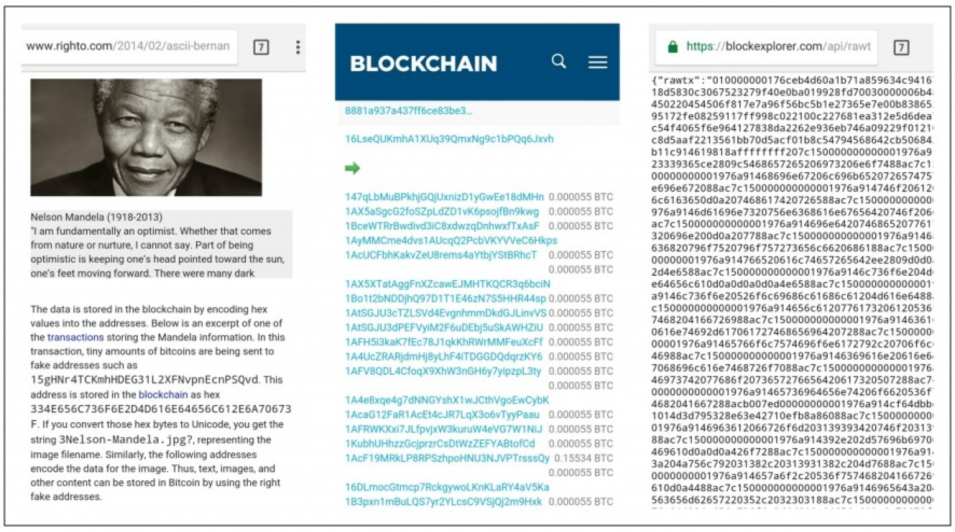
Steganography in Bitcoin's Blockchain

bebee.com/producer/@roberto-a-foglietta/steganography-in-bitcoin-s-blockchain



www.righto.com/2014/02/ascii-bernan

Nelson Mandela (1918-2013)
"I am fundamentally an optimist. Whether that comes from nature or nurture, I cannot say. Part of being optimistic is keeping one's head pointed toward the sun, one's feet moving forward. There were many dark

The data is stored in the blockchain by encoding hex values into the addresses. Below is an excerpt of one of the transactions storing the Mandela information. In this transaction, tiny amounts of bitcoins are being sent to fake addresses such as `15gHNr4TCKmhHDEG31L2XFNvpnEcnPSQvd`. This address is stored in the blockchain as hex `334E656C736F6E2D4D616E64656C612E6A70673F`. If you convert those hex bytes to Unicode, you get the string `3Nelson-Mandela.jpg?`, representing the image filename. Similarly, the following addresses encode the data for the image. Thus, text, images, and other content can be stored in Bitcoin by using the right fake addresses.

BLOCKCHAIN

```
8881a937a437ff6ce83be3...

16LseQUKmhA1XUq39QmxNg9c1bPQq6Jxvh

➡

147qLbMuBPkhjGQjUxnizD1yGwEe18dMHn  0.000055 BTC
1AX5aSgcG2foSZpLdZD1vK6psojfBn9kwg  0.000055 BTC
1BceWTRrBwdivd3iC8xdwzqDnhwxfTxAsF  0.000055 BTC
1AyMMCme4dvs1AUcqQ2PcbVKYVVeC6Hkps
1AcUCFbhKakvZeU8rems4aYtbjYStBRhcT  0.000055 BTC
                                    0.000055 BTC
1AX5XTatAggFnXZcawEJMHTKQCR3q6bciN
1Bo1t2bNDDjhQ97D1T1E46zN7S5HHR44sp  0.000055 BTC
1AtSGJU3cTZLSVd4EvgnhmmDkdGJLinvVS  0.000055 BTC
1AtSGJU3dPEFVyiM2F6uDEbj5uSkAWHZiU  0.000055 BTC
1AFH5i3kaK7fEc78J1qkKhRWrMMFeuXcFf  0.000055 BTC
1A4UcZRARjdmHj8yLhF4iTDGGDQdqrzKY6  0.000055 BTC
1AFV8QDL4CfoqX9XhW3nGH6y7yipzpL3ty  0.000055 BTC
                                    0.000055 BTC
1A4e8xqe4g7dNNGYshX1wJCthVgoEwCybK
1AcaG12FaR1AcEt4cJR7LqX3o6vTyyPaau  0.000055 BTC
1AFRWKXxi7JLfpvjxW3kuruW4eVG7W1NiJ  0.000055 BTC
1KubhUHhzzGcjprzrCsDtWzZEFYABtofCd  0.000055 BTC
1AcF19MRkLP8RPSzhpoHNU3NJVPTrsssQy  0.15534 BTC
                                    0.000055 BTC
16DLmocGtmcp7RckgywoLKnKLaRY4aV5Ka
1B3pxn1mBuLQS7yr2YLcsC9VSjQj2m9Hxk  0.000055 BTC
```

https://blockexplorer.com/api/rawt

{"rawtx":"010000000176ceb4d60a1b71a859634c9416
18d5830c3067523279f40e0ba019928fd70030000006b4
450220454506f817e7a96f56bc5b1e27365e7e00b83865
95172fe08259117ff998c022100c227681ea312e5d6dea
c54f4065f6e964127838da2262e936eb746a09229f0121
c8d5aaf2213561bb70d5acf01b8c54794568642cb50684
b11c914619818affffffff207c15000000000001976a9
23339365ce2809c546865726520697320 6e6f7488ac7c1
0000000001976a91468696e67206c696b652072657475
e696e672088ac7c150000000000001976a914746f20612
6c6163650d0a207468617420726588ac7c150000000000
976a9146d61696e7320756e6368616e67656420746f206
ac7c150000000000001976a914696e642074686520776 1
320696e200d0a207788ac7c150000000000001976a9146
636820796f7520796f757273656c6620686188ac7c1500
00000001976a914766520616c74657265642ee2809d0d0
2d4e6588ac7c150000000000001976a9146c736f6e204d
e64656c610d0a0d0a0d0a4e6588ac7c15000000000001
a9146c736f6e20526f6c69686c61686c61204d616e6488
c150000000000001976a914656c6120776173206120536
74682041667269 88ac7c150000000000001976a9146361
0616e74692d617061727468656964207288ac7c1500000
00001976a91465766f6c7574696f6e6172792c20706f6c
46988ac7c150000000000001976a9146369616e20616e6
7068696c616e7468726f7088ac7c150000000000001976
46973742077686f207365727665642061732050 7288ac7
0000000000001976a91465736964656e74206f6620536f
4682041667288acb007ed00000000001976a914cf64dbb
1014d3d795328e63e42710efb8a86088ac7c1500000000
01976a91469636120667 26f6d203139393420746f20313
88ac7c150000000000001976a914392e202d57696b6970
469610d0a0d0a426f7288ac7c150000000000001976a91
3a204a756c792031382c20313931382c204d7688ac7c15
0000000001976a914657a6f2c20536f757468204166726
610d0a4488ac7c150000000000001976a9146965643a20
563656d62657220352c2032303188ac7c150000000000

Published on March 24 on beBee

Introduction

Recently the news reported that some people discovered into Bitcoin's Blockchain **the existence of a couple of thousands of secret messages**.

In particular some of them are containing links to illicit information, links that could be broken removing the pointed source *ab origine* and leaving the broken and thus useless links in the Blockchain.

Among this stuff, the news reported that it were concealed an image, such kind of image that it would illigal to keep in any civil and developed country.

For this reason someone argues that because the Blockchain could not amended by this information, the whole Bitcoin Blockchain should consider illegal and thus destroyed.

Did you had a loud laugh? It is ok and you would not have any need to read this article. Otherwise, keep reading.

Steganography

Steganography is the practice of concealing a secret message into another one in such a way those look at the public message cannot see the secret one nor suspect it exists at all.

For example, the hidden message may be written with an invisible ink – like lemon juice – between the visible lines of a private letter – like in the **The Name of the Rose**.

The word steganography combines the Greek words*steganos* (**στεγανός**), meaning "covered, concealed, or protected," and *graphein* (**γράφειν**) meaning "writing".

The first recorded use of the term was in 1499 by **Johannes Trithemius** in his **Steganographia**, a treatise on cryptography and steganography, disguised as a book on magic.

Some implementations of steganography that lack a shared secret are forms of **security through obscurity**, and key-dependent steganographic schemes adhere to **Kerckhoffs's principle**.

Blockchain and Bitcoin

A **blockchain** is a continuously growing list of records, called *blocks*, which are linked and secured using **cryptography**.

By design, a blockchain is inherently resistant to modification of the data.

It works as an open, **distributed ledger** that can record transactions between two parties efficiently and in a verifiable and permanent way by a.

Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the ledger's network majority.

Blockchains are **secure by design** and exemplify a distributed computing system with high **Byzantine fault tolerance**. **Decentralized** consensus has therefore been achieved with a blockchain.

Blockchain was invented by **Satoshi Nakamoto** in 2008 for use in the **cryptocurrency** **bitcoin**, as its public transactions ledger.

The invention of the blockchain for bitcoin made it the first digital currency to solve the **double spending** problem without the need of a trusted authority or central server.

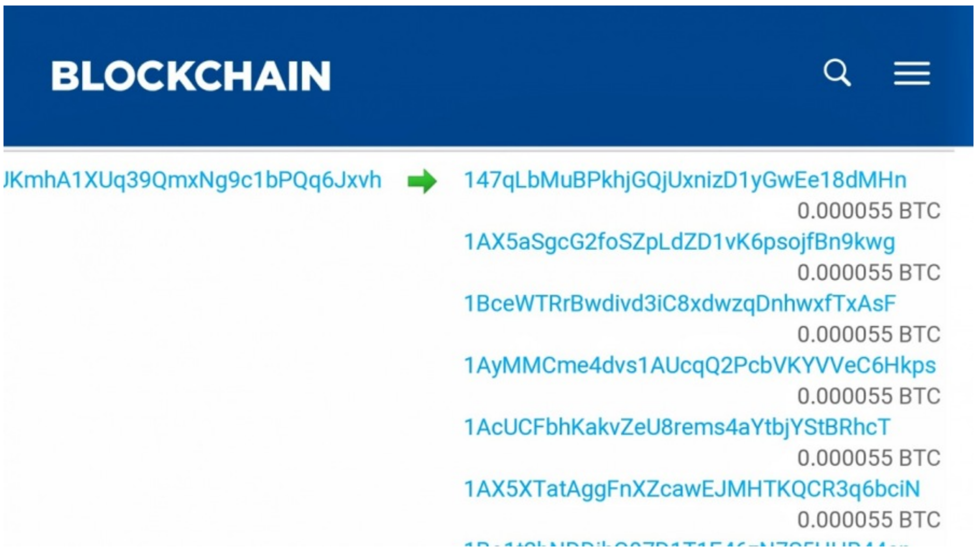
Here we are!

Stenography in bitcoin's blockchain is not an issue because stenography happens in any format data is stored, inevitably.

Amazingly, someone might be surprised that bitcoin's blockchain could contain arbitrary information, piece by piece, in a sequence of transactions like a Mandela's Tribute which is publicly available and engraved in, forever.

It is not an issue

However, it became clear that this is not an issue in the moment we check how the Mandela's Tribute is stored into bitcoin's blockchain:



```
JKmhA1XUq39QmxNg9c1bPQq6Jxvh  ➡  147qLbMuBPkhjGQjUxnizD1yGwEe18dMHn
                                                      0.000055 BTC
                                 1AX5aSgcG2foSZpLdZD1vK6psojfBn9kwg
                                                      0.000055 BTC
                                 1BceWTRrBwdivd3iC8xdwzqDnhwxfTxAsF
                                                      0.000055 BTC
                                 1AyMMCme4dvs1AUcqQ2PcbVKYVVeC6Hkps
                                                      0.000055 BTC
                                 1AcUCFbhKakvZeU8rems4aYtbjYStBRhcT
                                                      0.000055 BTC
                                 1AX5XTatAggFnXZcawEJMHTKQCR3q6bciN
                                                      0.000055 BTC
```

Did you see anything else than letters and numbers? Nope? Me neither.

That's the main point of the steganography. In order to collect back the hidden message we need some information:

there is a hidden message

where is the hidden message

how to extract the hidden m.

how to decode the hidden m.

If we do not know just one of these information, it may impossible or near impossible for us to retrieve the information. Moreover, if we ignore the first point, we do not even know the information exists at all.

It is a matter of will, only

Imagine we know that accessing a steganographed image into the bitcoin blockchain is a violation of the law.

Imagine, we have all the information above about this conceiled image and we have the bitcoin's blockchain.

Thus, we have all we need to access at that data at every time we would like.

The will to break the law it is our own personal choice, only. There is not any way to break the way above our will.

Those will break the law, they will do with or without bitcoin or blockchain.

It is the blockchain not the bitcoin

Any issue of this kind is not related in any way with bitcoin but with blockchain. Obviously, bitcoin need blockchain to exist and to work but the blockchain technology may be used in many others ways that have nothing to do with bitcoin.

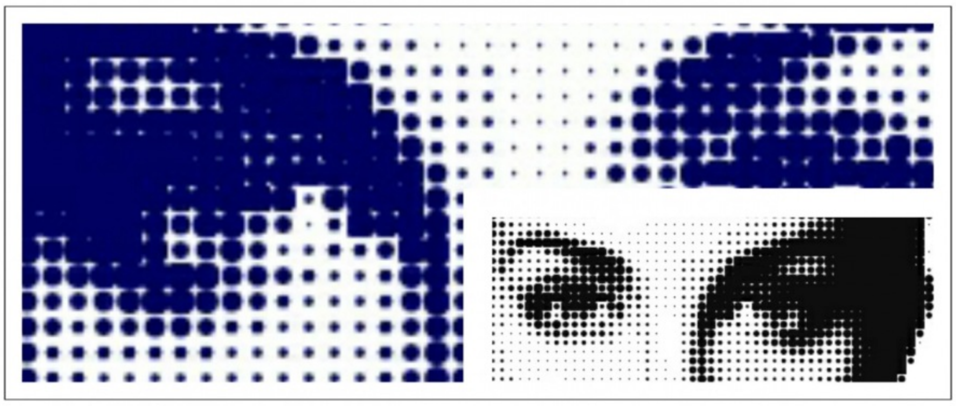
Thus, every blockchain open ledger may suffer such kind of conceiled injection and nobody could prevent from it in any way.

Every public write-only ledger would suffer the same issue. Moreover, every public write-once not editable block of information could be used for the same aim. Let me explain this.

Bits and dots

Mandela's tribute has been encoded in sequence of bitcoin's transactions.

Such collection of numbers and letters could be converted into a image file which would be a specific encoding of an image which is nothing else thab a way to convert bits into dots.



Every software developer could write a piece of code that is able to show an image {a set of dots} starting from a block of alphanumeric characters {an arbitrary text} and s/he could code it in such a way that a specific page of the Holy Bible – the first page of the Genesis, for example – would decoded into such Mandela picture. Any other page would probably show anything else than random dots but that one in particular, baam!

How this could be possible? Because the dots are related with bits by a deconding function. Usually we write encoding and decoding function to convert dots in bits and bits in dots back.

Bits <-- d(_) || e(_) --> Dots

We could always choose to write a deconding function that makes such a magic and if we are smart enough, we could write the inverse of such deconding function to obtain the encoding function.

A couple of foreign spies

If the two of us were spies we may decide before to separate, to choose a specific public writen-only text and later we may exchange between us just functions:

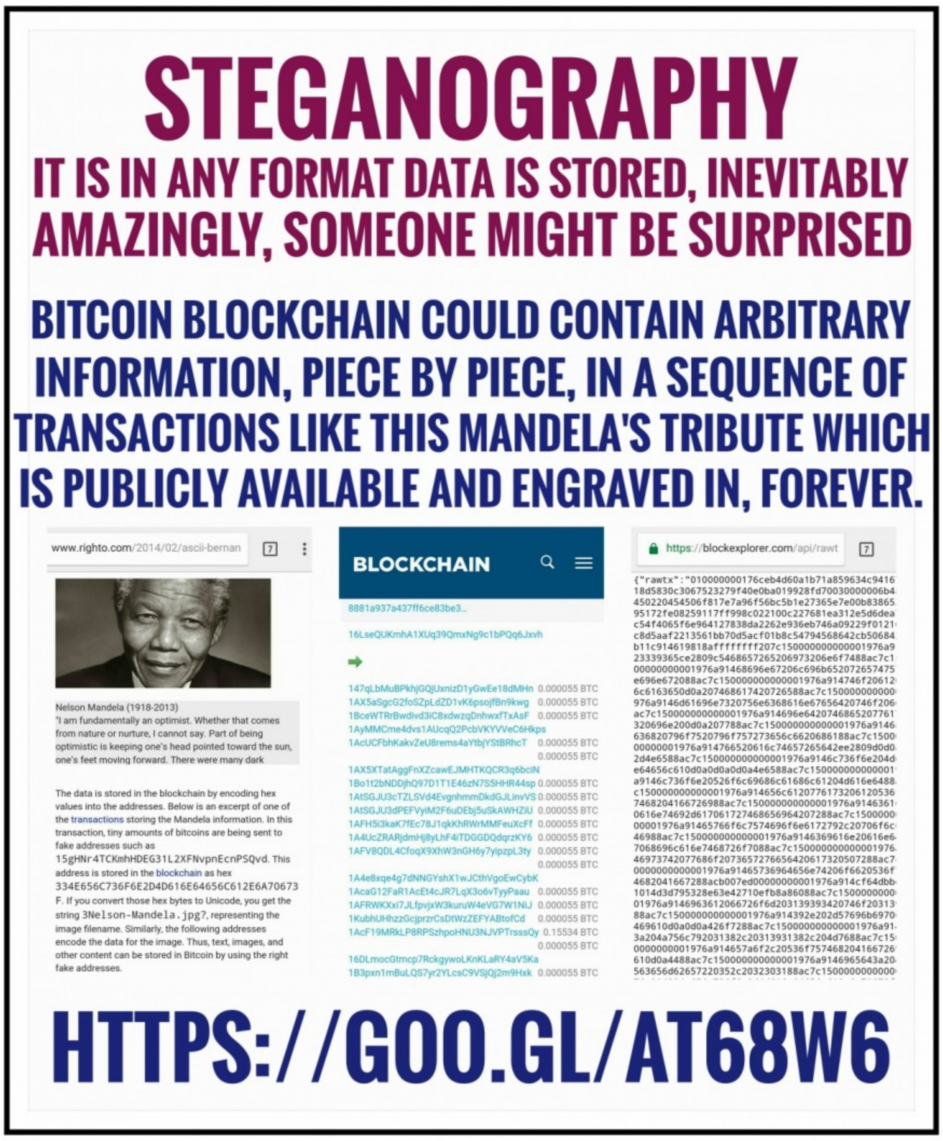
> whisper_1 = function_1(first_amendment);
>
> ...
>
> whisper_N = function_N(first_amendment)

The day we might be caught by CIA whispering secrets each others, we would claim that all those whispering were into first amendment!

Sure, it is true but the will to break the law is in our own will and not in the tools we might use for doing so.

Conclusion

Feel free to download this image and share with your friends for their peace of minds and hearts: good guys knew!



STEGANOGRAPHY

IT IS IN ANY FORMAT DATA IS STORED, INEVITABLY AMAZINGLY, SOMEONE MIGHT BE SURPRISED

BITCOIN BLOCKCHAIN COULD CONTAIN ARBITRARY INFORMATION, PIECE BY PIECE, IN A SEQUENCE OF TRANSACTIONS LIKE THIS MANDELA'S TRIBUTE WHICH IS PUBLICLY AVAILABLE AND ENGRAVED IN, FOREVER.

Nelson Mandela (1918-2013)
"I am fundamentally an optimist. Whether that comes from nature or nurture, I cannot say. Part of being optimistic is keeping one's head pointed toward the sun, one's feet moving forward. There were many dark

The data is stored in the blockchain by encoding hex values into the addresses. Below is an excerpt of one of the transactions storing the Mandela information. In this transaction, tiny amounts of bitcoins are being sent to fake addresses such as `15gHNr4TCKmhHDEG31L2XFNvpnEcnPSQvd`. This address is stored in the blockchain as hex `334E656C736F6E2D4D616E64656C612E6A70673F`. If you convert those hex bytes to Unicode, you get the string `3Nelson-Mandela.jpg?`, representing the image filename. Similarly, the following addresses encode the data for the image. Thus, text, images, and other content can be stored in Bitcoin by using the right fake addresses.

```
8881a937a437ff6ce83be3...

16LseQUKmhA1XUq39QmxNg9c1bPQq6Jxvh

➡

147qLbMuBPkhjGQjUxnizD1yGwEe18dMHn 0.000055 BTC
1AX5aSgcG2foSZpLdZD1vK6psojfBn9kwg  0.000055 BTC
1BceWTRrBwdivd3iC8xdwzqDnhwxfTxAsF  0.000055 BTC
1AyMMCme4dvs1AUcqQ2PcbVKYVVeC6Hkps
1AcUCFbhKakvZeU8rems4aYtbjYStBRhcT  0.000055 BTC
                                    0.000055 BTC
1AX5XTatAggFnXZcawEJMHTKQCR3q6bciN
1Bo1t2bNDDjhQ97D1T1E46zN7S5HHR44sp 0.000055 BTC
1AtSGJU3cTZLSVd4EvgnhmmDkdGJLinvVS 0.000055 BTC
1AtSGJU3dPEFVyiM2F6uDEbj5uSkAWHZiU  0.000055 BTC
1AFH5i3kaK7fEc78J1qkKhRWrMMFeuXcFf  0.000055 BTC
1A4UcZRARjdmHj8yLhF4iTDGGDQdqrzKY6  0.000055 BTC
1AFV8QDL4CfoqX9XhW3nGH6y7yipzpL3ty  0.000055 BTC
                                    0.000055 BTC
1A4e8xqe4g7dNNGYshX1wJCthVgoEwCybK
1AcaG12FaR1AcEt4cJR7LqX3o6vTyyPaau  0.000055 BTC
1AFRWKXxi7JLfpvjxW3kuruW4eVG7W1NiJ  0.000055 BTC
1KubhUHhzzGcjprzrCsDtWzZEFYABtofCd  0.000055 BTC
1AcF19MRkLP8RPSzhpoHNU3NJVPTrsssQy 0.15534 BTC
                                    0.000055 BTC
16DLmocGtmcp7RckgywoLKnKLaRY4aV5Ka
1B3pxn1mBuLQS7yr2YLcsC9VSjQj2m9Hxk  0.000055 BTC
```

{"rawtx":"010000000176ceb4d60a1b71a859634c9416
18d5830c3067523279f40e0ba019928fd70030000006b4
450220454506f817e7a96f56bc5b1e27365e7e00b83865
95172fe08259117ff998c022100c227681ea312e5d6dea
c54f4065f6e964127838da2262e936eb746a09229f0121
c8d5aaf2213561bb70d5acf01b8c54794568642cb50684
b11c914619818affffffff207c15000000000000001976a9
23339365ce2809c5468657265206973206e6f7488ac7c1
00000000001976a91468696e67206c696b652072657475
e696e672088ac7c15000000000000001976a914746f20612
6c6163650d0a207468617420726588ac7c150000000000
976a9146d61696e7320756e6368616e67656420746f206
ac7c15000000000000001976a914696e642074686520776
320696e200d0a207788ac7c15000000000000001976a9146
636820796f7520796f757273656c6620686188ac7c1500
00000001976a914766520616c74657265642ee2809d0d0
2d4e6588ac7c15000000000000001976a9146c736f6e204d
e64656c610d0a0d0a0d0a4e6588ac7c15000000000000001
a9146c736f6e20526f6c69686c61686c61204d616e6488
c15000000000000001976a914656c612077617320612053
7468204166726988ac7c15000000000000001976a9146361
0616e74692d617061727468656964207288ac7c1500000
00001976a91465766f6c7574696f6e6172792c20706f6c
46988ac7c15000000000000001976a9146369616e20616e6
7068696c616e7468726f7088ac7c15000000000000001976
46973742077686f20736572766564206173205072886ac7
000000000001976a91465736964656e74206f6620536f
4682041667288acb007ed00000000001976a914cf64dbb
1014d3d795328e63e42710efb8a86088ac7c1500000000
01976a91469636120667266f6d203139393420746f20313
88ac7c15000000000000001976a914392e202d57696b6970
469610d0a0d0a426f7288ac7c15000000000000001976a91
3a204a756c792031382c20313931382c204d7688ac7c15
0000000001976a914657a6f2c20536f757468204166726
610d0a4488ac7c15000000000000001976a9146965643a20
563656d62657220352c2032303188ac7c1500000000000

HTTPS://GOO.GL/AT68W6

That's all folks.