Bitslog

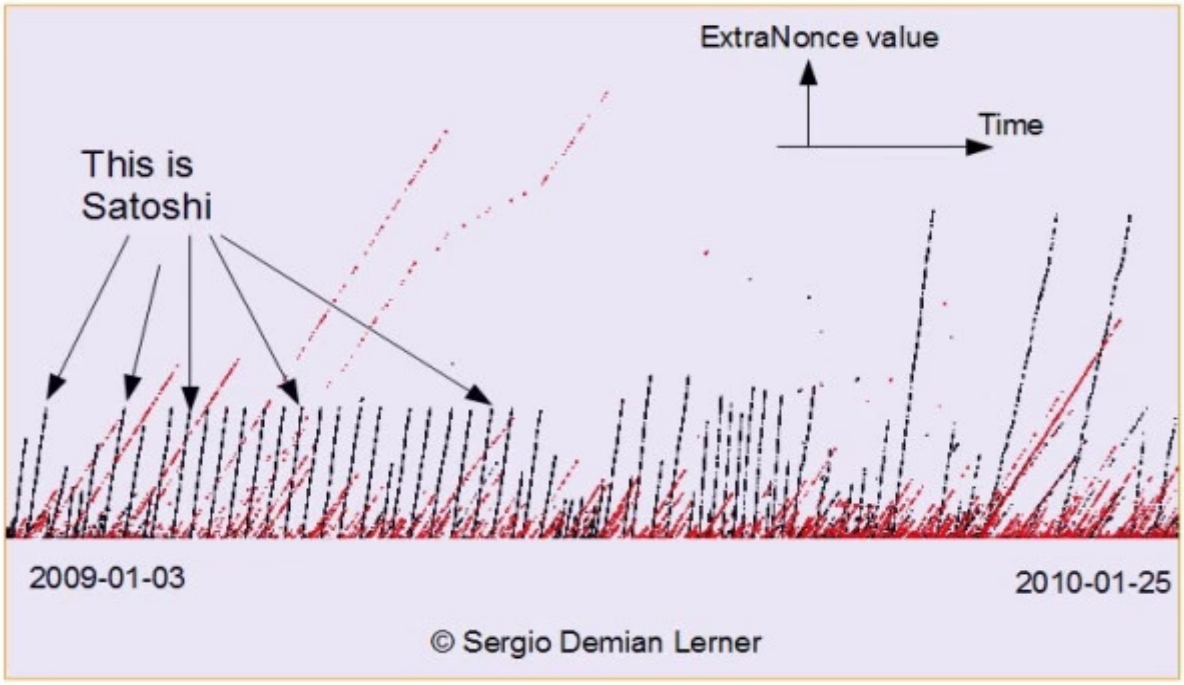
The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius

I won't discuss anything in this post. I'm tired of discussing technical things with people with skewed opinions and monetary interest. I've talked enough in the Bitcointalk forum (https://bitcointalk.org/index.php?topic=175996.0) about Satoshi. Some people screamed at me. But a picture is worth a thousand words. And I will show pictures that everyone can replicate. Please forgive me for the awful image design.

The graphs were made by a new block chain analysis technique I tested that consist on tracking the ExtraNonce fields in the coinbase field of the coinbase transaction, which is the one that creates bitcoins. As far as I know, is hasn't been done before. In the following graphs each dot is the creation of 50 BTC. I have only analyzed and printed graphs from block 0 upto block 36288. I wonder what will I get when I process the remaining three years.
The extraNonce fields increments every time the nonce fields (which is 32 bits) overflows, so it's a slow realtime clock, until the application is restarted, in which case it goes back to 1. Note the X-Axis in the graphs is not time (as it's said on the graph). It's the block number (that's a mistake).

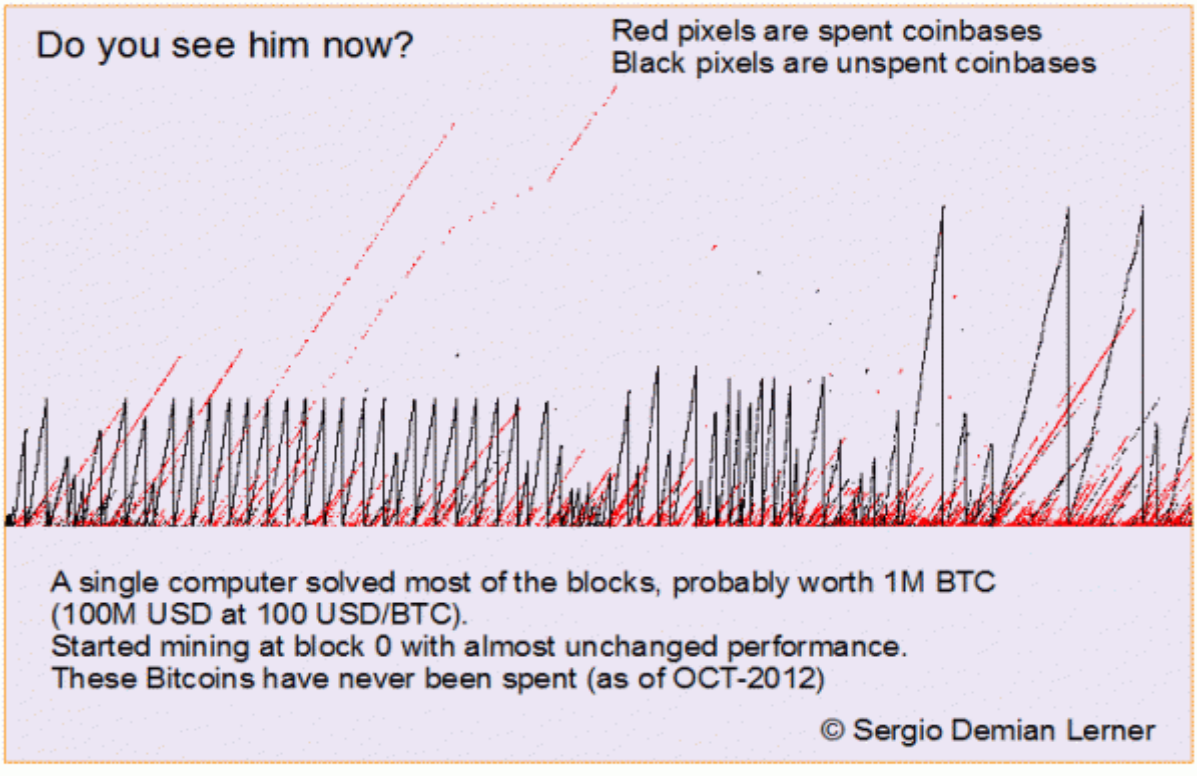
I don't think there is a moral obligation not to publish this information since it's already on public domain (the blockchain). Also Satoshi was completely aware of the poor anonymization capabilities of Bitcoin (a trade-off for performance and reduced bandwidth). Nevertheless, this lost of privacy could have been absent if random ExtraNonces had been used instead of incremental ones. So I could be thought as a Bitcoin privacy vulnerability for the miners.

Disclaimer: I can't assure with 100% certainty that the all the black dots are owned by Satoshi, but almost all are owned by a single entity, and that entity began mining right from block 1, and with the same performance as the genesis block. It can be identified by constant slope segments that occasionally restart. Also this entity is the only entity that has shown complete trust in Bitcoin, since it hasn't spend any coins (as last as the eye can see). I estimate at eyesight that Satoshi fortune is around 1M Bitcoins, or 100M USD at current exchange rate. I'm sure there will be plenty of people that will carefully analyze the source data set and come up with the exact figure, which will be very close, but nevertheless they will scream at me again.



(https://bitslog.files.wordpress.com/2013/04/all10-5-e1366485644588.jpg)

The vertical lines in the graph below were added by me, to show when the mining application is restarted, approximately every 100 hours, probably to backup the wallet.



(https://bitslog.files.wordpress.com/2013/04/all10-5-p2-e1366486301633.gif)

One of the consequences of these graph is that if the real name of the sender of a single transaction belonging to the entity is identified, then Satoshi mystery identity will be revealed. I bet that this will happen in the days following this post.

These are the tools and assumptions I made:

1. I used the file boostrap,dat, I assume that boostrap.dat contains only the best chain (not orphan blocks)

2. I only take into account coinbase transactions.

3. I've assumed that if a coinbase output is spent, then none of the spent coins went back to Satoshi.

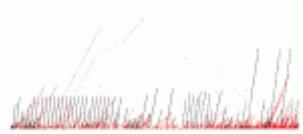
Note that from the 1814400 BTC awarded, 1148800 BTC has never been spent (63%). I suppose (but have not checked it yet) that these are exactly the segments that belong to the mystery entity,
If someone wants to check my computations, is welcomed, because I used a special block chain parser made by myself with little testing.

If anyone wants the source data set, is here Upto36288 (https://bitslog.files.wordpress.com/2013/04/upto36288.xls).

If you like my work and want to encourage me in researching further you can donate to this address: 17mcFB7Xyymd9hxp2bgNPz1ruWsdoPoCnZ

Best regards,
Sergio.

Edit: For comparison, here is the same diagram but using time (instead block number) in the X-axis. Note that the slopes are now completely coherent.



(https://bitslog.files.wordpress.com/2013/04/all-t1000-5.gif)

Bitcoin , Satoshi Nakamoto

This entry was posted on April 17, 2013, 6:32 am and is filed under Uncategorized. You can follow any responses to this entry through RSS 2.0. You can leave a response, or trackback from your own site.

COMMENTS (26) TRACKBACKS (1)

#1 by Lasse Birk Olesen on April 17, 2013 - 11:49 am

"One of the consequences of these graph is that if the real name of the sender of a single transaction belonging to the entity is identified, then Satoshi mystery identity will be revealed. I bet that this will happen in the days following this post."