The New Satoshi Emails: Early Developer Sirius Releases 120 Pages Detailing Work on Bitcoin

Pete Rizzo ⋮ 6-8 minutes ⋮ 2/23/2024

Satoshi Nakamoto's earliest collaborator Martii 'Sirius' Malmi has released his entire email correspondence with Bitcoin's creator.

Spurred by an ongoing lawsuit in the U.K., the new emails are the most significant addition to the canon of what we know about Bitcoin's still anonymous creator.

Here are the most important new findings.

EMAIL #1: SATOSHI'S BITCOIN SCALING ASSUMPTIONS

SUBJECT: Re: Bitcoin
FROM: Satoshi Nakamoto <satoshin@gmx.com>
TO: Martti Malmi <sirius-m@users.sourceforge.net>
DATE: 02/05/2009 18:06

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.

When asked how Bitcoin might scale in the future, Satoshi theorized the network might have a maximum of 100,000 nodes.

Here he goes into the calculations assessing the economics of bandwidth costs to nodes (read: miners) in propagating transactions across the network, the economic costs that would incur, and how that could be cost effectively passed on to users.

He also discusses the implementation of users paying fees, and hints at the potential for the fee necessary for confirmation of your transaction being market driven due to the processing capacity of the network.

All in all, it's interesting napkin math, though nothing out of the ordinary for those who have read Satoshi's full Bitcoin forum posts.

There Satoshi talked frequently about his vision for how the network might grow larger, and it's notable much of his ideas were not proven to be viable based on subsequent development work.

> 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

EMAIL #2: Bitcoin Doesn't Waste Energy

Though he wouldn't stick around to see the tremendous uptick in Bitcoin mining using stranded resources, it turns out, Satoshi knew the network was greent.

One of the first criticisms to be lobbied at his new creation, Satoshi spent time addressing the idea that Bitcoin mining was wasteful on the forums, most notably saying that not having a currency like Bitcoin would be the bigger waste.

Here, however, he expands on the idea in more detail, and in a more vivid and descriptive way than we've seen before.

> 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

EMAIL #3: Satoshi on Time-stamping

A headed debated today remains whether Bitcoin is money, or whether it can or does have other ancillary uses.

In this email exchange, Satoshi seems to offer some insight on the debate, noting his belief the blockchain can be used as a distributed time-stamping server. This is akin to what has happened in Guatemala, where the blockchain has been used to certify contentious elections in recent years.

> 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.

EMAIL #4: Satoshi Talks DigiCash

Satoshi describing the differences between #Bitcoin and DigiCash, David Chaum's failed e-money.

This is notable as Chaum's work had a profound impact on the cypherpunks, including Hal Finney. He specifically discusses the differences in privacy properties of the two models, and notes that unlike Chaum's scheme did not support an offline model, requiring all participants to be online to make use of the system.

He also explains the finite supply cap of bitcoin.

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

EMAIL #5: Satoshi Was Concerned About Promoting Bitcoin

Satoshi was concerned about his legal risk in launching #Bitcoin, noting he was "uncomfortable" with explicitly labeling it an investment.

Note: *Here also we see he didn't come up with the term "cryptocurrency" himself.*

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?

EMAIL #6: Satoshi Got Burned Out on Bitcoin

By July 2009, Satoshi was tired, saying he "needed a break" from Bitcoin. Here, he also explains Hal's absence from the work. He also mentions spending a period of 18 months at that point developing Bitcoin.

A curious note as well, he asks Malmi if he had any ideas for applications people can actually use Bitcoin for.

> 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.

EMAIL #7: Bitcoin, A Way to Get Free Money

Satoshi discussing how #Bitcoin might gain adoption. Of note is his emphasis that Bitcoin was easy to obtain given that you could mine it on a computer. He also goes to postulate how the nature of a market trading for Bitcoin would evolve, discussing how skeptical people might be of its value, stating he was confident the increasing mining difficulty would prove its scarcity to people.

Very different from how we think about BTC today in terms of acquiring it, but demonstrating a prescience of how people would mentally value it in the future.

> 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.

EMAIL #8: A Mysterious Bitcoin Donor Emerges

In June 2010, someone offered to donate $2,000 to Satoshi for his #Bitcoin work. Notably, he had the donor send it to Martti's address. He also communicated care that the donor's privacy was respected.

```
>> 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 #9: Satoshi Was a Fan of Free Transactions

Already known, but Satoshi was pretty adamant that early users consider #Bitcoin "free." Here he is discussing removing transaction fees from the UX of an early software.

It's interesting that his reasoning was to obscure this feature from users, but simultaneously acknowledged its necessity in the far future.

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.

EMAIL #10: Satoshi Was Dedicated to His Bitcoin Work

Satoshi worked on #Bitcoin on Christmas day. There are some interesting implications here to consider regarding his personal life.

SUBJECT: Re: Bitcoin stuff
FROM: Satoshi Nakamoto <satoshin@gmx.com>
TO: mmalmi@cc.hut.fi
DATE: 25/12/2009 16:11

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 #11: Bitcoin, A Web Currency for Currency Trading?

Satoshi saw #Bitcoin taking hold as a way to trade other internet currencies like Liberty Reserve. He also goes on to discuss the potential for markets selling gift

cards for bitcoin, which wound up becoming and is to this day a significant market for bitcoin.

Note: *Liberty Reserve was later shut down by the US.*

> 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 #12: Satoshi's First Disappearance

Satoshi had a mysterious leave of absence from #Bitcoin in 2010. Here he is talking about it with Martti, though it's notably also short on details.

> 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.

EMAIL #13: Satoshi Realized Bitcoin Wasn't Anonymous

It was Satoshi who removed the language that Bitcoin was "anonymous" from http://Bitcoin.org. He worried it made Bitcoin sound "shady." This echoes his later sentiments around Wikileaks announcing their acceptance of bitcoin for donations.

> 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.

EMAIL #14: Satoshi Gives Praise to His Protege

Worth noting given the historical revisionism around this, Satoshi thought very highly of Gavin Andresen. Here he is praising Gavin and referring to someone else as a "goofball."

> > I told him to go ahead. I don't do automatic backups atm. We should have
> > more server admins soon when I get bitcoinexchange.com to another
> > server. I could give the root password to you and somebody else. Xunie
> > has volunteered, but we might find somebody even more professional from
> > the forum and keep the number of admins at the minimum. If the outage
> > was due to heavy load, he could help us move to lighttpd or optimize
> > resources otherwise. Should we make a recruitment thread on the forum?
>
> It should be Gavin. I trust him, he's responsible, professional, and
> technically much more linux capable than me.
>
> (I don't know Xunie, but he hasn't posted for months and he was a goofball)

EMAIL #15: Satoshi Says Sayonara

We finally have a copy of the email Satoshi sent other developers before taking his name off the project website. As they've said, Satoshi doesn't mention his intention to step back from the project at all.

SUBJECT: Project Developers
FROM: Satoshi Nakamoto <satoshin@gmx.com>
TO: Martti Malmi <mmalmi@cc.hut.fi>
DATE: 07/12/2010 15:38

Mind if I add you to the Project Developers list on the Contact page? You wrote some code before so you should be there. It would have to be your real name for consistency. If you want to have an e-mail address listed, I'll make an image out of it so it doesn't attract spam.

Overall no substantial new information is brought to light, but the emails do give a new angle to Satoshi's interactions with others involved in the project before his departure.