How to evaluate a claim that a certain person is Satoshi Nakamoto
A public service document from Coin Center

by Jerry Brito & Peter Van Valkenburgh

Last updated: Friday, 8 April 2016 - 21:03:36 GMT

If someone steps forward to claim that they are Satoshi Nakamoto, or is outed as such, there likely will be evidence put forward to substantiate the claim. We thought it would be useful to write down some facts that could be used by journalists and other curious individuals in assessing the credibility of any such evidence.

We don't believe it matters who Satoshi is, but his identity is arguably of public interest and any purported revelation will be covered in the press. Given that the media has twice identified the wrong person based on mistaken readings of circumstantial evidence, we wanted to put down some notes on how to critically assess evidence that a certain person is Satoshi.

[We would appreciate it those with a good technical understanding or historical knowledge could help us answer some questions below, correct our mistakes, or provide other insight. We will update this document to reflect anything new we learn.]

I. Facts about Satoshi's Purported PGP Key

Here are some things we know:

1. There is a PGP public key that is purported to have belonged to Satoshi Nakamoto (the "Satoshi key").

2. Signing with a PGP key does not prove someone's identity; it only proves that the person signing has access to the private key. Typically, before relying on a PGP signature as a proxy for identity, one would want to verify in-person that the signer has access to that private key and then trust that the signer has not given, or lost, control of the key to a third party. If an in-person verification is not possible, a less-reliable alternative way to link identity to a public key is to publish the key from social network accounts or web domains that one controls, thus implying that control of the accounts and control of the key is under the same person.

3. As far as we can tell, there is no evidence of Satoshi ever signing a message with the Satoshi key *or any* PGP key. [If you have any evidence, please let us know] See, for example:

http://bitcoin-development.narkive.com/bQ54N7i4/bitcoin-development-does-anyone-have-anything-at-all-signed-by-satoshi-s-pgp-key

https://twitter.com/jgarzik/status/718217457190567936

4. The Satoshi key was published at the bitcoin.org domain.

The bitcoin.org domain was registered on August 18, 2008, two months before the Bitcoin white paper was first released, and it is generally accepted that it was Satoshi who registered it. (For one thing, the first message from Satoshi to the Cryptography mailing list announcing the Bitcoin white paper on October 31, 2008 contained a link to a PDF of the white paper hosted at bitcoin.org.)

The earliest record of bitcoin.org at the Internet Archive is from January 31, 2009. There is a link at the bottom of that archived page to Satoshi's PGP key block. Clicking on that link takes one to a PGP ASCII armored file with the signature block. The URL for that file was http://bitcoin.org/Satoshi_Nakamoto.asc. The earliest archived copy of that URL on the Internet Archive is February 28, 2011. (On later versions of the bitcoin.org home page, the same link to Satoshi's PGP key block resolve to a different URL: https://bitcoin.org/satoshinakamoto.asc. The earliest archived copy of that different URL on the Internet Archive is April 20, 2013. Both of these files, however, contain identical key blocks.) There is no apparent way to verify whether the Satoshi key was present on the Bitcoin.org domain prior to February 28, 2011. [If you have a way, please let us know. *Should have used a blockchain! :o)*]

5. The Satoshi key was added to the MIT PGP Public Key Server with a listed creation time of October 30, 2008.[1] Keys submitted to the MIT PGP Public Key Server are not verified in any way, and creation dates can be easily backdated. There is no apparent way of identifying when the key was added to the MIT key server.

6. In the Bitcoin Foundation bylaws on GitHub, as of May 2013, there is a reference to a PGP public key fingerprint asserted to belong to Satoshi Nakamoto:

> "vii. Satoshi Nakamoto, at satoshin@gmx.com, author of the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" published on http://bitcoin.org and owner of the PGP Public Key with fingerprint: DE4E FCA3 E1AB 9E41 CE96 CECB 18C0 9E86 5EC9 48A1."

[1] The key block of the MIT key is substantially larger than the key block of the bitcoin.org key, but the first ~9 lines are identical to the key on bitcoin.org. This is apparently the case because the Satoshi key has been signed by many other random persons on the server.

This is the fingerprint for the Satoshi key, and this fingerprint was vouched for by Gavin Andresen in a GitHub thread, but it is not clear if he simply meant that it matched the key published at Bitcoin.org, or if he had verified it in some other way. [Gavin: Please let us know.]

7. The email address associated with the Satoshi key (on the MIT server, on the earliest archived copy of the Bitcoin.org site, and on the Bitcoin Foundation bylaws) is satoshin@gmx.com. That is also the email listed on the PDF of the Bitcoin white paper. The message first announcing the Bitcoin white paper to the Cryptography mailing list was sent from satoshi@vistomail.com.

Conclusions:

Given that the earliest publicly verifiable date of the existence of the Satoshi key is February 28, 2011 (while Satoshi's last public posting took place on December 12, 2010), and given that there is no evidence that Satoshi ever used the Satoshi key, and no evidence that anyone ever verified Satoshi's personal access to the key, we can conclude that Satoshi Nakamoto's association with the Satoshi key is circumstantial and not definitive. If someone were to successfully sign with the Satoshi PGP key, it would not prove that he is Satoshi. It would only be interesting circumstantial evidence that should lead one to question how they obtained that private key. One possible answer is that they are Satoshi, but there are many other plausible answers as well.

II. So what kind of evidence is convincing of Satoshi's identity?

Cryptographic Evidence

1. Bitcoin addresses are hashed public keys that have corresponding private keys, much like in PGP. To spend bitcoins associated with an address, a user must sign a transaction with the corresponding private key.

2. The first block in the Bitcoin blockchain is known as the Genesis Block and it is generally accepted that Satoshi mined this block. The block reward address for the Genesis Block is 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa (let's call this the "genesis address"). The Genesis Block is a special case in that its mining reward cannot be spent because it does not reference a previous block. Although it is not possible to spend bitcoins associated with the genesis address, it would be possible for Satoshi to reveal the public key that hashes to the genesis address. Therefore, revealing the public key of the genesis address, and then signing a transaction with the corresponding private key would be good evidence that one is Satoshi.

3. It is generally believed that Hal Finney was the second person to join the Bitcoin network, and the first person to receive a Bitcoin transaction. In his words:

> When Satoshi announced the first release of the software, I grabbed it right away. I think I was the first person besides Satoshi to run bitcoin. I mined block 70-something, and I was the recipient of the first bitcoin transaction, when Satoshi sent ten coins to me as a test. I carried on an email conversation with Satoshi over the next few days, mostly me reporting bugs and him fixing them. [Is there any other way to verify corroborate this? Or do we simply trust Finney, now deceased?]

That transaction sending 10 bitcoins from Satoshi to Hal Finney is generally believed to be this one sent on January 12, 2009:

https://blockchain.info/tx/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16

It spent virgin bitcoins from an address (12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S) that received a reward of 50 bitcoins for mining block 9 on January 9, 2009. As a result, this transaction is generally believed [1,2] to be the only message Satoshi has ever been known to sign cryptographically. Therefore, signing transactions with the private key corresponding to this bitcoin address would be good evidence that one is Satoshi.

4. As noted above, Hal Finney is believed to be the second person to mine on the Bitcoin network, and he said that he “mined block 70-something.” This means that the blocks mined before then were presumably mined by Satoshi, although it is impossible to be certain. It is likely, though, that Satoshi mined many of the first few blocks, with the probability of it being Satoshi increasing the closer you get to the Genesis Block. Therefore, signing transactions with the private keys corresponding to a large number of the earliest block reward addresses would be good evidence that one is Satoshi.

Beyond Cryptographic Evidence: A Smell Test

If someone were to provide cryptographic evidence as outlined above, it would not prove that they are Satoshi. It would only supply evidence for their claim. One would have to put that evidence in context with other known facts and open questions.

For example, if someone was able to sign with the Satoshi PGP key, but not with any of the Bitcoin keys, or if someone could sign with one or two early Bitcoin keys, but not with the genesis key, one should expect the person to provide a logical and reasonable explanation for the discrepancy. Cryptographic evidence in the absence of a coherent story should be unconvincing.

Additionally, any cryptographic evidence supplied that a certain person is Satoshi should be balanced against other evidence that the person in question is not Satoshi. For example, if the person claiming to be Satoshi has a credibility problem (perhaps because they are known to

have previously lied about university degrees and business partnerships and have been known to falsify information, etc.), that should weigh against treating any cryptographic evidence as dispositive.

Finally, in making a judgment about whether someone is Satoshi, one should look at the totality of the circumstances and ask oneself if the impression one has of the person claiming to be, or outed as, Satoshi fits the known characteristics of Satoshi. These are characteristics that have been revealed not just through his historical writings, but through his behavior as well. Chief among these is his penchant for privacy.

Social Evidence

Cryptography cannot prove who you are, only that you have access to a particular computer code. And a plausible story for your behavior is also not proof, just an exercise in persuasion. The final piece of evidence that should be considered in trying to asses the identity of a person that no one has ever seen or heard is social. There is a small group of persons who had extensive and regular communication with Satoshi from 2009 to 2010-11. These include Martti Malmi, Gavin Andresen, Jeff Garzik, Mike Hearn, and others. [Please let me know who else may fit this bill.] Their opinion, having personally communicated and collaborated with Satoshi, would deserve some weight. It is important to note that the opinion of “prominent” persons in the Bitcoin community who did not communicate and collaborate with Satoshi are no more weighty than anyone else’s.