net. The
complete selection of links is below if you want a different one.

I had it on bitcoin.org for a minute, but took it off. It breaks the
lock in SSL mode with a mixed content warning, "partially encrypted" and
"contains unauthenticated content". Anyway, do we really want
sourceforge tracking everyone? It's more privacy friendly without it.

The available logos and the correct HTML to use for the Bitcoin project are:

Logo 1 (Dimensions: 80 x 15; Background: Black)

HTML Code: <img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=8"
width="80" height="15" alt="Get Bitcoin at SourceForge.net. Fast, secure
and Free Open Source software downloads" />

Logo 2 (Dimensions: 80 x 15; Background: Silver)

HTML Code: <img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=9"
width="80" height="15" alt="Get Bitcoin at SourceForge.net. Fast, secure
and Free Open Source software downloads" />

Logo 3 (Dimensions: 80 x 15; Background: White)

HTML Code: <img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=10"
width="80" height="15" alt="Get Bitcoin at SourceForge.net. Fast, secure
and Free Open Source software downloads" />

Logo 4 (Dimensions: 120 x 30; Background: Black)

HTML Code: <img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=11"
width="120" height="30" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" />

Logo 5 (Dimensions: 120 x 30; Background: Silver)

HTML Code: <a href="http://sourceforge.net/projects/bitcoin"><img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&type=12"

```
width="120" height="30" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" /></a>

Logo 6 (Dimensions: 120 x 30; Background: White)

HTML Code: <a href="http://sourceforge.net/projects/bitcoin"><img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&amp;type=13"
width="120" height="30" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" /></a>

Logo 7 (Dimensions: 150 x 40; Background: Black)

HTML Code: <a href="http://sourceforge.net/projects/bitcoin"><img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&amp;type=14"
width="150" height="40" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" /></a>

Logo 8 (Dimensions: 150 x 40; Background: Silver)

HTML Code: <a href="http://sourceforge.net/projects/bitcoin"><img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&amp;type=15"
width="150" height="40" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" /></a>

Logo 9 (Dimensions: 150 x 40; Background: White)

HTML Code: <a href="http://sourceforge.net/projects/bitcoin"><img
src="http://sflogo.sourceforge.net/sflogo.php?group_id=244765&amp;type=16"
width="150" height="40" alt="Get Bitcoin at SourceForge.net. Fast,
secure and Free Open Source software downloads" /></a>


mmalmi@cc.hut.fi wrote:
> It would be also great if you can get the Sourceforge logo from the SF
> project admin and add it to the site footer.
>
>> The current site layout looks nice and simple. The logo just should be
>> changed. If we want to go live quickly, we can just replace it with the
>> site title and make a better logo later.
>>
>> If we need help with site administration or contacts to professional
>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>
>
>
```

Email #123

Date: Mon, 07 Dec 2009 13:49:08 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Sourceforge tracker

```
I made a copy of the logo onto the local server, so we can still use
it for graphics. It's not disallowed by the SF trademark policy.

> I added the sourceforge tracker to bitcoin.sourceforge.net.  The
> complete selection of links is below if you want a different one.
>
> I had it on bitcoin.org for a minute, but took it off.  It breaks the
> lock in SSL mode with a mixed content warning, "partially encrypted"
> and "contains unauthenticated content".  Anyway, do we really want
```

```
> sourceforge tracking everyone?  It's more privacy friendly without it.
>
> mmalmi@cc.hut.fi wrote:
>> It would be also great if you can get the Sourceforge logo from the
>>  SF project admin and add it to the site footer.
>>
>>> The current site layout looks nice and simple. The logo just should be
>>> changed. If we want to go live quickly, we can just replace it with the
>>> site title and make a better logo later.
>>>
>>> If we need help with site administration or contacts to professional
>>> web graphic artists, we can ask Dave. He does Drupal stuff for work.
>>
>>
>>
```

Email #124

Date: Tue, 08 Dec 2009 05:43:33 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Drupal site online

To: Martti Malmi <mmalmi@cc.hut.fi>

```
I went ahead and put the new Drupal site online.  Enough time has passed
for a safe transition, and the site looks good.  There's more work I
should do on the theme, but it's good enough so far.  This is a huge
improvement over the old bitcoin.org page.
```

Email #125

Date: Tue, 08 Dec 2009 12:50:20 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Drupal site online

```
Good job. I redirected bitcoin.sourceforge.net there.

> I went ahead and put the new Drupal site online.  Enough time has
> passed for a safe transition, and the site looks good.  There's more
> work I should do on the theme, but it's good enough so far.  This is a
> huge improvement over the old bitcoin.org page.
```

Email #126

Date: Fri, 11 Dec 2009 03:30:10 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: custom3 theme

To: Martti Malmi <mmalmi@cc.hut.fi>

```
I wasn't satisfied with my custom2 theme.  It felt crowded, the
header/logo seemed wrong and the heavy left margin stationery style is
outdated.

custom3 online now is a more standard layout similar to a lot of
```

```
commercial software homepages.  Maybe it's just me, but I really like
the random blue squares.
```

Email #127

Date: Sun, 13 Dec 2009 22:12:38 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Version 0.2 almost ready to release

```
> It's almost time to release version 0.2.  If you have a minute, could
> you try this release candidate (attached)?  If there aren't any
> problems and I don't think of anything I missed, this could be released
> in a day or two.

No problems so far. Seems fine.

> I zipped the setup exe because I doubt the e-mail servers will allow
> exe attachments.  I'm not sure it'll allow zip either, but pretty sure
> the tar.gz one will get through.
>
> Attachments:
> 3,092,916 bitcoin-0.2.0-setup.zip
> 2,402,522 bitcoin-0.2.0-linux.tar.gz
> 3,061,059 bitcoin-0.2.0-win32.zip

Both got through here.
```

Email #128

Date: Tue, 15 Dec 2009 06:40:04 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: RC2

```
> Found something I felt I had to fix with the initial block download.
> Do you mind testing an initial block download again?

The first time I tried it on Windows, the initial download took a few
minutes to start, even though it got many connections quickly. I tried
again twice, and didn't have the same problem again. I don't know
whether it's related to your latest update or not.

On Ubuntu it worked fine.

> Hope this isn't in the middle of your final exams right now.

Well actually it is, but it's not too bad. Time is a matter of arrangement.
```

Email #129

Date: Wed, 16 Dec 2009 04:57:36 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: RC2

To: mmalmi@cc.hut.fi

```
mmalmi@cc.hut.fi wrote:
> The first time I tried it on Windows, the initial download took a few
> minutes to start, even though it got many connections quickly. I tried
```

```
> again twice, and didn't have the same problem again. I don't know
> whether it's related to your latest update or not.

Most of the fixes are on the sender's side, so if you were downloading the
network upgrades to 0.2.

How long did the initial download take?
```

Email #130

Date: Wed, 16 Dec 2009 17:41:41 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: RC2

```
>> The first time I tried it on Windows, the initial download took a
>> few minutes to start, even though it got many connections quickly.
>> I tried again twice, and didn't have the same problem again. I
>> don't know whether it's related to your latest update or not.
>
> Most of the fixes are on the sender's side, so if you were downloading
> from a 0.1.5 node, some problems are still there.  It'll get better as
> the network upgrades to 0.2.
>
> How long did the initial download take?

About 1,5h.
```

Email #131

Date: Wed, 16 Dec 2009 16:54:46 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Planned release announcement text

To: Martti Malmi <mmalmi@cc.hut.fi>

```
Here's the planned release announcement text.  Probably releasing shortly.

Bitcoin version 0.2 is here!

Download links:
Windows Setup Program
Windows Zip File
Linux (tested on Ubuntu)

New features

Martti Malmi
  - Minimize to system tray option
  - Autostart on boot option so you can keep it running in the
background automatically
  - New options dialog layout for future expansion
  - Setup program for Windows
  - Linux version
Satoshi Nakamoto
  - Multi-processor support for coin generation
  - Proxy support for use with TOR
  - Fixed some slowdowns in the initial block download
  - Various refinements to keep the network running smoothly

We also have a new forum at http://www.bitcoin.org/smf/ if you have any
questions.
```

```
Thanks to Martti Malmi (sirius-m) for his coding work and for hosting
the new site and forum, and thanks to New Liberty Standard for testing
the Linux version.

Satoshi Nakamoto
```

Email #132

Date: Thu, 17 Dec 2009 06:49:02 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [bitcoin-list] Bitcoin 0.2 released

To: bitcoin-list@lists.sourceforge.net

```
Bitcoin 0.2 is here!

Download (Windows, and now Linux version available)
http://sourceforge.net/projects/bitcoin/files/

New Features

Martti Malmi
  - Minimize to system tray option
  - Autostart on boot option so you can keep it running in the
background automatically
  - New options dialog layout for future expansion
  - Setup program for Windows
  - Linux version (tested on Ubuntu)
Satoshi Nakamoto
  - Multi-processor support for coin generation
  - Proxy support for use with TOR
  - Fixed some slowdowns in the initial block download

We also have a new forum at http://www.bitcoin.org/smf/

Many thanks to Martti (sirius-m) for all his development work, and to
New Liberty Standard for his help with testing the Linux version.

Satoshi Nakamoto

------------------------------------------------------------------------------
This SF.Net email is sponsored by the Verizon Developer Community
Take advantage of Verizon's best-in-class app development support
A streamlined, 14 day to market process makes app distribution fast and easy
Join now and get one step closer to millions of Verizon customers
http://p.sf.net/sfu/verizon-dev2dev
_______________________________________________
bitcoin-list mailing list
bitcoin-list@lists.sourceforge.net
https://lists.sourceforge.net/lists/listinfo/bitcoin-list
```

Email #133

Date: Tue, 22 Dec 2009 15:49:14 +0200

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Bitcoin stuff

```
I have registered the domain name bitcoinexchange.com and will start
coding the service sometime soon as a nice leisure activity. I'm
envisioning a simple Google-like interface with no registration and
only two texts fields on the front page, where you insert the amount
```

of money you wish to trade, and either your PayPal address to buy
dollars or bitcoin address to buy bitcoins. On the next page you'll
get a new bitcoin address for sending the coins or a check code for
the PayPal transaction text.

PayPal is good for the beginning - it's simple and has no startup
costs, but later on I might accept credit cards also.

Do you still need the maintenance account? It's ok if you do, but
change the password to something else.

Email #134

Date: Tue, 22 Dec 2009 19:00:41 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

To: mmalmi@cc.hut.fi

Thanks for creating the maintenance account, it would have been
impossible to do all that without it. I'm really always going to need
it. OK, I changed the password to a 20 character random password.

That's a good domain. People rarely type domain names anymore, they use
autocomplete or click links on search engines.

I need to make a way for you to programmatically get new generated
bitcoin addresses. Either that or you could have them send to your IP
address, but then you have to rely on them to put the order number in
the comment.

When generating the new address, there can be an option to add an entry
to the address book associated with the address, so the received
transaction will be labelled. I kinda hid the labels after early users
found them confusing, but it would be very helpful for this application.
  You have to widen up the comment column to see them.

Are you going to manually review and enter orders, at least to begin
with? I sure would.

I'm thinking I should move the UI in the direction of having the user
ask for their bitcoin address when they want one. "give me a bitcoin to
receive a payment with". I suppose next to the send button, there would
by a receive button, you press it and it says "here's a new address to
use, here's the button to copy it to the clipboard, do you want to label
it?" and maybe some explanation about why you shouldn't reuse addresses.

Or maybe just a "New Address" button next to the address box that you
should hit each time to change it.

mmalmi@cc.hut.fi wrote:
> I have registered the domain name bitcoinexchange.com and will start
> coding the service sometime soon as a nice leisure activity. I'm
> envisioning a simple Google-like interface with no registration and only
> two texts fields on the front page, where you insert the amount of money
> you wish to trade, and either your PayPal address to buy dollars or
> bitcoin address to buy bitcoins. On the next page you'll get a new
> bitcoin address for sending the coins or a check code for the PayPal
> transaction text.
>
> PayPal is good for the beginning - it's simple and has no startup costs,
> but later on I might accept credit cards also.
>

> Do you still need the maintenance account? It's ok if you do, but change
> the password to something else.
>

Email #135

Date: Wed, 23 Dec 2009 11:12:03 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

> I need to make a way for you to programmatically get new generated
> bitcoin addresses. Either that or you could have them send to your IP
> address, but then you have to rely on them to put the order number in
> the comment.

I'd also need at least the command line tools to check if coins have
been received and to send coins. It would require some way to
communicate with the Bitcoin process running in the background. I
don't know how that should be done, maybe with something RPC related.

It would also be great if the background process was non-graphical -
the VPS on the current service level doesn't have enough memory to run
the X Windowing environment, unless I come up with some ways to free
memory.

> Are you going to manually review and enter orders, at least to begin
> with? I sure would.

Yes, at least to begin with, when the customer sells bc's and receives
dollars. I wouldn't give a script the access to my dollar reserves so
lightly. The other way around (customer's dollars -> bitcoins) it
doesn't feel that insecure, and it's certainly nicer for the customer
to receive his bitcoins immediately.

> mmalmi@cc.hut.fi wrote:
>> I have registered the domain name bitcoinexchange.com and will
>> start coding the service sometime soon as a nice leisure activity.
>> I'm envisioning a simple Google-like interface with no registration
>> and only two texts fields on the front page, where you insert the
>> amount of money you wish to trade, and either your PayPal address
>> to buy dollars or bitcoin address to buy bitcoins. On the next page
>> you'll get a new bitcoin address for sending the coins or a check
>> code for the PayPal transaction text.
>>
>> PayPal is good for the beginning - it's simple and has no startup
>> costs, but later on I might accept credit cards also.
>>
>> Do you still need the maintenance account? It's ok if you do, but
>> change the password to something else.
>>

Email #136

Date: Wed, 23 Dec 2009 17:53:18 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> I'd also need at least the command line tools to check if coins have
> been received and to send coins. It would require some way to
> communicate with the Bitcoin process running in the background. I don't
> know how that should be done, maybe with something RPC related.
>
> It would also be great if the background process was non-graphical - the
> VPS on the current service level doesn't have enough memory to run the X
> Windowing environment, unless I come up with some ways to free memory.

I had been wondering why everyone keeps harping on no-UI, when already
you can run it with only a small icon on the tray, which is common for
server services on Windows. So I guess this is why. I had chalked it
up to unix snobbery if they couldn't abide a tiny little icon on a
desktop they never see.

Not opening any windows is easy, but it may fail because the gtk
libraries aren't there. wxWidgets has __WXBASE__ for "Only wxBase, no
GUI features". You could try building for that instead of __WXGTK__ and
see what happens. It would be preferable if there's any way to do it as
a command line switch on the same executable, rather than yet another
build variation to release.

How much memory do you have to work with? Bitcoin necessarily takes a
fair bit of memory; about 75MB on Windows. Is that a problem?

Command line control is one of the next things on the list. I want to
design the API carefully.

Receiving payments is the part that has a lot of design choices to be
made. The caller needs to identify the transactions of interest, that's
where the one-bitcoin-address-per-transaction model helps. Searching
the comments text for an order number is another possibility. There's
polled, asking what has been received to the given bitcoin address, and
event driven. I guess in event driven, bitcoin would be told to run a
command line when a certain amount is received to a certain bitcoin address.

Email #137

Date: Fri, 25 Dec 2009 15:25:43 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

> How much memory do you have to work with?
The VPS has 320MB RAM, 50MB of which is currently free. There's also
500MB swap space.

> Bitcoin necessarily takes a
> fair bit of memory; about 75MB on Windows. Is that a problem?

Sure about that? Windows task manager shows about 13MB memory usage here.

Email #138

Date: Fri, 25 Dec 2009 16:11:14 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin stuff

To: mmalmi@cc.hut.fi

You're right, I was looking at a test run with 250,000 blocks... duh.

A normal one shows 17MB memory usage and 10MB VM size.

mmalmi@cc.hut.fi wrote:
>> How much memory do you have to work with?
> The VPS has 320MB RAM, 50MB of which is currently free. There's also
> 500MB swap space.
>
>> Bitcoin necessarily takes a
>> fair bit of memory; about 75MB on Windows. Is that a problem?
>
> Sure about that? Windows task manager shows about 13MB memory usage here.
>

Email #139

Date: Tue, 05 Jan 2010 03:55:14 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bitcoin Exchange

I have a prototype of the bitcoinexchange.com service up now (auth:
bitcoin/bit). It's running on the Python-powered Django web
application framework, which is a pleasure to work with, compared to
php.

I'll have to do some studying for a few days now, after which I can
return to work with the exchange service. Among other things I'll fix
the pricing so that the price of Bitcoins grows towards infinity when
my supply of them gets closer to zero. That way I can find the market
rate and stay at the point where supply meets demand. I'm not yet
completely sure what the parameters of the hyperbolic pricing curve
should be, so that's something to think about.

Email #140

Date: Wed, 03 Feb 2010 11:27:17 +0200

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Bitcoin API

Have you decided upon the inter-process calling method of the Bitcoin
API yet? An easy solution would be the socket interface provided by
wxWidgets: http://docs.wxwidgets.org/trunk/overview_ipc.html. The
Bitcoin program running a wxServer could be then accessed by calling
the bitcoin executable from the command line or by coding your own
wxClient app.

Another option would be to just use the plain BSD sockets.

Can you send me a 64-bit Linux binary of Bitcoin if you have one? I
tried compiling on the VPS, but it ran out of memory. Tried the 32-bit
version (with ia32-libs) also, but it didn't find the shared libraries.

Email #141

Date: Thu, 04 Feb 2010 02:20:10 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Exchange ideas

To: Martti Malmi <mmalmi@cc.hut.fi>

```
You could always exchange for Liberty Reserve.  It's an online currency
similar to e-Bullion, Pecunix or Webmoney that allows exchanges no
questions asked and with privacy.

LR and the others are hard to buy but easy to cash out.  Hard to buy
because exchangers are very cautious about getting ripped off by
reversed payments, so they require more details and holding time.
Cashing out is very easy.  LR is non-reversible, so there are oodles of
exchanges eager to turn LR into any kind of payment.

Bitcoin is the reverse, in that it's easy to get Bitcoins just by
generating them.  It would be easy for customers to go
bitcoin->LR->cash, bitcoin->LR->gold, bitcoin->LR->paypal or maybe they
just want to save the money, then just bitcoin->LR.

There's also the idea BTC2PSC had to sell paysafecards for bitcoins.
Either online delivery by sending the card number by e-mail, or delivery
of the unopened physical card in the mails.  There are many variations
of these cards.  In some countries, they're called Gift Cards, and can
be used wherever credit cards are accepted.  I think they're used more
by people who don't have the credit history to get a real credit card,
so they buy gift cards themselves to pay for things that require a
credit card.
```

Email #142

Date: Thu, 04 Feb 2010 01:32:50 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Exchange options

To: Martti Malmi <mmalmi@cc.hut.fi>

```
Don't rush ahead and get yourself rejected from all the payment options
before you've had time to see if there's a better approach.  I suggest
you wait before contacting any more payment processors.  You may get
ideas from things other users come up with and try.

Just some random incomplete ideas: There may be a way to position it as
an intermediate credit for micropayments for some virtual good or
something.  Or maybe if the payments are only in one direction.  If you
only buy bitcoins, then you're only sending money out not taking
people's money, that would still be useful to peg the currency.  That
might be payment for computer time.

Credit card is only one way.  Don't even talk about the idea of
returning money to customer's credit cards.  Credit card companies hate
that.

In any case, any payment processor is going to expect you to be selling
something real.

Do you have electronic transfer or paper cheque in your country? (even
if only within Europe)
```

Email #143

Date: Wed, 03 Feb 2010 20:25:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin API

To: mmalmi@cc.hut.fi

```
Is there any way to find out what the missing shared libraries are?  It
would help to know.

It probably needs the gtk libraries, in which case you'll have the same
problem with the 64-bit version.  I would like to have a single
executable that can also run on a UI-less system, but I'm not sure how
on linux to link to things but still be able to run and not use them if
the library is not present.  Maybe we should statically link the GTK.
Licensewise, it's LGPL, but since it's only used on unix, that would be
OK.  (we can't link LGPL stuff on windows because we provide the OpenSSL
DLL, but on linux OpenSSL comes with the OS)

My 64-bit (debug stripped) executable is attached.  It includes untested
changes that are not in SVN yet: UI changes and the wallet fSpent flag
resync stuff.

I've been researching options for interprocess calling.  I want
something that will be easy for a variety of server side languages to
call, particularly PHP.  Cross-platform to windows is a plus.

I'm not sure if I want it to be something that can be accessed across
the network.  That would introduce security issues.  If it can only be
accessed on the local system, then local security authentication covers
it, and it is incapable of being hacked remotely.

At surface level, not looking into any details yet, the current front
runners are:
D-Bus:
    local system only
    used by qt, gnome and skype
    bindings: c, python, java, c++,
          php listed as "in progress"
          .net listed as unmaintained
          not sure how ready it is on windows
XML-RPC:
    widely used, built in libraries on PHP
    it's more for web clients to talk to server, transport is http, so
its a security question

Is it possible to open a socket that can only be accessed locally?

mmalmi@cc.hut.fi wrote:
> Have you decided upon the inter-process calling method of the Bitcoin
> API yet? An easy solution would be the socket interface provided by
> wxWidgets: http://docs.wxwidgets.org/trunk/overview_ipc.html. The
> Bitcoin program running a wxServer could be then accessed by calling the
> bitcoin executable from the command line or by coding your own wxClient
> app.
>
> Another option would be to just use the plain BSD sockets.
>
> Can you send me a 64-bit Linux binary of Bitcoin if you have one? I
> tried compiling on the VPS, but it ran out of memory. Tried the 32-bit
> version (with ia32-libs) also, but it didn't find the shared libraries.
>
```

Email #144

Date: Thu, 04 Feb 2010 19:47:36 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoin API

> Is there any way to find out what the missing shared libraries are? It
> would help to know.

This is what "ldd bitcoin" says:

```
        linux-gate.so.1 =>  (0xf778c000)
        libcrypto.so.0.9.8 => /usr/lib32/i686/cmov/libcrypto.so.0.9.8
(0xf762a000)
        libgtk-x11-2.0.so.0 => not found
        libgthread-2.0.so.0 => not found
        libSM.so.6 => /usr/lib32/libSM.so.6 (0xf7621000)
        libstdc++.so.6 => /usr/lib32/libstdc++.so.6 (0xf7533000)
        libm.so.6 => /lib32/libm.so.6 (0xf750f000)
        libgcc_s.so.1 => /usr/lib32/libgcc_s.so.1 (0xf7502000)
        libc.so.6 => /lib32/libc.so.6 (0xf73b0000)
        libdl.so.2 => /lib32/libdl.so.2 (0xf73ac000)
        libgdk-x11-2.0.so.0 => not found
        libXinerama.so.1 => /usr/lib32/libXinerama.so.1 (0xf73a8000)
        libgdk_pixbuf-2.0.so.0 => not found
        libX11.so.6 => /usr/lib32/libX11.so.6 (0xf72b9000)
        libpango-1.0.so.0 => not found
        libgobject-2.0.so.0 => not found
        libglib-2.0.so.0 => not found
        libpthread.so.0 => /lib32/libpthread.so.0 (0xf72a1000)
        libpng12.so.0 => /usr/lib32/libpng12.so.0 (0xf727e000)
        libz.so.1 => /usr/lib32/libz.so.1 (0xf7269000)
        libICE.so.6 => /usr/lib32/libICE.so.6 (0xf7251000)
        /lib/ld-linux.so.2 (0xf778d000)
        libXext.so.6 => /usr/lib32/libXext.so.6 (0xf7243000)
        libxcb-xlib.so.0 => /usr/lib32/libxcb-xlib.so.0 (0xf7241000)
        libxcb.so.1 => /usr/lib32/libxcb.so.1 (0xf7229000)
        libXau.so.6 => /usr/lib32/libXau.so.6 (0xf7226000)
        libXdmcp.so.6 => /usr/lib32/libXdmcp.so.6 (0xf7220000)
```

Notfounds seem to be gtk-libraries indeed. I have those files in my /usr/lib folder, but maybe they're ignored because they're 64bit, or maybe only /usr/lib32 is searched. I haven't tested on other 64bit machines.

> My 64-bit (debug stripped) executable is attached. It includes
> untested changes that are not in SVN yet: UI changes and the wallet
> fSpent flag resync stuff.

The package doesn't open, it says "not in gzip format".

> Is it possible to open a socket that can only be accessed locally?

Yes, you can use IPC sockets ("Unix domain sockets") which are local only. That's done in the wx-api by using a filename in place of a port number. I committed an example of how the wxServer-Client communication is used, you can revert if you want to. Now there's the -blockamount command line option which asks the running instance for the block chain length.

I think this command line method could already be used from PHP, but it might be lighter if php itself could call the socket server directly. The wx's IPC overview mentions wxSocketEvent, wxSocketBase, wxSocketClient and wxSocketServer as being "Classes for the low-level TCP/IP API", which might be easier to use from php than what I used now (wxServer, wxClient, wxConnection). I'll look more into it.

Email #145

Date: Thu, 04 Feb 2010 18:50:35 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin API

To: mmalmi@cc.hut.fi

```
I must have accidentally typed j instead of z.  It's bz2 format.  Rename
to .tar.bz2 or just do tar -jxvf

> The package doesn't open, it says "not in gzip format".
>
```

Email #146

Date: Thu, 04 Feb 2010 19:33:26 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: UTF-8 to ANSI hack in CAboutDialog

To: Martti Malmi <mmalmi@cc.hut.fi>

```
What was the reason for this change?

#if !wxUSE_UNICODE
...
     if (str.Find('Â') != wxNOT_FOUND)
         str.Remove(str.Find('Â'), 1);
to:
     if (str.Find('ï¿½') != wxNOT_FOUND)
         str.Remove(str.Find('ï¿½'), 1);

wxFormBuilder turns the (c) symbol into UTF-8 automatically.  On
wxWidgets-2.8.9 ansi, it shows as a copyright symbol with an extra trash
character, which this hack fixes up for the non-unicode (ansi) case.
```

Email #147

Date: Thu, 04 Feb 2010 19:59:48 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin API

To: mmalmi@cc.hut.fi

```
Good, then no need to consider d-bus.  Is there something like IPC
sockets on Windows?  I guess we could look how wx does it, or maybe the
XML-RPC library will already know what to do.  Windows has named pipes,
maybe that's the best analogue.

I don't think I want to invent my own RPC protocol, I want to use an
existing standard.  PHP, Java, Python or anything will be able to talk
to the server directly the same way the command line commands do.

I'm going to start reading on XML-RPC.  It's coming up in searches as
the most widely used protocol and widely supported.  PHP includes it in
its standard libraries.

>> Is it possible to open a socket that can only be accessed locally?
>
```

> Yes, you can use IPC sockets ("Unix domain sockets") which are local
> only. That's done in the wx-api by using a filename in place of a port
> number. I committed an example of how the wxServer-Client communication
> is used, you can revert if you want to. Now there's the -blockamount
> command line option which asks the running instance for the block chain
> length.
>
> I think this command line method could already be used from PHP, but it
> might be lighter if php itself could call the socket server directly.
> The wx's IPC overview mentions wxSocketEvent, wxSocketBase,
> wxSocketClient and wxSocketServer as being "Classes for the low-level
> TCP/IP API", which might be easier to use from php than what I used now
> (wxServer, wxClient, wxConnection). I'll look more into it.
>
>
>

Email #148

Date: Fri, 05 Feb 2010 04:08:54 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoin API research status

To: Martti Malmi <mmalmi@cc.hut.fi>

I noticed this in the docs for wxSocketServer::Accept(bool wait = true):
"If wait is true and there are no pending connections to be accepted, it
will wait for the next incoming connection to arrive. **Warning: This
will block the GUI."

wxWidgets is pathologically single-threaded. Not only single-threaded,
but must-be-the-GUI-thread-ed. Even for something as non-UI as
wxStandardPaths I got nailed. All this is fine for UI code, since this
is the same constraint placed by Windows anyway, but for UI-less server
daemon code, wx calls are uncertain.

Status of my research currently:

For PHP, Python, etc to access the server, we need to use regular
sockets. I think we can make it local-only by binding to localhost
only, so it can only be accessed through the loopback. They say it's
also watertight to simply check the IP of connections received and
disconnect anything not 127.0.0.1. May as well do both.

XML-RPC is a bit fat. There are 4 libraries for C++ but they're all big
and hard to build, dependencies, license issues. Some posters complain
all the C++ and PHP XML-RPC libraries are buggy.

JSON-RPC is a simpler more elegant standard. It's simple enough I could
use a generic JSON parser.

PHP, Python and Java all have good implementations of JSON-RPC.

I'm currently leaning towards JSON-RPC.

Email #149

Date: Fri, 05 Feb 2010 09:16:23 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: UTF-8 to ANSI hack in CAboutDialog

```
I didn't change it knowingly, must have been some encoding problem.

> What was the reason for this change?
>
> #if !wxUSE_UNICODE
> ...
>     if (str.Find('Â') != wxNOT_FOUND)
>         str.Remove(str.Find('Â'), 1);
> to:
>     if (str.Find('ï¿½') != wxNOT_FOUND)
>         str.Remove(str.Find('ï¿½'), 1);
>
> wxFormBuilder turns the (c) symbol into UTF-8 automatically.  On
> wxWidgets-2.8.9 ansi, it shows as a copyright symbol with an extra
> trash character, which this hack fixes up for the non-unicode (ansi)
> case.
```

Email #150

Date: Fri, 05 Feb 2010 09:56:16 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Exchange options

```
Liberty Reserve sounds good. I could first make a service that only
accepts LR, and add more options later. The weakness is that buying LR
is an extra step of inconvenience when the customer just wants to get
Bitcoins. But maybe I don't have too much choice here.

> Do you have electronic transfer or paper cheque in your country? (even
> if only within Europe)

Yes, electronic bank transfer is available. During 2010 most European
countries will become a part of SEPA (Single Euro Payments Area),
which means that all payments within Europe are to be considered
domestic. Banks will have to apply the same fees and standards to all
domestic transfers, so they'll probably all be free of charge and
complete in one bank day. For international transfers there's the
SWIFT/IBAN system, which usually costs some extra.

A longer term project for my exchange service would be to see what
kinds of integration options the banks have to offer. Bank transfers
would reach nearly as many customers as credit cards do.
```

Email #151

Date: Fri, 05 Feb 2010 18:29:12 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Exchange options

To: mmalmi@cc.hut.fi

```
Maybe the current difficulty of buying LR is already the limit of how
easy it can get in that direction.

Every conventional payment method has refutability as their way to cope
with their lack of passwords and crypto.  The system is wide open to
copying plaintext credit card numbers and account numbers, and they deal
with it by reversing the transaction after the fact.  The system works
```

for physical goods that have to be delivered somewhere, and services which can't be resold. It's a problem when it interfaces with precious metals and currency conversion.

The first step of being easy in one direction, bitcoin->LR or anything of established value, goes a long way. Even those who don't use the conversion still benefit from knowing that they could. Trading bitcoin becomes an easier way to trade the ability to claim LR, similar to how paper money was once the right to claim gold. Nobody has to ever actually claim the LR to get the benefit of having the option that they could if they wanted to.

A lot of times you just need a minuscule amount of online currency. The hassle of buying the other online currencies is too much for buying a small amount. The ease of getting a small amount of bitcoin may help bootstrap an ecosystem of sellers of micropayment sized online goods selling to that market. If the sellers can get LR for bitcoins, they're happy, and that may be subsidized at first by investors who want to buy bc in large lots.

The main thing holding online currencies back is the lack of an easy way to get a small amount of currency. Bitcoin opens that up. It'll be the only online currency that's both easy to cash out and easy to get a small amount. It'll just be the usual harder difficulty to buy a large amount.

mmalmi@cc.hut.fi wrote:
> Liberty Reserve sounds good. I could first make a service that only
> accepts LR, and add more options later. The weakness is that buying LR
> is an extra step of inconvenience when the customer just wants to get
> Bitcoins. But maybe I don't have too much choice here.
>
>> Do you have electronic transfer or paper cheque in your country? (even
>> if only within Europe)
>
> Yes, electronic bank transfer is available. During 2010 most European
> countries will become a part of SEPA (Single Euro Payments Area), which
> means that all payments within Europe are to be considered domestic.
> Banks will have to apply the same fees and standards to all domestic
> transfers, so they'll probably all be free of charge and complete in one
> bank day. For international transfers there's the SWIFT/IBAN system,
> which usually costs some extra.
>
> A longer term project for my exchange service would be to see what kinds
> of integration options the banks have to offer. Bank transfers would
> reach nearly as many customers as credit cards do.
>

Email #152

Date: Fri, 05 Feb 2010 18:39:18 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: UTF-8 to ANSI hack in CAboutDialog

To: mmalmi@cc.hut.fi

Right, I'll change it to this so it doesn't get broken again:
```
     if (str.Find('\xC2') != wxNOT_FOUND)
         str.Remove(str.Find('\xC2'), 1);
```

mmalmi@cc.hut.fi wrote:
> I didn't change it knowingly, must have been some encoding problem.
>

```
>> What was the reason for this change?
>>
>> #if !wxUSE_UNICODE
>> ...
>>     if (str.Find('Â') != wxNOT_FOUND)
>>         str.Remove(str.Find('Â'), 1);
>> to:
>>     if (str.Find('ï¿½') != wxNOT_FOUND)
>>         str.Remove(str.Find('ï¿½'), 1);
>>
>> wxFormBuilder turns the (c) symbol into UTF-8 automatically.  On
>> wxWidgets-2.8.9 ansi, it shows as a copyright symbol with an extra
>> trash character, which this hack fixes up for the non-unicode (ansi)
>> case.
>
>
>
```

Email #153

Date: Sun, 07 Feb 2010 06:12:04 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: JSON-RPC status

To: Martti Malmi <mmalmi@cc.hut.fi>

```
The JSON-RPC implementation is going well.  I'm using boost::asio for
sockets.  JSON-RPC can be plain socket or HTTP, but it seems most other
implementations are HTTP, so I made my own simple HTTP headers.  For
JSON parsing I'm using JSON Spirit, which makes full use of STL and has
been really nice to use.  It's header-only so it's no added build work,
and small enough to just add it to our source tree.  MIT license.  This
should all be working in a few more days.

The forum sure is taking off.  I didn't expect to have so much activity
so fast.
```

Email #154

Date: Sun, 07 Feb 2010 12:45:53 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

```
That's great! I'll start familiarizing myself with Liberty Reserve and
its api.

> The JSON-RPC implementation is going well.  I'm using boost::asio for
> sockets.  JSON-RPC can be plain socket or HTTP, but it seems most other
> implementations are HTTP, so I made my own simple HTTP headers.  For
> JSON parsing I'm using JSON Spirit, which makes full use of STL and has
> been really nice to use.  It's header-only so it's no added build work,
> and small enough to just add it to our source tree.  MIT license.  This
> should all be working in a few more days.
>
> The forum sure is taking off.  I didn't expect to have so much activity
> so fast.
```

Email #155

Date: Mon, 08 Feb 2010 15:28:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Translation

To: Martti Malmi <mmalmi@cc.hut.fi>

```
Does Drupal have any special multi-language support, or do you just
create copies of pages by hand?

BlueSky offered to do translation on the forum.  If you create a
www.bitcoin.org/zh/ copy of the site and give him an account with just
the ability to create new pages and edit text, he'll probably translate
the site into Chinese for you and maybe maintain it.
```

Email #156

Date: Tue, 09 Feb 2010 17:42:06 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

```
Drupal supports multiple languages. I didn't yet figure out how to
make it automatically show the translation at bitcoin.org/zh-hans
though.

> Does Drupal have any special multi-language support, or do you just
> create copies of pages by hand?
>
> BlueSky offered to do translation on the forum.  If you create a
> www.bitcoin.org/zh/ copy of the site and give him an account with just
> the ability to create new pages and edit text, he'll probably translate
> the site into Chinese for you and maybe maintain it.
```

Email #157

Date: Thu, 11 Feb 2010 20:50:12 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

```
I got the translations working correctly, now it should automatically
detect the language from the browser settings. Choosing manually is of
course also possible. I asked the translators to send me their
translations as pm or e-mail. I guess I'll make a Finnish translation
myself at some point. Multiple translations add to the site's
credibility.

Drupal is asking to do a security update. Do we have other customized
files we need to backup than those located in the "sites" directory?
```

Email #158

Date: Thu, 11 Feb 2010 22:58:29 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

To: mmalmi@cc.hut.fi

I didn't make any changes to Drupal code. The only thing other than installing themes was the .htaccess file (which really is needed, it didn't work in the global config file).

It was only SMF where I made some PHP changes.

You might find it preferable not to translate it into your own language. Often the standard answer about legalities is that it's only intended for people in other countries. Translating it into your home language weakens that argument.

mmalmi@cc.hut.fi wrote:
> I got the translations working correctly, now it should automatically
> detect the language from the browser settings. Choosing manually is of
> course also possible. I asked the translators to send me their
> translations as pm or e-mail. I guess I'll make a Finnish translation
> myself at some point. Multiple translations add to the site's credibility.
>
> Drupal is asking to do a security update. Do we have other customized
> files we need to backup than those located in the "sites" directory?
>

Email #159

Date: Fri, 12 Feb 2010 12:06:43 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Translation

I'm not too worried about that, since I'm not doing anything illegal, even with my exchange service. If I were, it wouldn't help me that I'm only offering the service for foreigners. Things may of course be different under other jurisdictions, but that's how it is in my country. The law monopoly here is less uncivilized than many others.

> You might find it preferable not to translate it into your own
> language. Often the standard answer about legalities is that it's only
> intended for people in other countries. Translating it into your home
> language weakens that argument.

Email #160

Date: Sat, 13 Feb 2010 01:08:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

To: mmalmi@cc.hut.fi

I uploaded my JSON-RPC and command line implementation to SVN. I'm waiting to post on the forum when I've had more time to think about the commands. At least some method names are going to change.

To enable the RPC server, add the switch -server. It's not on by default.

Client commands are without any switches, as such:
```
bitcoin getblockcount
bitcoin getdifficulty
bitcoin getnewaddress somelabel
bitcoin sendtoaddress 1DvqsbZ... 1.00
bitcoin getallpayments 0
bitcoin stop
```

Applications would normally use JSON-RPC directly, not command line.

I haven't tested my JSON-RPC server with anything else yet. If you do,
please tell me how it goes. You're using Python, right?

Getting the Linux version to run without the GTK installed will be a
separate task.

mmalmi@cc.hut.fi wrote:
> That's great! I'll start familiarizing myself with Liberty Reserve and
> its api.
>
>> The JSON-RPC implementation is going well. I'm using boost::asio for
>> sockets. JSON-RPC can be plain socket or HTTP, but it seems most other
>> implementations are HTTP, so I made my own simple HTTP headers. For
>> JSON parsing I'm using JSON Spirit, which makes full use of STL and has
>> been really nice to use. It's header-only so it's no added build work,
>> and small enough to just add it to our source tree. MIT license. This
>> should all be working in a few more days.
>>
>> The forum sure is taking off. I didn't expect to have so much activity
>> so fast.
>
>
>

Email #161

Date: Sun, 14 Feb 2010 19:55:51 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

> I haven't tested my JSON-RPC server with anything else yet. If you do,
> please tell me how it goes. You're using Python, right?
>
> Getting the Linux version to run without the GTK installed will be a
> separate task.

Yes, using Python. I didn't test the JSON-RPC yet as I don't have
Bitcoin running on the vps yet. It doesn't work without a window
manager even if GTK libraries are installed. I asked about it at
wxWidgets forum (http://wxforum.shadonet.com/viewtopic.php?t=26954)
but they didn't have much clue. Maybe we'll just need to make two
different binaries.

Email #162

Date: Sun, 14 Feb 2010 19:59:12 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Exchange options

I'm moving in the direction of making transactions automated only when
the customer buys coins with SMS payment provided by ZayPay. Pecunix
is the only reliable and practical enough e-currency that I'd store my
reserves in, but the exchange fees are quite high (about 5%).

When I'm buying coins, my recommended payment method would be IBAN

```
transfer. I could also say "contact us if you want to buy/sell with
any other payment option" and handle each order separately. I could
manually accept single orders with even PayPal, as long as I don't
store my money there and the customer pays the fees.
```

Email #163

Date: Sun, 14 Feb 2010 21:48:31 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

To: mmalmi@cc.hut.fi

```
mmalmi@cc.hut.fi wrote:
>> I haven't tested my JSON-RPC server with anything else yet.  If you do,
>> please tell me how it goes.  You're using Python, right?
>>
>> Getting the Linux version to run without the GTK installed will be a
>> separate task.
>
> Yes, using Python. I didn't test the JSON-RPC yet as I don't have
> Bitcoin running on the vps yet. It doesn't work without a window manager
> even if GTK libraries are installed. I asked about it at wxWidgets forum
> (http://wxforum.shadonet.com/viewtopic.php?t=26954) but they didn't have
> much clue. Maybe we'll just need to make two different binaries.

I will probably relent and do that.  I can move init and shutdown into
init.cpp or start.cpp or something, link only wxbase and not link ui.o
and uibase.o.

wxWidgets is mostly Windows people, they wouldn't know much about GTK.

Don't you have an Ubuntu laptop you can test and compile on so you don't
have to toy with the vps?
```

Email #164

Date: Mon, 15 Feb 2010 15:00:34 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

```
> Don't you have an Ubuntu laptop you can test and compile on so you
> don't have to toy with the vps?

Yes. Tested with Python's JSON-RPC, and seems to work fine! Really
easy to use.
```

Email #165

Date: Mon, 15 Feb 2010 18:11:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

To: mmalmi@cc.hut.fi

```
mmalmi@cc.hut.fi wrote:
>> Don't you have an Ubuntu laptop you can test and compile on so you
>> don't have to toy with the vps?
>
> Yes. Tested with Python's JSON-RPC, and seems to work fine! Really easy
```

```
> to use.

Hurray, I got it on the first go.

Could you send me the Python code you used?  So if I do some testing
later I don't have to figure it out myself.
```

Email #166

Date: Mon, 15 Feb 2010 20:33:23 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: JSON-RPC status

```
> mmalmi@cc.hut.fi wrote:
>>> Don't you have an Ubuntu laptop you can test and compile on so you
>>> don't have to toy with the vps?
>>
>> Yes. Tested with Python's JSON-RPC, and seems to work fine! Really
>> easy to use.
>
> Hurray, I got it on the first go.
>
> Could you send me the Python code you used?  So if I do some testing
> later I don't have to figure it out myself.

Just downloaded the python-json-rpc
(http://json-rpc.org/wiki/python-json-rpc) from their svn and tested
by talking to the Python interpreter directly. Like this:

pythons = ServiceProxy("http://localhost:8332")
s.getblockcount()
```

Email #167

Date: Wed, 17 Feb 2010 19:32:04 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Non-GUI option

```
Just a few clues I've found about running the same binary without a GUI:

1) GTK supports running a program without display:
http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check. This
doesn't tell if it's possible in wxWidgets though.

2) wxAppConsole of wx 2.9 might be useful somehow. Just replacing
wxApp with wxAppConsole doesn't work, I'm not sure how it should be
used. It's not very well documented.

3) Another option might be to use IMPLEMENT_APP_NO_MAIN() and make our
own main method.
```

Email #168

Date: Mon, 22 Feb 2010 20:17:42 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

To: mmalmi@cc.hut.fi

```
mmalmi@cc.hut.fi wrote:
> Just a few clues I've found about running the same binary without a GUI:
>
> 1) GTK supports running a program without display:
> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
> This doesn't tell if it's possible in wxWidgets though.

I see it calls gtk-init-check in wxApp::Initialize.

I can subclass Initialize, call the original one while suppressing the
error message and ignore the return value.  It seems to be working.

Any suggestions what to name the command line switches and how to
describe them?  Is there any traditional standard?  I'm currently using:
-daemon (or -d)   (Enables RPC and runs in the background)
-server           (Enables RPC)
```

Email #169

Date: Tue, 23 Feb 2010 01:41:01 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

To: Martti Malmi <mmalmi@cc.hut.fi>

```
>> Just a few clues I've found about running the same binary without a GUI:
>>
>> 1) GTK supports running a program without display:
>> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
>> This doesn't tell if it's possible in wxWidgets though.
>
> I see it calls gtk-init-check in wxApp::Initialize.
>
> I can subclass Initialize, call the original one while suppressing the
> error message and ignore the return value.  It seems to be working.

This is working.  A few more things and I'll upload it.

We'll need to tell people to install the GTK libraries.  Do you remember
the apt-get command to install GTK, and can you install it without
having a GUI installed?
```

Email #170

Date: Tue, 23 Feb 2010 15:19:51 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

```
> mmalmi@cc.hut.fi wrote:
>> Just a few clues I've found about running the same binary without a GUI:
>>
>> 1) GTK supports running a program without display:
>> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
>> This doesn't tell if it's possible in wxWidgets though.
>
> I see it calls gtk-init-check in wxApp::Initialize.
>
> I can subclass Initialize, call the original one while suppressing the
> error message and ignore the return value.  It seems to be working.
>
> Any suggestions what to name the command line switches and how to
```

```
> describe them?  Is there any traditional standard?  I'm currently using:
> -daemon (or -d)   (Enables RPC and runs in the background)
> -server           (Enables RPC)

That seems good, I don't know of any standards about it.
```

Email #171

Date: Tue, 23 Feb 2010 16:47:59 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

```
>>> Just a few clues I've found about running the same binary without a GUI:
>>>
>>> 1) GTK supports running a program without display:
>>> http://library.gnome.org/devel/gtk/2.12/gtk-General.html#gtk-init-check.
>>> This doesn't tell if it's possible in wxWidgets though.
>>
>> I see it calls gtk-init-check in wxApp::Initialize.
>>
>> I can subclass Initialize, call the original one while suppressing
>> the error message and ignore the return value.  It seems to be
>> working.
>
> This is working.  A few more things and I'll upload it.
>
> We'll need to tell people to install the GTK libraries.  Do you
> remember the apt-get command to install GTK, and can you install it
> without having a GUI installed?

It was probably apt-get install libgtk2.0-0. You can search for
available packages like this: "apt-cache search libgtk".

I'll give Drupal accounts to the bitcoin.org translators, so they can
keep the translations up to date.
```

Email #172

Date: Wed, 24 Feb 2010 06:34:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Non-GUI option

To: mmalmi@cc.hut.fi

```
> I'll give Drupal accounts to the bitcoin.org translators, so they can
> keep the translations up to date.

Good, that gives them a little sense of ownership and responsibility.

I hope we get at least one .mo file for the software translation in time
to put into the 0.3 release.
```

Email #173

Date: Sun, 28 Feb 2010 06:12:44 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Bitcoind

I tried debugging my build of bitcoind with ddd debugger, but didn't have much success yet. It always ends up taking all the system's memory and finally crashes. Could you please send me again the latest 64 bit build of bitcoind, so I can see if the problem is about my build?

Email #174

Date: Sun, 28 Feb 2010 14:47:01 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

I put it at bitcoin.org/download/linux64-0.2.7.1.tar.gz. You can delete it when you've got it.

I thought about what might cause the problem you're having and made a change that this build includes. This might have been unsafe code, although it would probably always get lucky.

```
in util.cpp, old:
const char* wxGetTranslation(const char* pszEnglish)
{
     // Wrapper of wxGetTranslation returning the same const char* type as was passed in
     static CCriticalSection cs;
     CRITICAL_BLOCK(cs)
     {
         // Look in cache
         static map<string, char*> mapCache;
         map<string, char*>::iterator mi = mapCache.find(pszEnglish);
         if (mi != mapCache.end())
             return (*mi).second;

         // wxWidgets translation
         const char* pszTranslated = wxGetTranslation(wxString(pszEnglish, wxConvUTF8)).utf8_str();

         // We don't cache unknown strings because caller might be passing in a
         // dynamic string and we would keep allocating memory for each variation.
         if (strcmp(pszEnglish, pszTranslated) == 0)
             return pszEnglish;

         // Add to cache, memory doesn't need to be freed.  We only cache because
         // we must pass back a pointer to permanently allocated memory.
         char* pszCached = new char[strlen(pszTranslated)+1];
         strcpy(pszCached, pszTranslated);
         mapCache[pszEnglish] = pszCached;
         return pszCached;
     }
     return NULL;
}

new:
const char* wxGetTranslation(const char* pszEnglish)
{
     // Wrapper of wxGetTranslation returning the same const char* type as was passed in
     static CCriticalSection cs;
     CRITICAL_BLOCK(cs)
```

```
    {
        // Look in cache
        static map<string, char*> mapCache;
        map<string, char*>::iterator mi = mapCache.find(pszEnglish);
        if (mi != mapCache.end())
            return (*mi).second;

        // wxWidgets translation
        wxString strTranslated = wxGetTranslation(wxString(pszEnglish,
wxConvUTF8));

        // We don't cache unknown strings because caller might be
passing in a
        // dynamic string and we would keep allocating memory for each
variation.
        if (strcmp(pszEnglish, strTranslated.utf8_str()) == 0)
            return pszEnglish;

        // Add to cache, memory doesn't need to be freed.  We only
cache because
        // we must pass back a pointer to permanently allocated memory.
        char* pszCached = new char[strlen(strTranslated.utf8_str())+1];
        strcpy(pszCached, strTranslated.utf8_str());
        mapCache[pszEnglish] = pszCached;
        return pszCached;
    }
    return NULL;
}

If you still suspect this code, for testing you could change it to:
const char* wxGetTranslation(const char* pszEnglish)
{
    return pszEnglish;
}


mmalmi@cc.hut.fi wrote:
> I tried debugging my build of bitcoind with ddd debugger, but didn't
> have much success yet. It always ends up taking all the system's memory
> and finally crashes. Could you please send me again the latest 64 bit
> build of bitcoind, so I can see if the problem is about my build?
>
```

Email #175

Date: Sun, 28 Feb 2010 20:09:07 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

```
Could you send me the debug.log?

mmalmi@cc.hut.fi wrote:
> I tried debugging my build of bitcoind with ddd debugger, but didn't
> have much success yet. It always ends up taking all the system's memory
> and finally crashes. Could you please send me again the latest 64 bit
> build of bitcoind, so I can see if the problem is about my build?
>
```

Email #176

Date: Tue, 02 Mar 2010 21:33:24 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoind

```
Here goes. I forgot to mention the crash error message:

terminate called after throwing an instance of 'std::bad_alloc'
what():  std::bad_alloc

> Could you send me the debug.log?
>
> mmalmi@cc.hut.fi wrote:
>> I tried debugging my build of bitcoind with ddd debugger, but
>> didn't have much success yet. It always ends up taking all the
>> system's memory and finally crashes. Could you please send me again
>>  the latest 64 bit build of bitcoind, so I can see if the problem
>> is  about my build?
>>
```

Email #177
Date: Tue, 02 Mar 2010 21:36:10 +0200
From: mmalmi@cc.hut.fi
To: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoind

```
This was from the compilation you sent, the same problem occurred with it.

> Here goes. I forgot to mention the crash error message:
>
> terminate called after throwing an instance of 'std::bad_alloc'
> what():  std::bad_alloc
>
>> Could you send me the debug.log?
>>
>> mmalmi@cc.hut.fi wrote:
>>> I tried debugging my build of bitcoind with ddd debugger, but
>>> didn't have much success yet. It always ends up taking all the
>>> system's memory and finally crashes. Could you please send me
>>> again   the latest 64 bit build of bitcoind, so I can see if the
>>> problem  is  about my build?
>>>
```

Email #178
Date: Tue, 02 Mar 2010 22:27:22 +0000
From: Satoshi Nakamoto <satoshin@gmx.com>
Subject: Re: Bitcoind
To: mmalmi@cc.hut.fi

```
Does it still do it if you didn't do getinfo?

You could comment out the CreateThreads listed below, then re-enable
them one at a time until it does it again.  Then we would know which
```

```
thread the problem is in.

net.cpp, under // Start threads
     CreateThread(ThreadIRCSeed, NULL)
     CreateThread(ThreadSocketHandler, NULL, true)
     CreateThread(ThreadOpenConnections, NULL)
     CreateThread(ThreadMessageHandler, NULL)

init.cpp:
     CreateThread(ThreadRPCServer, NULL);

mmalmi@cc.hut.fi wrote:
> Here goes. I forgot to mention the crash error message:
>
> terminate called after throwing an instance of 'std::bad_alloc'
> what():  std::bad_alloc
>
>> Could you send me the debug.log?
>>
>> mmalmi@cc.hut.fi wrote:
>>> I tried debugging my build of bitcoind with ddd debugger, but  didn't
>>> have much success yet. It always ends up taking all the  system's
>>> memory and finally crashes. Could you please send me again  the
>>> latest 64 bit build of bitcoind, so I can see if the problem is
>>> about my build?
>>>
>
>
>
```

Email #179

Date: Wed, 03 Mar 2010 03:50:39 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

```
I get the error regardless of the getinfo. Commenting out
ThreadIRCSeed fixed the problem.

> Does it still do it if you didn't do getinfo?
>
> You could comment out the CreateThreads listed below, then re-enable
> them one at a time until it does it again.  Then we would know which
> thread the problem is in.
>
> net.cpp, under // Start threads
>     CreateThread(ThreadIRCSeed, NULL)
>     CreateThread(ThreadSocketHandler, NULL, true)
>     CreateThread(ThreadOpenConnections, NULL)
>     CreateThread(ThreadMessageHandler, NULL)
>
> init.cpp:
>     CreateThread(ThreadRPCServer, NULL);
>
> mmalmi@cc.hut.fi wrote:
>> Here goes. I forgot to mention the crash error message:
>>
>> terminate called after throwing an instance of 'std::bad_alloc'
>> what():  std::bad_alloc
>>
>>> Could you send me the debug.log?
```

```
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>> didn't have much success yet. It always ends up taking all the
>>>> system's memory and finally crashes. Could you please send me
>>>> again  the latest 64 bit build of bitcoind, so I can see if the
>>>> problem is  about my build?
>>>>
>>
>>
>>
```

Email #180

Date: Wed, 03 Mar 2010 03:54:52 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

```
That narrows it down a lot.  It didn't print any IRC activity in
debug.log, so I guess it couldn't have gotten past the RecvUntil.
Eyeballing it I don't see anything obvious.  I guess it would have to be
either in ConnectSocket or RecvUntil.

Try it with the attached irc.cpp and net.cpp and send me the debug.log.

Or you could run it in gdb and step through ThreadIRCSeed
gdb --args bitcoin [switches]
b ThreadIRCSeed
run
step
or u to step over and up out of routines.

mmalmi@cc.hut.fi wrote:
> I get the error regardless of the getinfo. Commenting out ThreadIRCSeed
> fixed the problem.
>
>> Does it still do it if you didn't do getinfo?
>>
>> You could comment out the CreateThreads listed below, then re-enable
>> them one at a time until it does it again.  Then we would know which
>> thread the problem is in.
>>
>> net.cpp, under // Start threads
>>     CreateThread(ThreadIRCSeed, NULL)
>>     CreateThread(ThreadSocketHandler, NULL, true)
>>     CreateThread(ThreadOpenConnections, NULL)
>>     CreateThread(ThreadMessageHandler, NULL)
>>
>> init.cpp:
>>     CreateThread(ThreadRPCServer, NULL);
>>
>> mmalmi@cc.hut.fi wrote:
>>> Here goes. I forgot to mention the crash error message:
>>>
>>> terminate called after throwing an instance of 'std::bad_alloc'
>>> what():  std::bad_alloc
>>>
>>>> Could you send me the debug.log?
>>>>
```

```
>>>> mmalmi@cc.hut.fi wrote:
>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>> didn't have much success yet. It always ends up taking all the
>>>>> system's memory and finally crashes. Could you please send me
>>>>> again  the latest 64 bit build of bitcoind, so I can see if the
>>>>> problem is  about my build?
>>>>>
>>>
>>>
>>>
>
>
>
```

Email #181

Date: Wed, 03 Mar 2010 14:32:01 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

```
debug.log attached

> That narrows it down a lot.  It didn't print any IRC activity in
> debug.log, so I guess it couldn't have gotten past the RecvUntil.
> Eyeballing it I don't see anything obvious.  I guess it would have to
> be either in ConnectSocket or RecvUntil.
>
> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>
> Or you could run it in gdb and step through ThreadIRCSeed
> gdb --args bitcoin [switches]
> b ThreadIRCSeed
> run
> step
> or u to step over and up out of routines.
>
> mmalmi@cc.hut.fi wrote:
>> I get the error regardless of the getinfo. Commenting out
>> ThreadIRCSeed fixed the problem.
>>
>>> Does it still do it if you didn't do getinfo?
>>>
>>> You could comment out the CreateThreads listed below, then re-enable
>>> them one at a time until it does it again.  Then we would know which
>>> thread the problem is in.
>>>
>>> net.cpp, under // Start threads
>>>    CreateThread(ThreadIRCSeed, NULL)
>>>    CreateThread(ThreadSocketHandler, NULL, true)
>>>    CreateThread(ThreadOpenConnections, NULL)
>>>    CreateThread(ThreadMessageHandler, NULL)
>>>
>>> init.cpp:
>>>    CreateThread(ThreadRPCServer, NULL);
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> Here goes. I forgot to mention the crash error message:
>>>>
>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>> what():  std::bad_alloc
>>>>
```

```
>>>>> Could you send me the debug.log?
>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>  didn't have much success yet. It always ends up taking all the
>>>>>>    system's memory and finally crashes. Could you please send
>>>>>> me   again  the latest 64 bit build of bitcoind, so I can see
>>>>>> if the   problem is  about my build?
>>>>>>
>>>>
>>>>
>>>>
>>
>>
>>
```

Email #182

Date: Wed, 03 Mar 2010 17:15:28 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

```
It's in RecvUntil, but I still can't see anything wrong with it.  The
only thing I can think of is if the socket is receiving a spew of
characters.

Try this irc.cpp.  debug.log may grow rapidly so be ready to kill it.

mmalmi@cc.hut.fi wrote:
> debug.log attached
>
>> That narrows it down a lot.  It didn't print any IRC activity in
>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>> Eyeballing it I don't see anything obvious.  I guess it would have to
>> be either in ConnectSocket or RecvUntil.
>>
>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>
>> Or you could run it in gdb and step through ThreadIRCSeed
>> gdb --args bitcoin [switches]
>> b ThreadIRCSeed
>> run
>> step
>> or u to step over and up out of routines.
>>
>> mmalmi@cc.hut.fi wrote:
>>> I get the error regardless of the getinfo. Commenting out
>>> ThreadIRCSeed fixed the problem.
>>>
>>>> Does it still do it if you didn't do getinfo?
>>>>
>>>> You could comment out the CreateThreads listed below, then re-enable
>>>> them one at a time until it does it again.  Then we would know which
>>>> thread the problem is in.
>>>>
>>>> net.cpp, under // Start threads
>>>>    CreateThread(ThreadIRCSeed, NULL)
>>>>    CreateThread(ThreadSocketHandler, NULL, true)
>>>>    CreateThread(ThreadOpenConnections, NULL)
```

```
>>>>    CreateThread(ThreadMessageHandler, NULL)
>>>>
>>>> init.cpp:
>>>>    CreateThread(ThreadRPCServer, NULL);
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> Here goes. I forgot to mention the crash error message:
>>>>>
>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>> what():  std::bad_alloc
>>>>>
>>>>>> Could you send me the debug.log?
>>>>>>
>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>  didn't have much success yet. It always ends up taking all the
>>>>>>>    system's memory and finally crashes. Could you please send
>>>>>>> me   again  the latest 64 bit build of bitcoind, so I can see if
>>>>>>> the   problem is  about my build?
>>>>>>>
>>>>>
>>>>>
>>>>>
>>>
>>>
>>>
>
>
>
```

Email #183

Date: Fri, 05 Mar 2010 00:27:08 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

```
Here's the debug.log. I stopped bitcoind before it took up all the memory.

> It's in RecvUntil, but I still can't see anything wrong with it.  The
> only thing I can think of is if the socket is receiving a spew of
> characters.
>
> Try this irc.cpp.  debug.log may grow rapidly so be ready to kill it.
>
> mmalmi@cc.hut.fi wrote:
>> debug.log attached
>>
>>> That narrows it down a lot.  It didn't print any IRC activity in
>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>> Eyeballing it I don't see anything obvious.  I guess it would have to
>>> be either in ConnectSocket or RecvUntil.
>>>
>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>
>>> Or you could run it in gdb and step through ThreadIRCSeed
>>> gdb --args bitcoin [switches]
>>> b ThreadIRCSeed
>>> run
>>> step
>>> or u to step over and up out of routines.
>>>
```

```
>>> mmalmi@cc.hut.fi wrote:
>>>> I get the error regardless of the getinfo. Commenting out
>>>> ThreadIRCSeed fixed the problem.
>>>>
>>>>> Does it still do it if you didn't do getinfo?
>>>>>
>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>> them one at a time until it does it again.  Then we would know which
>>>>> thread the problem is in.
>>>>>
>>>>> net.cpp, under // Start threads
>>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>>
>>>>> init.cpp:
>>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>
>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>> what():  std::bad_alloc
>>>>>>
>>>>>>> Could you send me the debug.log?
>>>>>>>
>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>     didn't have much success yet. It always ends up taking
>>>>>>>> all  the   system's memory and finally crashes. Could you
>>>>>>>> please  send me   again  the latest 64 bit build of bitcoind,
>>>>>>>> so I  can see if the  problem is  about my build?
>>>>>>>>
>>>>>>
>>>>>>
>>>>>>
>>>>
>>>>
>>>>
>>
>>
>>
```

[Email #184]

Date: Fri, 05 Mar 2010 02:09:02 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

```
Here's another test run debug.log I got when debugging with gdb. The
program started eating memory after the debug line "irc 8" and within
a few seconds crashed with "terminate called after throwing an
instance of 'std::bad_alloc'".

> It's in RecvUntil, but I still can't see anything wrong with it.  The
> only thing I can think of is if the socket is receiving a spew of
> characters.
>
```

> Try this irc.cpp. debug.log may grow rapidly so be ready to kill it.
>
> mmalmi@cc.hut.fi wrote:
>> debug.log attached
>>
>>> That narrows it down a lot. It didn't print any IRC activity in
>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>> be either in ConnectSocket or RecvUntil.
>>>
>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>
>>> Or you could run it in gdb and step through ThreadIRCSeed
>>> gdb --args bitcoin [switches]
>>> b ThreadIRCSeed
>>> run
>>> step
>>> or u to step over and up out of routines.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> I get the error regardless of the getinfo. Commenting out
>>>> ThreadIRCSeed fixed the problem.
>>>>
>>>>> Does it still do it if you didn't do getinfo?
>>>>>
>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>> them one at a time until it does it again. Then we would know which
>>>>> thread the problem is in.
>>>>>
>>>>> net.cpp, under // Start threads
>>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>>
>>>>> init.cpp:
>>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>
>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>> what(): std::bad_alloc
>>>>>>
>>>>>>> Could you send me the debug.log?
>>>>>>>
>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>   didn't have much success yet. It always ends up taking
>>>>>>>> all the   system's memory and finally crashes. Could you
>>>>>>>> please send me   again the latest 64 bit build of bitcoind,
>>>>>>>> so I can see if the problem is about my build?
>>>>>>>>
>>>>>>
>>>>>>
>>>>>>
>>>>
>>>>
>>>>
>>
>>
>>

Email #185

Date: Fri, 05 Mar 2010 00:42:16 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

```
It's in util.c ParseString.  I'm guessing the problem is incompatibility
between the type "unsigned int" and the type of str.npos, which is
size_type.

Try changing the two "unsigned int"s to "size_type".

old:
void ParseString(const string& str, char c, vector<string>& v)
{
     unsigned int i1 = 0;
     unsigned int i2;
     do
     {
         i2 = str.find(c, i1);
         v.push_back(str.substr(i1, i2-i1));
         i1 = i2+1;
     }
     while (i2 != str.npos);
}

new:
void ParseString(const string& str, char c, vector<string>& v)
{
     size_type i1 = 0;
     size_type i2;
     do
     {
         i2 = str.find(c, i1);
         v.push_back(str.substr(i1, i2-i1));
         i1 = i2+1;
     }
     while (i2 != str.npos);
}


mmalmi@cc.hut.fi wrote:
> Here's another test run debug.log I got when debugging with gdb. The
> program started eating memory after the debug line "irc 8" and within a
> few seconds crashed with "terminate called after throwing an instance of
> 'std::bad_alloc'".
>
>> It's in RecvUntil, but I still can't see anything wrong with it.  The
>> only thing I can think of is if the socket is receiving a spew of
>> characters.
>>
>> Try this irc.cpp.  debug.log may grow rapidly so be ready to kill it.
>>
>> mmalmi@cc.hut.fi wrote:
>>> debug.log attached
>>>
>>>> That narrows it down a lot.  It didn't print any IRC activity in
>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>>> Eyeballing it I don't see anything obvious.  I guess it would have to
>>>> be either in ConnectSocket or RecvUntil.
```

```
>>>>
>>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>>
>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>> gdb --args bitcoin [switches]
>>>> b ThreadIRCSeed
>>>> run
>>>> step
>>>> or u to step over and up out of routines.
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> I get the error regardless of the getinfo. Commenting out
>>>>> ThreadIRCSeed fixed the problem.
>>>>>
>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>
>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>> them one at a time until it does it again.  Then we would know which
>>>>>> thread the problem is in.
>>>>>>
>>>>>> net.cpp, under // Start threads
>>>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>>>
>>>>>> init.cpp:
>>>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>>>
>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>>
>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>> what():  std::bad_alloc
>>>>>>>
>>>>>>>> Could you send me the debug.log?
>>>>>>>>
>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>>     didn't have much success yet. It always ends up taking all
>>>>>>>>> the   system's memory and finally crashes. Could you please
>>>>>>>>> send me   again  the latest 64 bit build of bitcoind, so I  can
>>>>>>>>> see if the  problem is  about my build?
>>>>>>>>>
>>>>>>>
>>>>>>>
>>>>>>>
>>>>>
>>>>>
>>>>>
>>>
>>>
>>>
>>
>>
>>
>
>
>
```

[Email #186]

Date: Fri, 05 Mar 2010 00:54:40 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

```
Actually, please try this instead, this is more correct:

void ParseString(const string& str, char c, vector<string>& v)
{
     string::size_type i1 = 0;
     string::size_type i2;
     loop
     {
         i2 = str.find(c, i1);
         if (i2 == str.npos)
         {
             v.push_back(str.substr(i1));
             return;
         }
         v.push_back(str.substr(i1, i2-i1));
         i1 = i2+1;
     }
}



Satoshi Nakamoto wrote:
> It's in util.c ParseString.  I'm guessing the problem is incompatibility
> between the type "unsigned int" and the type of str.npos, which is
> size_type.
>
> Try changing the two "unsigned int"s to "size_type".
>
> old:
> void ParseString(const string& str, char c, vector<string>& v)
> {
>     unsigned int i1 = 0;
>     unsigned int i2;
>     do
>     {
>         i2 = str.find(c, i1);
>         v.push_back(str.substr(i1, i2-i1));
>         i1 = i2+1;
>     }
>     while (i2 != str.npos);
> }
>
> new:
> void ParseString(const string& str, char c, vector<string>& v)
> {
>     size_type i1 = 0;
>     size_type i2;
>     do
>     {
>         i2 = str.find(c, i1);
>         v.push_back(str.substr(i1, i2-i1));
>         i1 = i2+1;
>     }
>     while (i2 != str.npos);
> }
>
>
> mmalmi@cc.hut.fi wrote:
>> Here's another test run debug.log I got when debugging with gdb. The
>> program started eating memory after the debug line "irc 8" and within
>> a few seconds crashed with "terminate called after throwing an
>> instance of 'std::bad_alloc'".
```

>>
>>> It's in RecvUntil, but I still can't see anything wrong with it. The
>>> only thing I can think of is if the socket is receiving a spew of
>>> characters.
>>>
>>> Try this irc.cpp. debug.log may grow rapidly so be ready to kill it.
>>>
>>> mmalmi@cc.hut.fi wrote:
>>>> debug.log attached
>>>>
>>>>> That narrows it down a lot. It didn't print any IRC activity in
>>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>>>> be either in ConnectSocket or RecvUntil.
>>>>>
>>>>> Try it with the attached irc.cpp and net.cpp and send me the
>>>>> debug.log.
>>>>>
>>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>>> gdb --args bitcoin [switches]
>>>>> b ThreadIRCSeed
>>>>> run
>>>>> step
>>>>> or u to step over and up out of routines.
>>>>>
>>>>> mmalmi@cc.hut.fi wrote:
>>>>>> I get the error regardless of the getinfo. Commenting out
>>>>>> ThreadIRCSeed fixed the problem.
>>>>>>
>>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>>
>>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>>> them one at a time until it does it again. Then we would know which
>>>>>>> thread the problem is in.
>>>>>>>
>>>>>>> net.cpp, under // Start threads
>>>>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>>>>
>>>>>>> init.cpp:
>>>>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>>>>
>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>>>
>>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>>> what(): std::bad_alloc
>>>>>>>>
>>>>>>>>> Could you send me the debug.log?
>>>>>>>>>
>>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>>>   didn't have much success yet. It always ends up taking
>>>>>>>>>> all the   system's memory and finally crashes. Could you
>>>>>>>>>> please send me   again the latest 64 bit build of bitcoind,
>>>>>>>>>> so I can see if the problem is about my build?
>>>>>>>>>>
>>>>>>>>
>>>>>>>>
>>>>>>>>
>>>>>>
>>>>>>

>>>>>>
>>>>
>>>>
>>>>
>>
>>
>>
>
>

Email #187

Date: Fri, 05 Mar 2010 03:33:34 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

```
Great! Works fine now.

> Actually, please try this instead, this is more correct:
>
> void ParseString(const string& str, char c, vector<string>& v)
> {
>     string::size_type i1 = 0;
>     string::size_type i2;
>     loop
>     {
>         i2 = str.find(c, i1);
>         if (i2 == str.npos)
>         {
>             v.push_back(str.substr(i1));
>             return;
>         }
>         v.push_back(str.substr(i1, i2-i1));
>         i1 = i2+1;
>     }
> }
>
>
>
> Satoshi Nakamoto wrote:
>> It's in util.c ParseString.  I'm guessing the problem is
>> incompatibility between the type "unsigned int" and the type of
>> str.npos, which is size_type.
>>
>> Try changing the two "unsigned int"s to "size_type".
>>
>> old:
>> void ParseString(const string& str, char c, vector<string>& v)
>> {
>>    unsigned int i1 = 0;
>>    unsigned int i2;
>>    do
>>    {
>>        i2 = str.find(c, i1);
>>        v.push_back(str.substr(i1, i2-i1));
>>        i1 = i2+1;
>>    }
>>    while (i2 != str.npos);
>> }
>>
>> new:
```

```
>> void ParseString(const string& str, char c, vector<string>& v)
>> {
>>    size_type i1 = 0;
>>    size_type i2;
>>    do
>>    {
>>        i2 = str.find(c, i1);
>>        v.push_back(str.substr(i1, i2-i1));
>>        i1 = i2+1;
>>    }
>>    while (i2 != str.npos);
>> }
>>
>>
>> mmalmi@cc.hut.fi wrote:
>>> Here's another test run debug.log I got when debugging with gdb.
>>> The program started eating memory after the debug line "irc 8" and
>>>  within a few seconds crashed with "terminate called after
>>> throwing  an instance of 'std::bad_alloc'".
>>>
>>>> It's in RecvUntil, but I still can't see anything wrong with it.  The
>>>> only thing I can think of is if the socket is receiving a spew of
>>>> characters.
>>>>
>>>> Try this irc.cpp.  debug.log may grow rapidly so be ready to kill it.
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> debug.log attached
>>>>>
>>>>>> That narrows it down a lot.  It didn't print any IRC activity in
>>>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>>>>> Eyeballing it I don't see anything obvious.  I guess it would have to
>>>>>> be either in ConnectSocket or RecvUntil.
>>>>>>
>>>>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>>>>
>>>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>>>> gdb --args bitcoin [switches]
>>>>>> b ThreadIRCSeed
>>>>>> run
>>>>>> step
>>>>>> or u to step over and up out of routines.
>>>>>>
>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> I get the error regardless of the getinfo. Commenting out
>>>>>>> ThreadIRCSeed fixed the problem.
>>>>>>>
>>>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>>>
>>>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>>>> them one at a time until it does it again.  Then we would know which
>>>>>>>> thread the problem is in.
>>>>>>>>
>>>>>>>> net.cpp, under // Start threads
>>>>>>>>  CreateThread(ThreadIRCSeed, NULL)
>>>>>>>>  CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>>>  CreateThread(ThreadOpenConnections, NULL)
>>>>>>>>  CreateThread(ThreadMessageHandler, NULL)
>>>>>>>>
>>>>>>>> init.cpp:
>>>>>>>>  CreateThread(ThreadRPCServer, NULL);
>>>>>>>>
>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>> Here goes. I forgot to mention the crash error message:
```

```
>>>>>>>>>
>>>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>>>> what():  std::bad_alloc
>>>>>>>>>
>>>>>>>>>> Could you send me the debug.log?
>>>>>>>>>>
>>>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger,
>>>>>>>>>>> but    didn't have much success yet. It always ends up
>>>>>>>>>>> taking all  the   system's memory and finally crashes.
>>>>>>>>>>> Could you please  send me   again  the latest 64 bit build
>>>>>>>>>>>  of bitcoind, so I  can see if the  problem is  about my
>>>>>>>>>>> build?
>>>>>>>>>>>
>>>>>>>>>
>>>>>>>>>
>>>>>>>>>
>>>>>>>>
>>>>>>>>
>>>>>>>>
>>>>>>
>>>>>>
>>>>>>
>>>
>>>
>>>
>>
>>
```

Email #188

Date: Fri, 05 Mar 2010 01:42:00 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Bitcoind

To: mmalmi@cc.hut.fi

```
I confirmed that ParseString has this problem, and uploaded the fixed
util.cpp to SVN.

string::npos == -1

Comparing unsigned int -1 (0xffffffff) with long unsigned int -1
(0xffffffffffffffff) results in the unsigned int being promoted to
64-bit, which is 0x00000000ffffffff != 0xffffffffffffffff.

mmalmi@cc.hut.fi wrote:
> Here's another test run debug.log I got when debugging with gdb. The
> program started eating memory after the debug line "irc 8" and within a
> few seconds crashed with "terminate called after throwing an instance of
> 'std::bad_alloc'".
>
>> It's in RecvUntil, but I still can't see anything wrong with it.  The
>> only thing I can think of is if the socket is receiving a spew of
>> characters.
>>
>> Try this irc.cpp.  debug.log may grow rapidly so be ready to kill it.
>>
>> mmalmi@cc.hut.fi wrote:
>>> debug.log attached
>>>
```

>>>> That narrows it down a lot. It didn't print any IRC activity in
>>>> debug.log, so I guess it couldn't have gotten past the RecvUntil.
>>>> Eyeballing it I don't see anything obvious. I guess it would have to
>>>> be either in ConnectSocket or RecvUntil.
>>>>
>>>> Try it with the attached irc.cpp and net.cpp and send me the debug.log.
>>>>
>>>> Or you could run it in gdb and step through ThreadIRCSeed
>>>> gdb --args bitcoin [switches]
>>>> b ThreadIRCSeed
>>>> run
>>>> step
>>>> or u to step over and up out of routines.
>>>>
>>>> mmalmi@cc.hut.fi wrote:
>>>>> I get the error regardless of the getinfo. Commenting out
>>>>> ThreadIRCSeed fixed the problem.
>>>>>
>>>>>> Does it still do it if you didn't do getinfo?
>>>>>>
>>>>>> You could comment out the CreateThreads listed below, then re-enable
>>>>>> them one at a time until it does it again. Then we would know which
>>>>>> thread the problem is in.
>>>>>>
>>>>>> net.cpp, under // Start threads
>>>>>>   CreateThread(ThreadIRCSeed, NULL)
>>>>>>   CreateThread(ThreadSocketHandler, NULL, true)
>>>>>>   CreateThread(ThreadOpenConnections, NULL)
>>>>>>   CreateThread(ThreadMessageHandler, NULL)
>>>>>>
>>>>>> init.cpp:
>>>>>>   CreateThread(ThreadRPCServer, NULL);
>>>>>>
>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>> Here goes. I forgot to mention the crash error message:
>>>>>>>
>>>>>>> terminate called after throwing an instance of 'std::bad_alloc'
>>>>>>> what(): std::bad_alloc
>>>>>>>
>>>>>>>> Could you send me the debug.log?
>>>>>>>>
>>>>>>>> mmalmi@cc.hut.fi wrote:
>>>>>>>>> I tried debugging my build of bitcoind with ddd debugger, but
>>>>>>>>>   didn't have much success yet. It always ends up taking all
>>>>>>>>> the   system's memory and finally crashes. Could you please
>>>>>>>>> send me   again the latest 64 bit build of bitcoind, so I can
>>>>>>>>> see if the problem is about my build?
>>>>>>>>>
>>>>>>>
>>>>>>>
>>>>>>>
>>>>>
>>>>>
>>>>>
>>>
>>>
>>>
>
>
>

[Email #189]

Date: Sat, 06 Mar 2010 06:39:53 +0000

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Blog

To: Martti Malmi <mmalmi@cc.hut.fi>

```
There's a blog writer who wants to write a story about Bitcoin, but I
don't have time right now to answer his questions.  Would you be
interested in answering his questions if I refer him to you?  We might
get a good link out of it.

The blog is
http://themonetaryfuture.blogspot.com
```

Email #190

Date: Sun, 07 Mar 2010 02:46:35 +0200

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Blog

```
Yes, I could do that.

> There's a blog writer who wants to write a story about Bitcoin, but I
> don't have time right now to answer his questions.  Would you be
> interested in answering his questions if I refer him to you?  We might
> get a good link out of it.
>
> The blog is
> http://themonetaryfuture.blogspot.com
```

Email #191

Date: Fri, 14 May 2010 09:16:52 +0300

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Status update

```
Hi!

How are you doing? Haven't seen you around in a while.

I've been at full-time work lately, and will be until the end of June,
so I haven't had that much time to work with Bitcoin or my exchange
service. I have a working beta of my service though, and a few weeks
ago made my first transaction: sold 10,000 btc for 20 euros via EU
bank transfer. Maybe I can make it public soon.

I divided the forum into 6 boards, which are Bitcoin Discussion,
Development & Technical Discussion, Technical support, Economics,
Marketplace and Trading Discussion. Hope this is ok?

I also added a page "Trade" on the bitcoin.org site, where
btc-accepting services are listed. It's nice to see that there are
already useful services that accept btc.

The community has been growing nicely. We've had around 10-20 people
and active discussion at #bitcoin-dev lately.
```

It would be nice to get the daemon-able binaries to SF.net. We have
some skilled programmers in the community now, so maybe we can finish
the JSON API functions if you don't have time to.

Best regards.

Email #192

Date: Sun, 16 May 2010 20:12:21 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Status update

To: mmalmi@cc.hut.fi

I've also been busy with other things for the last month and a half. I
just now downloaded my e-mail since the beginning of April. I mostly
have things sorted and should be back to Bitcoin shortly. Glad that
you've been handling things in my absence. Congrats on your first
transaction!

As I recall, the code was nearly ready for a 0.3 release. I think all
it needed was a little testing time and to install the new icon xpm.

The JSON API functions are complete. I wanted to take another fresh
look at them in case I think of any better function names before
committing. I ought to write some sample code showing the proper way to
use them, particularly with polling for received transactions. When I
left off, I was thinking about bolting a payment mechanism onto a free
upload server software as an example. It would make sense to actually
build one practical application with the API before releasing it. You
don't realise the problems with an API until you actually try to use it.

mmalmi@cc.hut.fi wrote:
> Hi!
>
> How are you doing? Haven't seen you around in a while.
>
> I've been at full-time work lately, and will be until the end of June,
> so I haven't had that much time to work with Bitcoin or my exchange
> service. I have a working beta of my service though, and a few weeks ago
> made my first transaction: sold 10,000 btc for 20 euros via EU bank
> transfer. Maybe I can make it public soon.
>
> I divided the forum into 6 boards, which are Bitcoin Discussion,
> Development & Technical Discussion, Technical support, Economics,
> Marketplace and Trading Discussion. Hope this is ok?
>
> I also added a page "Trade" on the bitcoin.org site, where btc-accepting
> services are listed. It's nice to see that there are already useful
> services that accept btc.
>
> The community has been growing nicely. We've had around 10-20 people and
> active discussion at #bitcoin-dev lately.
>
> It would be nice to get the daemon-able binaries to SF.net. We have some
> skilled programmers in the community now, so maybe we can finish the
> JSON API functions if you don't have time to.
>
> Best regards.
>

Email #193

Date: Tue, 22 Jun 2010 18:36:22 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: 0.3.0 rc1 quickie download link

To: Martti Malmi <mmalmi@cc.hut.fi>

```
If bandwidth is a problem, delete my link in the "0.3 almost ready"
thread.  I just don't want to upload it to sourceforge for a quickie
share for a day or two, possibly taking it down immediately if there's a
bug.  Sourceforge has a policy of not allowing removal of files once
they're added, and it's a pain to upload to.  I'll delete the file once
the release is ready.

BTW, it's looking like I may be able to get us some money soon to cover
web host costs, back your exchange service, etc, in the form of cash in
the mail.  Can you receive it and act as the project's treasurer?
```

Email #194

Date: Tue, 22 Jun 2010 21:51:21 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: 0.3.0 rc1 quickie download link

```
> If bandwidth is a problem, delete my link in the "0.3 almost ready"
> thread.  I just don't want to upload it to sourceforge for a quickie
> share for a day or two, possibly taking it down immediately if there's
> a bug.  Sourceforge has a policy of not allowing removal of files once
> they're added, and it's a pain to upload to.  I'll delete the file once
> the release is ready.

Ok, I'll monitor it. Bandwidth hasn't been a problem so far - it's
been about 2 GB (0.5 dollars) per month at most. Other costs are about
15$ a month.

> BTW, it's looking like I may be able to get us some money soon to cover
> web host costs, back your exchange service, etc, in the form of cash in
> the mail.  Can you receive it and act as the project's treasurer?

That would be nice, I can do it. Sending cash in the mail may have its
risks, but maybe it's still the best anonymous option. We can also ask
for donations in BTC on the forum.
```

Email #195

Date: Wed, 23 Jun 2010 21:33:57 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: donation

To: mmalmi@cc.hut.fi

```
>> BTW, it's looking like I may be able to get us some money soon to cover
>> web host costs, back your exchange service, etc, in the form of cash in
>> the mail.  Can you receive it and act as the project's treasurer?
>
> That would be nice, I can do it. Sending cash in the mail may have its
> risks, but maybe it's still the best anonymous option. We can also ask
> for donations in BTC on the forum.

I got a donation offer for $2000 USD.  I need to get your postal mailing
```

address to have him send to. And yes, he wants to remain anonymous, so
please keep the envelope's origin private.

Email #196

Date: Fri, 25 Jun 2010 08:55:14 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: donation

You can give this address:

Martti Malmi
Visakoivunkuja 15 F 42
02130 Espoo
Finland

>>> BTW, it's looking like I may be able to get us some money soon to cover
>>> web host costs, back your exchange service, etc, in the form of cash in
>>> the mail. Can you receive it and act as the project's treasurer?
>>
>> That would be nice, I can do it. Sending cash in the mail may have
>> its risks, but maybe it's still the best anonymous option. We can
>> also ask for donations in BTC on the forum.
>
> I got a donation offer for $2000 USD. I need to get your postal
> mailing address to have him send to. And yes, he wants to remain
> anonymous, so please keep the envelope's origin private.

Email #197

Date: Tue, 06 Jul 2010 03:59:57 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Anonymous, homepage changes

To: Martti Malmi <mmalmi@cc.hut.fi>

I think we should de-emphasize the anonymous angle. With the popularity
of bitcoin addresses instead of sending by IP, we can't give the
impression it's automatically anonymous. It's possible to be
pseudonymous, but you have to be careful. If someone digs through the
transaction history and starts exposing information people thought was
anonymous, the backlash will be much worse if we haven't prepared
expectations by warning in advance that you have to take precautions if
you really want to make that work. Like Tor says, "Tor does not
magically encrypt all of your Internet activities. Understand what Tor
does and does not do for you."

Also, anonymous sounds a bit shady. I think the people who want
anonymous will still figure it out without us trumpeting it.

I made some changes to the bitcoin.org homepage. It's not really
crucial to update the translations. I tend to keep editing and
correcting for some time afterwards, so if they want to update, they
should wait.

I removed the word "anonymous", and the sentence about "anonymity
means", although you worded it so carefully "...CAN be kept hidden..."
it was a shame to remove it.

Instead, I added Tor instructions at the bottom, with instructions for how to stay anonymous (pseudonymous) directly after the Tor instructions: "If you want to remain anonymous (pseudonymous, really), be careful not to reveal any information linking your bitcoin addresses to your identity, and use a new bitcoin address for each payment you receive."

It helps that it can now seed automatically through Tor.

Even though it doesn't say anonymous until the bottom, I think anonymous seekers would already suspect it based on all the other attributes like no central authority to take your ID info and the way bitcoin addresses look.

Email #198

Date: Tue, 06 Jul 2010 19:03:50 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: 0.3.0 released

To: Martti Malmi <mmalmi@cc.hut.fi>

I uploaded 0.3.0 beta to sourceforge and updated the links on bitcoin.org. I still need to post the announcement message on the forum and mailing list. Here's what I've prepared:

Announcing version 0.3 of Bitcoin, the P2P cryptocurrency! Bitcoin is a digital currency using cryptography and a distributed network to replace the need for a trusted central server. Escape the arbitrary inflation risk of centrally managed currencies! Bitcoin's total circulation is limited to 21 million coins. The coins are gradually being released to the networks nodes based on the CPU power they contribute. You can get a share of them just by installing the software and contributing your idle CPU time.

What's new:
- Command line and JSON-RPC control
- Includes a daemon version without GUI
- Tabs for sent and received transactions
- 20% faster hashing
- Hashmeter performance display
- Mac OS X version (thanks to Laszlo)
- German, Dutch and Italian translations (thanks to DataWraith, Xunie and Joozero)

Email #199

Date: Tue, 06 Jul 2010 19:40:11 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: 0.3.0 released

To: Martti Malmi <mmalmi@cc.hut.fi>

Actually, "tabs for sent and received transactions" sounds really immature if it doesn't have that already. "Transaction filter tabs" sounds better.

I'm still editing it a little more and then I'll e-mail it to bitcoin-list and send it to the cryptography list.

"Get it at http://www.bitcoin.org or read the forum to find out more."

Satoshi Nakamoto wrote:
> I uploaded 0.3.0 beta to sourceforge and updated the links on
> bitcoin.org. I still need to post the announcement message on the forum
> and mailing list. Here's what I've prepared:
>
> Announcing version 0.3 of Bitcoin, the P2P cryptocurrency! Bitcoin is a
> digital currency using cryptography and a distributed network to replace
> the need for a trusted central server. Escape the arbitrary inflation
> risk of centrally managed currencies! Bitcoin's total circulation is
> limited to 21 million coins. The coins are gradually being released to
> the networks nodes based on the CPU power they contribute. You can get
> a share of them just by installing the software and contributing your
> idle CPU time.
>
> What's new:
> - Command line and JSON-RPC control
> - Includes a daemon version without GUI
> - Tabs for sent and received transactions
> - 20% faster hashing
> - Hashmeter performance display
> - Mac OS X version (thanks to Laszlo)
> - German, Dutch and Italian translations (thanks to DataWraith, Xunie
> and Joozero)
>

Email #200

Date: Tue, 06 Jul 2010 22:53:07 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [bitcoin-list] Bitcoin 0.3 released!

To: bitcoin-list@lists.sourceforge.net

Announcing version 0.3 of Bitcoin, the P2P cryptocurrency! Bitcoin is a
digital currency using cryptography and a distributed network to replace
the need for a trusted central server. Escape the arbitrary inflation
risk of centrally managed currencies! Bitcoin's total circulation is
limited to 21 million coins. The coins are gradually released to the
network's nodes based on the CPU power they contribute, so you can get a
share of them by contributing your idle CPU time.

What's new:
- Command line and JSON-RPC control
- Includes a daemon version without GUI
- Transaction filter tabs
- 20% faster hashing
- Hashmeter performance display
- Mac OS X version (thanks to Laszlo)
- German, Dutch and Italian translations (thanks to DataWraith, Xunie
and Joozero)

Get it at www.bitcoin.org, and read the forum to find out more.

Email #201

Date: Wed, 07 Jul 2010 01:17:54 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Anonymous, homepage changes

```
Ok, that sounds reasonable.

> I think we should de-emphasize the anonymous angle.  With the
> popularity of bitcoin addresses instead of sending by IP, we can't give
> the impression it's automatically anonymous.  It's possible to be
> pseudonymous, but you have to be careful.  If someone digs through the
> transaction history and starts exposing information people thought was
> anonymous, the backlash will be much worse if we haven't prepared
> expectations by warning in advance that you have to take precautions if
> you really want to make that work.  Like Tor says, "Tor does not
> magically encrypt all of your Internet activities.  Understand what Tor
> does and does not do for you."
>
> Also, anonymous sounds a bit shady.  I think the people who want
> anonymous will still figure it out without us trumpeting it.
>
> I made some changes to the bitcoin.org homepage.  It's not really
> crucial to update the translations.  I tend to keep editing and
> correcting for some time afterwards, so if they want to update, they
> should wait.
>
> I removed the word "anonymous", and the sentence about "anonymity
> means", although you worded it so carefully "...CAN be kept hidden..."
> it was a shame to remove it.
>
> Instead, I added Tor instructions at the bottom, with instructions for
> how to stay anonymous (pseudonymous) directly after the Tor
> instructions: "If you want to remain anonymous (pseudonymous, really),
> be careful not to reveal any information linking your bitcoin addresses
> to your identity, and use a new bitcoin address for each payment you
> receive."
>
> It helps that it can now seed automatically through Tor.
>
> Even though it doesn't say anonymous until the bottom, I think
> anonymous seekers would already suspect it based on all the other
> attributes like no central authority to take your ID info and the way
> bitcoin addresses look.
```

Email #202

Date: Wed, 14 Jul 2010 22:52:46 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Fwd: Re: bitcoin!!!!

To: Martti Malmi <mmalmi@cc.hut.fi>

```
I see the interior pages of the old sourceforge wiki are still up,
though the homepage forwards.


-------- Original Message --------
Subject: Re: bitcoin!!!!
```

Date: Wed, 14 Jul 2010 10:56:21 -0400
From: Sam <samm@sammaloney.com>
To: Satoshi Nakamoto <satoshin@gmx.com>
References: <201004111508.52168.samm@sammaloney.com>
<201007111859.29171.samm@sammaloney.com> <4C3DCD97.8030003@gmx.com>

It was an old FAQ on sourceforge that had been linked from slashdot (on a highly visible comment). people were going there because bitcoin.org was down
for a while.

http://bitcoin.sourceforge.net/wiki/index.php?page=FAQ

Probably not an issue anymore, but might be a good idea to delete or update that wiki page.

> I don't see any 0.1.5 download links on the FAQ. Do you mean
> bitcoin.org/faq? Is it on one of the other languages? Or maybe someone
> else fixed it already.
>
> > Anyways, I write to you now to let you know you must update the FAQ
> > immediately. It points to 0.15 of bitcoin for download. You must update
> > it to 0.30, as it is slashdotted!
>

Email #203

Date: Thu, 15 Jul 2010 18:41:10 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: bitcoin.org drupal users

To: Martti Malmi <mmalmi@cc.hut.fi>

Is it possible for the translators (at least the more trusted ones) to have user accounts on drupal so they can update their translated text directly? The user accounts on drupal appear to be pretty weak. I created a satoshi account and it can't even edit the side bar stuff, just the main text of pages. I don't think user accounts can access any of the admin stuff. Do you think it's safe, or do you feel insecure about doing that? If you're worried, maybe there's a way to lock just the english version of the homepage.

It would be nice if when I need to make changes to the homepage, I could enlist someone like Xunie to do the rote work of reflecting it to all the translations instead of having to do all that work myself. (many light changes don't require understanding the language to fix the translated pages)

Email #204

Date: Thu, 15 Jul 2010 18:43:55 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Fwd: Please update the bitcoin FAQ so new member can have the right info

To: Martti Malmi <mmalmi@cc.hut.fi>

-------- Original Message --------
Subject: Please update the bitcoin FAQ so new member can have the right info
Date: Mon, 12 Jul 2010 14:13:20 -0700
From: Jim Nguyen <jimmy.winn@gmail.com>
To: satoshin@gmx.com

Hi,

In the FAQ of bitcoin.org <http://bitcoin.org> the backing up of the wallet had old instructions, right? Should it just be to back up wallat.dat instead of the entire folder??? See below.

"How do I backup my wallet?

Your data is stored in the directory ''%appdata%\Bitcoin'', which is typically:

  Windows XP:
    C:\Documents and Settings\username\Application Data\Bitcoin
  Windows Vista:
    C:\Users\username\AppData\Roaming\Bitcoin

It’s recommended that you stop Bitcoin before backing it up to make sure the backup will be correct."

Email #205

Date: Thu, 15 Jul 2010 21:00:12 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: bitcoin.org server

To: Martti Malmi <mmalmi@cc.hut.fi>

You did some research when choosing hosting, this was a well chosen one, right? It seems like it would be a tremendous hassle to change, and we've had good luck with this one. Cheaper will usually have some offsetting drawback in quality.

I wonder if that extra memory is just disk cache or something.

I take it you haven't received anything from that donor yet? He seemed pretty certain he was going to send it, maybe more. (if you get anything, we need to keep private for him the fact that we got a donation)

Email #206

Date: Sat, 17 Jul 2010 04:27:38 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: bitcoin.org drupal users

Yes, we could give accounts to trusted translators. I haven't found a way to give them edit permissions to only one page, but they can be forced to create a new revision with every page change they make, and not be allowed to delete revisions. Xunie would be the first on the list I'd give an account. :)

> Is it possible for the translators (at least the more trusted ones) to
> have user accounts on drupal so they can update their translated text
> directly? The user accounts on drupal appear to be pretty weak. I
> created a satoshi account and it can't even edit the side bar stuff,
> just the main text of pages. I don't think user accounts can access
> any of the admin stuff. Do you think it's safe, or do you feel
> insecure about doing that? If you're worried, maybe there's a way to
> lock just the english version of the homepage.

```
>
> It would be nice if when I need to make changes to the homepage, I
> could enlist someone like Xunie to do the rote work of reflecting it to
> all the translations instead of having to do all that work myself.
> (many light changes don't require understanding the language to fix the
> translated pages)
```

Email #207

Date: Sat, 17 Jul 2010 04:33:46 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fwd: Re: bitcoin!!!!

```
Relocated the old site to /oldsite, now there's only the redirection.

> I see the interior pages of the old sourceforge wiki are still up,
> though the homepage forwards.
>
>
> -------- Original Message --------
> Subject: Re: bitcoin!!!!
> Date: Wed, 14 Jul 2010 10:56:21 -0400
> From: Sam <samm@sammaloney.com>
> To: Satoshi Nakamoto <satoshin@gmx.com>
> References: <201004111508.52168.samm@sammaloney.com>
> <201007111859.29171.samm@sammaloney.com> <4C3DCD97.8030003@gmx.com>
>
> It was an old FAQ on sourceforge that had been linked from slashdot (on a
> highly visible comment). people were going there because bitcoin.org was down
> for a while.
>
> http://bitcoin.sourceforge.net/wiki/index.php?page=FAQ
>
> Probably not an issue anymore, but might be a good idea to delete or update
> that wiki page.
>
>> I don't see any 0.1.5 download links on the FAQ.  Do you mean
>> bitcoin.org/faq?  Is it on one of the other languages?  Or maybe someone
>> else fixed it already.
>>
>>> Anyways, I write to you now to let you know you must update the FAQ
>>> immediately. It points to 0.15 of bitcoin for download. You must update
>>> it to 0.30, as it is slashdotted!
>>
```

Email #208

Date: Sun, 18 Jul 2010 02:21:45 +0300

From: mmalmi@cc.hut.fi

To: satoshin@gmx.com

Subject: Fwd: bitcoin hosting

```
Rackspace has very good support, good backend, good connections and
nicely scaling cloud based virtual servers. I got this offer from
Thufir:
```

```
-----
Hi Sirius,

Check out www.citrusdesignstudio.com. You will see through the portfolio that
I am a real business with many clients.

That is my business that I provide managed hosting through.
I also do unmanaged VPSes.

Normally I would charge $15/mo for 512MB.
I will do it for $10/mo for you.

To see my pricing, go to www.linnode.com. I match everything they have except
their great panel -- you have to email or call my people.

I provide VPS services normally for 3/4ths the posted cost on linnode.com.
(Rackspace is even more expensive.)

I will do it for 1/2 of linnode's price for you.

It scales linerally just like linnodes, so for 2048 MB of memory, I would
charge $40, etc.

Later!
-----

That would be worth considering, if they have good datacenters and
connections. $10 / month is about $20 less than what Rackspace costs.
On the other hand, Rackspace prices are no problem if the donation is
to arrive.
```

Email #209

Date: Sun, 18 Jul 2010 16:23:21 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: wiki

To: Martti Malmi <mmalmi@cc.hut.fi>

```
http://www.bitcoin.org/smf/index.php?topic=393.msg3785#msg3785

AndrewBuck:
...

EDIT:  The wiki doesn't seem to be sending the registration e-mail so I
can log in to edit, is there some problem with the server or something?

-Buck
```

Email #210

Date: Sun, 18 Jul 2010 16:23:10 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fwd: bitcoin hosting

To: mmalmi@cc.hut.fi

```
Please promise me you won't make a switch now.  The last thing we need
is switchover hassle on top of the slashdot flood of work we've got now.
  I'm losing my mind there are so many things that need to be done.
```

Also, it would suck to be on a smaller, less reliable host just to save
a measly $20.

I will try to think of a polite way to ask the donor if he sent it, but
right now there are other higher priority things that are going to bump
even that for a few days.

Would a donation of bitcoins help in the short term?

mmalmi@cc.hut.fi wrote:
> Rackspace has very good support, good backend, good connections and
> nicely scaling cloud based virtual servers. I got this offer from Thufir:
>
> -----
> Hi Sirius,
>
> Check out www.citrusdesignstudio.com. You will see through the portfolio
> that
> I am a real business with many clients.
>
> That is my business that I provide managed hosting through.
> I also do unmanaged VPSes.
>
> Normally I would charge $15/mo for 512MB.
> I will do it for $10/mo for you.
>
> To see my pricing, go to www.linnode.com. I match everything they have
> except
> their great panel -- you have to email or call my people.
>
> I provide VPS services normally for 3/4ths the posted cost on linnode.com.
> (Rackspace is even more expensive.)
>
> I will do it for 1/2 of linnode's price for you.
>
> It scales linerally just like linnodes, so for 2048 MB of memory, I would
> charge $40, etc.
>
> Later!
> -----
>
> That would be worth considering, if they have good datacenters and
> connections. $10 / month is about $20 less than what Rackspace costs. On
> the other hand, Rackspace prices are no problem if the donation is to
> arrive.
>

Email #211

Date: Mon, 19 Jul 2010 02:51:11 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Fwd: bitcoin hosting

Ok, I won't switch it. Donations in Bitcoin are helpful and can be
sent to 14EXchS9j3AAfim6mL4jtw6VWMosSUiG5U.

> Please promise me you won't make a switch now. The last thing we need
> is switchover hassle on top of the slashdot flood of work we've got
> now. I'm losing my mind there are so many things that need to be done.
>
> Also, it would suck to be on a smaller, less reliable host just to save

> a measly $20.
>
> I will try to think of a polite way to ask the donor if he sent it, but
> right now there are other higher priority things that are going to bump
> even that for a few days.
>
> Would a donation of bitcoins help in the short term?
>
> mmalmi@cc.hut.fi wrote:
>> Rackspace has very good support, good backend, good connections and
>> nicely scaling cloud based virtual servers. I got this offer from
>> Thufir:
>>
>> -----
>> Hi Sirius,
>>
>> Check out www.citrusdesignstudio.com. You will see through the
>> portfolio that
>> I am a real business with many clients.
>>
>> That is my business that I provide managed hosting through.
>> I also do unmanaged VPSes.
>>
>> Normally I would charge $15/mo for 512MB.
>> I will do it for $10/mo for you.
>>
>> To see my pricing, go to www.linnode.com. I match everything they
>> have except
>> their great panel -- you have to email or call my people.
>>
>> I provide VPS services normally for 3/4ths the posted cost on linnode.com.
>> (Rackspace is even more expensive.)
>>
>> I will do it for 1/2 of linnode's price for you.
>>
>> It scales linerally just like linnodes, so for 2048 MB of memory, I would
>> charge $40, etc.
>>
>> Later!
>> -----
>>
>> That would be worth considering, if they have good datacenters and
>> connections. $10 / month is about $20 less than what Rackspace
>> costs. On the other hand, Rackspace prices are no problem if the
>> donation is to arrive.
>>

Email #212

Date: Wed, 21 Jul 2010 23:33:18 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Donation

Good news: I received the donation of $3600. At least the hosting
costs are no problem anymore.

What do you think of the idea to offer rewards of $100-200 to the
first 5-10 established companies that start accepting Bitcoin? We'd
also assign them a dedicated support person to help with integration.

I have companies like prq.se, ipredator.se, relakks.com or
perfect-privacy.com in mind. We could also make the offer public.

Email #213

Date: Wed, 21 Jul 2010 23:28:33 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

To: mmalmi@cc.hut.fi

mmalmi@cc.hut.fi wrote:
> Good news: I received the donation of $3600. At least the hosting costs
> are no problem anymore.

That's great! I'll let him know it was received and thank him.

It might be a long time before we get another donation like that, we
should save a lot of it.

Spend what you need on hosting. Email me a simple accounting when you
take out money for expenses, like:
    -$60 rackspace monthly
   $2540 balance

> What do you think of the idea to offer rewards of $100-200 to the first
> 5-10 established companies that start accepting Bitcoin? We'd also
> assign them a dedicated support person to help with integration. I have
> companies like prq.se, ipredator.se, relakks.com or perfect-privacy.com
> in mind. We could also make the offer public.

$100-200 is chump change if they're a serious company, it would only
make us sound small.

What they need most is confidence they can convert it to fiat currency.
  That VOIP company essentially said so in a recent post. The best
thing we can do is make sure there's cash available to cash out and
support and steady the conversion rate.

The money is leveraged better that way too. Theoretically, imagine 10
businesses have their eye on a $100 bill being offered for bitcoins, but
don't actually cash out because they know it's there if they need it.
That one $100 bill allowed 10 different people to act like their 5000
bitcoins were equivalent to $100.

I think we should allocate $1000 at this point to your exchange.

Email #214

Date: Fri, 23 Jul 2010 07:41:11 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

> Spend what you need on hosting. Email me a simple accounting when you
> take out money for expenses, like:
>   -$60 rackspace monthly
> $2540 balance

Ok.

```
>> What do you think of the idea to offer rewards of $100-200 to the
>> first 5-10 established companies that start accepting Bitcoin? We'd
>>  also assign them a dedicated support person to help with
>> integration. I have companies like prq.se, ipredator.se,
>> relakks.com or perfect-privacy.com in mind. We could also make the
>> offer public.
>
> $100-200 is chump change if they're a serious company, it would only
> make us sound small.
>
> What they need most is confidence they can convert it to fiat currency.
>  That VOIP company essentially said so in a recent post.  The best
> thing we can do is make sure there's cash available to cash out and
> support and steady the conversion rate.
>
> The money is leveraged better that way too.  Theoretically, imagine 10
> businesses have their eye on a $100 bill being offered for bitcoins,
> but don't actually cash out because they know it's there if they need
> it. That one $100 bill allowed 10 different people to act like their
> 5000 bitcoins were equivalent to $100.
>
> I think we should allocate $1000 at this point to your exchange.

Alright, I'll add $1000 dollars to the exchange reserves. That way I
can offer more stable pricing.

A week ago somebody bought coins with 1000 €. That was probably meant
as a donation to some extent, since 1000 € would have bought him a lot
more coins at bitcoinmarket.com than at my service.
```

Email #215

Date: Fri, 23 Jul 2010 16:59:42 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

To: mmalmi@cc.hut.fi

```
>> I think we should allocate $1000 at this point to your exchange.
>
> Alright, I'll add $1000 dollars to the exchange reserves. That way I can
> offer more stable pricing.
>
> A week ago somebody bought coins with 1000 €. That was probably meant as
> a donation to some extent, since 1000 € would have bought him a lot more
> coins at bitcoinmarket.com than at my service.

Interesting, so how is the balance between purchases of coins and cash
going?

Btw, are you able to use my builds of bitcoind on your host, or do you
have to build it yourself?
```

Email #216

Date: Sat, 24 Jul 2010 07:32:37 +0300

From: mmalmi@cc.hut.fi

To: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

```
> Interesting, so how is the balance between purchases of coins and cash going?
```

```
About +1000€ (plus the $1000) and -40000 BTC since when I started. I
should have set the initial BTC price higher, it was only 1€ / 1000
BTC in the beginning.

> Btw, are you able to use my builds of bitcoind on your host, or do you
> have to build it yourself?

I had to build it myself. It had the same problem that has been
reported on the forums: /usr/lib/libstdc++.so.6: version
`GLIBCXX_3.4.11' not found.
```

Email #217

Date: Sat, 24 Jul 2010 15:38:53 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: Donation

To: mmalmi@cc.hut.fi

```
> A week ago somebody bought coins with 1000 €. That was probably meant as
> a donation to some extent, since 1000 € would have bought him a lot more
> coins at bitcoinmarket.com than at my service.

They probably couldn't have gotten that large of a trade on
bitcoinmarket.com.
```

Email #218

Date: Mon, 26 Jul 2010 19:22:08 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Re: /usr/lib/libstdc++.so.6: version `GLIBCXX_3.4.11'

To: mmalmi@cc.hut.fi

```
>> Btw, are you able to use my builds of bitcoind on your host, or do you
>> have to build it yourself?
>
> I had to build it myself. It had the same problem that has been reported
> on the forums: /usr/lib/libstdc++.so.6: version `GLIBCXX_3.4.11' not found.

Wish I could figure out how to fix that.  What version of GLIBCXX does
your system have?

Make sure you upgrade to Bitcoin 0.3.3 as soon as possible.
```

Email #219

Date: Thu, 29 Jul 2010 03:18:56 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: Forum e-mail notifications and PBL blacklist and wiki registration

To: Martti Malmi <mmalmi@cc.hut.fi>

```
http://www.bitcoin.org/smf/index.php?topic=338.0

> of e-mail blackhole list or at least the ISP that hosts the e-mail server for
registration is on one of those lists.
>
> "Looks like bitcoin.org is listed on the PBL."
> http://www.spamhaus.org/pbl/query/PBL340779
```

I think our problem may be that we have forum notifications on, like
e-mail you when you receive a PM, but we don't have e-mail verification
of new accounts. Can someone put someone else's e-mail address without
verifying it, then have stuff sent there? We need to stop that right
away before it gets used for something bad. Either disallow all
notification, or make sure e-mail addresses are verified.

I'm more inclined to disallow notifications or anything where the forum
sends you e-mail. I kinda like not requiring e-mail verification. But
if that's the only way to make sure we don't send e-mails to un-verified
addresses, then we could do that.

If we request to get off of PBL, we'd better make sure we've got the
problem secured first.

I changed Registration->settings->registration of new members to "Member
Activation". I assume that means it e-mail verifies.
"Member Activation
When this option is enabled any members registering to the forum will
have a activation link emailed to them which they must click before they
can become full members"

I think that's the only way to make sure the forum can't be used to send
to other people's e-mail addresses and potentially use it to spam.

Email #220

Date: Fri, 30 Jul 2010 06:34:38 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [bitcoin-list] Alert: upgrade to bitcoin 0.3.6

To: bitcoin-list@lists.sourceforge.net

Please upgrade to 0.3.6 ASAP to get an important bugfix.

See the bitcoin.org homepage for download links.

Email #221

Date: Mon, 02 Aug 2010 21:56:06 +0100

From: Satoshi Nakamoto <satoshin@gmx.com>

Subject: [Fwd: no activation mail]

To: Martti Malmi <mmalmi@cc.hut.fi>

Oh great, now we're screwed.

We probably got spam blocked because we were allowing registrations
without e-mail verification. But now that we've enabled it, our
verification e-mails are blocked.

There could still be some existing user accounts created before the
registration requirement being used by spammers.