**BLOCK CHAIN ID**

**Abstract:**

The Paper attempts to find secure and reliable way of maintaining registry of people identity using Bitcoin blockchains and cryptography tools. First section of the paper describes current challenges of maintaining registry in centralized way. Second section of paper describes the concepts of cryptography technologies used. Final section describes one of the implementation for maintaining decentralized registry of people identity “Blockchain ID”.

**Introduction:**

Person Identity or ID is document that provides information about the person. They are required to provide basic entitlements like to enter country or organization, driving a car. Personal Identification to a person is provided by Government organizations and private organization which are centralized. Most of the people failed get Identification because lack of governance, infrastructure. Centralized registry of personal information exposed personal information when they are attacked such as attacks on NSA, Sony and iCloud by hackers.

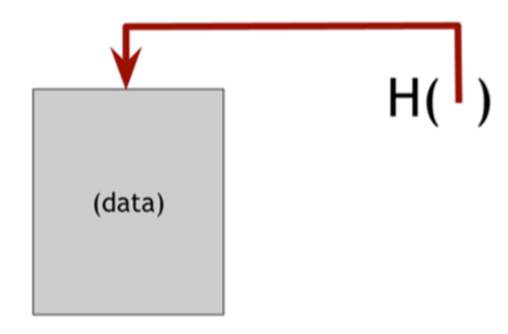
**Solution:**

Optimal solution is to create decentralized registrar using Blockchains and sophisticated cryptography tools.

**Concepts of Block Chains:**

**Hash Pointer:**

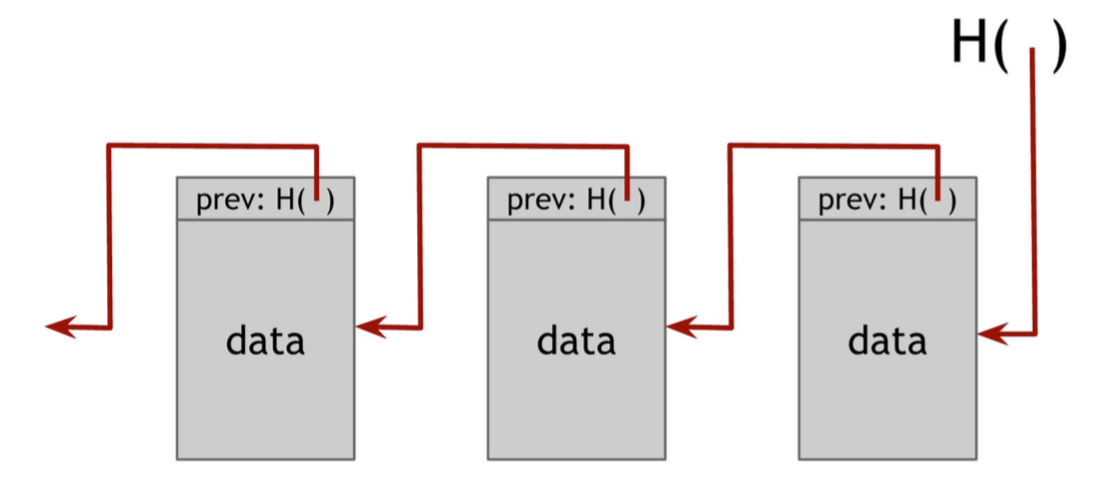
Is pointer where information is stored together with cryptographic hash. Hash pointer gives more flexibility than normal pointer to verify that information is not changed.



**Data structures using Hash Pointers**

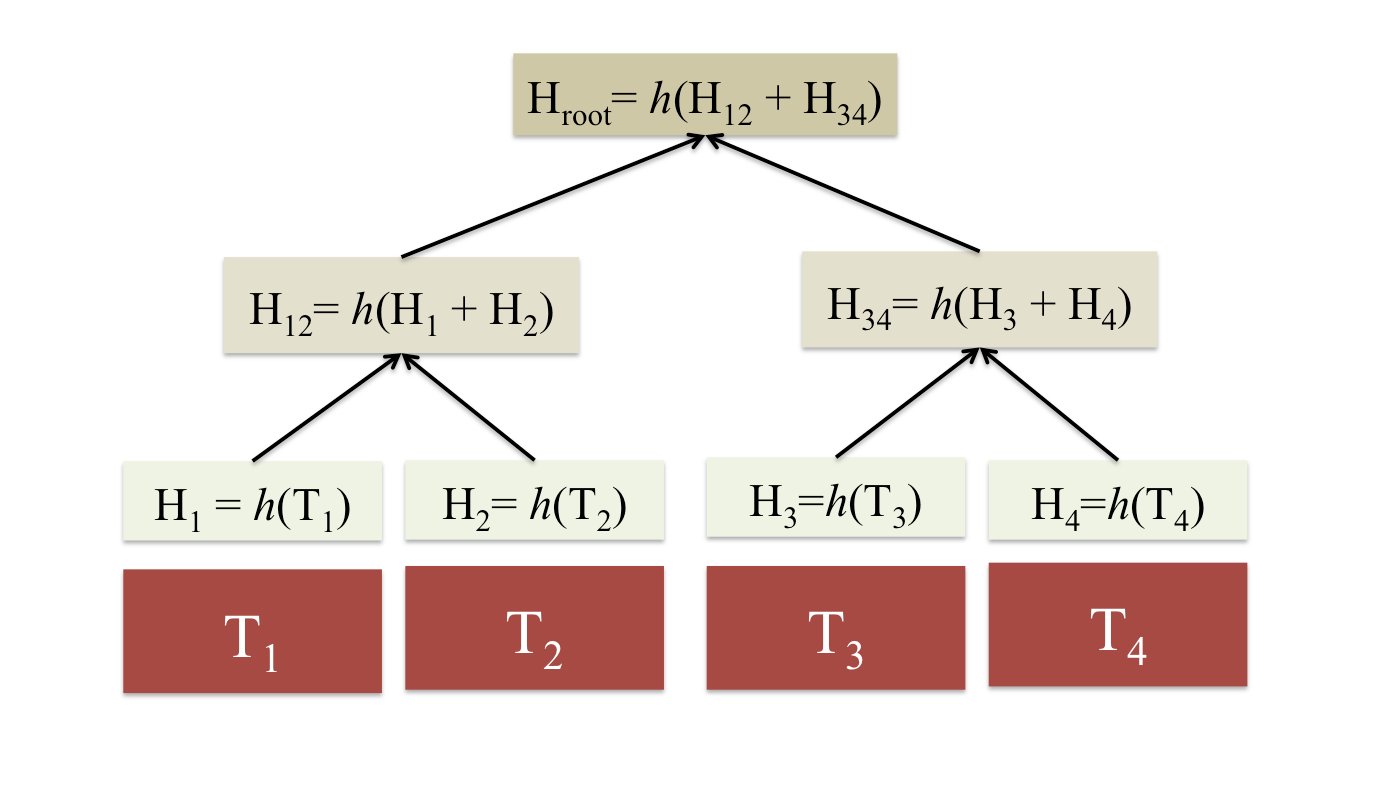
**Blockchains:**

A blockchain linked list that uses hash pointer instead of normal pointer. By using hash pointer each block not only tells about value of previous block but also digest of the value that allows to verify that the information hasn’t changed . Block Chains are tamper resist. If anyone tries to change data in any block hash value changes which don’t match with succeeding block. He has to change upto head of blockchain which can’t be changed which is also known as genesis block.



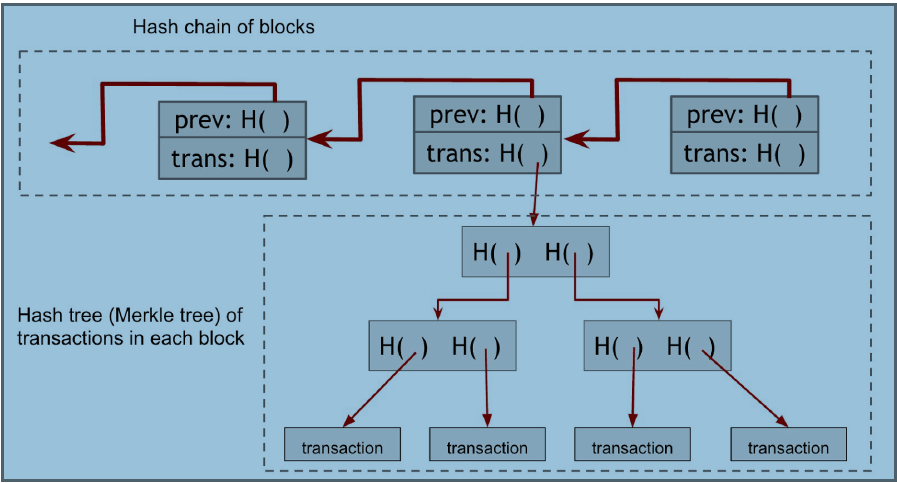
**Merkle Tree:**

Is Binary Tree with hash pointers. Hash of blocks are stored in parent nodes. Merkle Trees are tamper resistant. If anyone wants to tamper a block at bottom of the tree, that will cause hash pointer one level up to not match and he has tamper to root of the tree where he is not able to change. Proof of membership for Merkle tree unlike block chain can be checked in log(n) time.



**Bitcoin Blockchains:**

Bitcoin Blockchains are combination of blockchains and Merkle tree. Each block has a block header, a hash pointer to the previous block in the sequence. Second data structure is Merkle Tree internal to each block. Information saved in block chain is tamper proof. Once message saved in blockchain. message will be saved forever.



**SHA-256:**

The **SHA** (Secure Hash Algorithm) is one of the cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. **SHA**-**256** algorithm generates an almost-unique, fixed size **256**-bit (32-byte) hash. Hash is a one-way function – it cannot be decrypted back.

**PGP (Pretty Good Privacy) :**

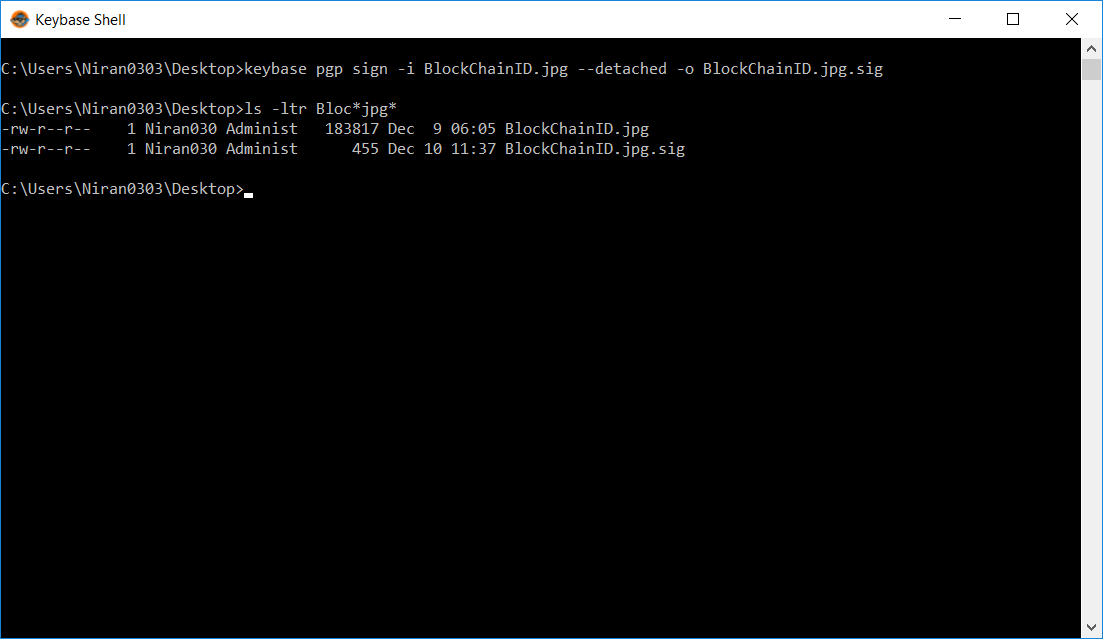
PGP is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting and decrypting texts, e-mails, files and directories

**Implementation of Block Chain ID**

1. Take image
2. Edit Photograph with details
3. Sign edited image using PGP key (Good Protection)
4. Create hash digest of three files full image, edited image, signature of edited image.
5. Add Merkle root of latest transaction, hash of three files full image,edited image, signature of edited image.
6. Verify message posted in Block Chain
7. Edited Image can be used as self-identity.

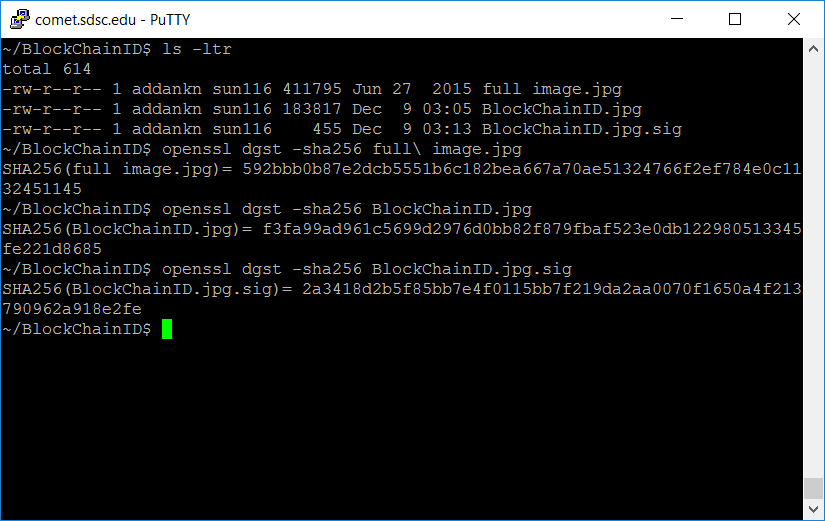
**Sign Edited Image:**

Edited Image is signed by using pgp tools like openpgp or keybase. Once document is signed we bind the state of the document to its cryptographic signature preventing us from changing its contents without detection.

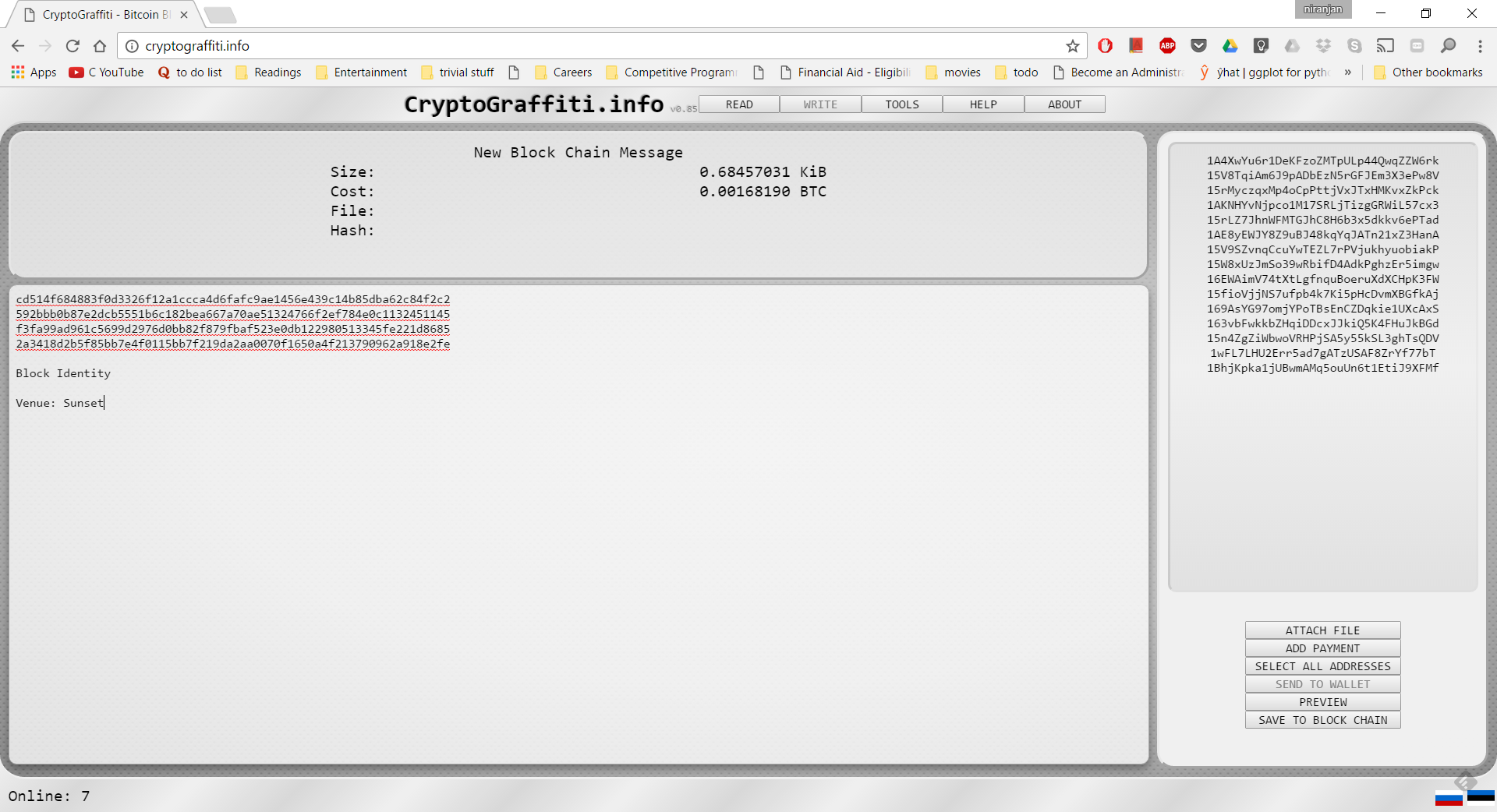


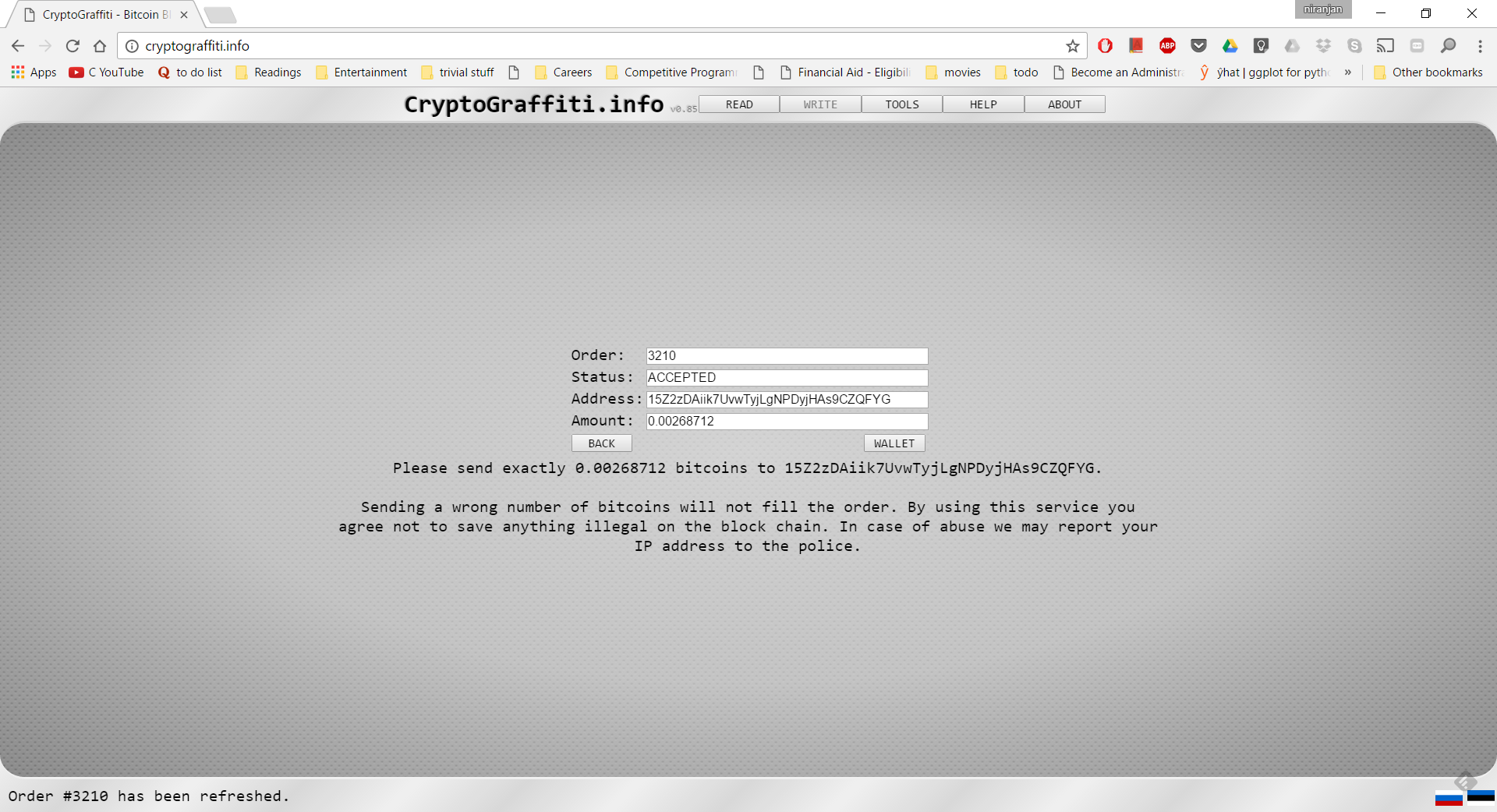
**Creating Hash of the files:**

Hash of files are created using cryptographic tools like openssl.

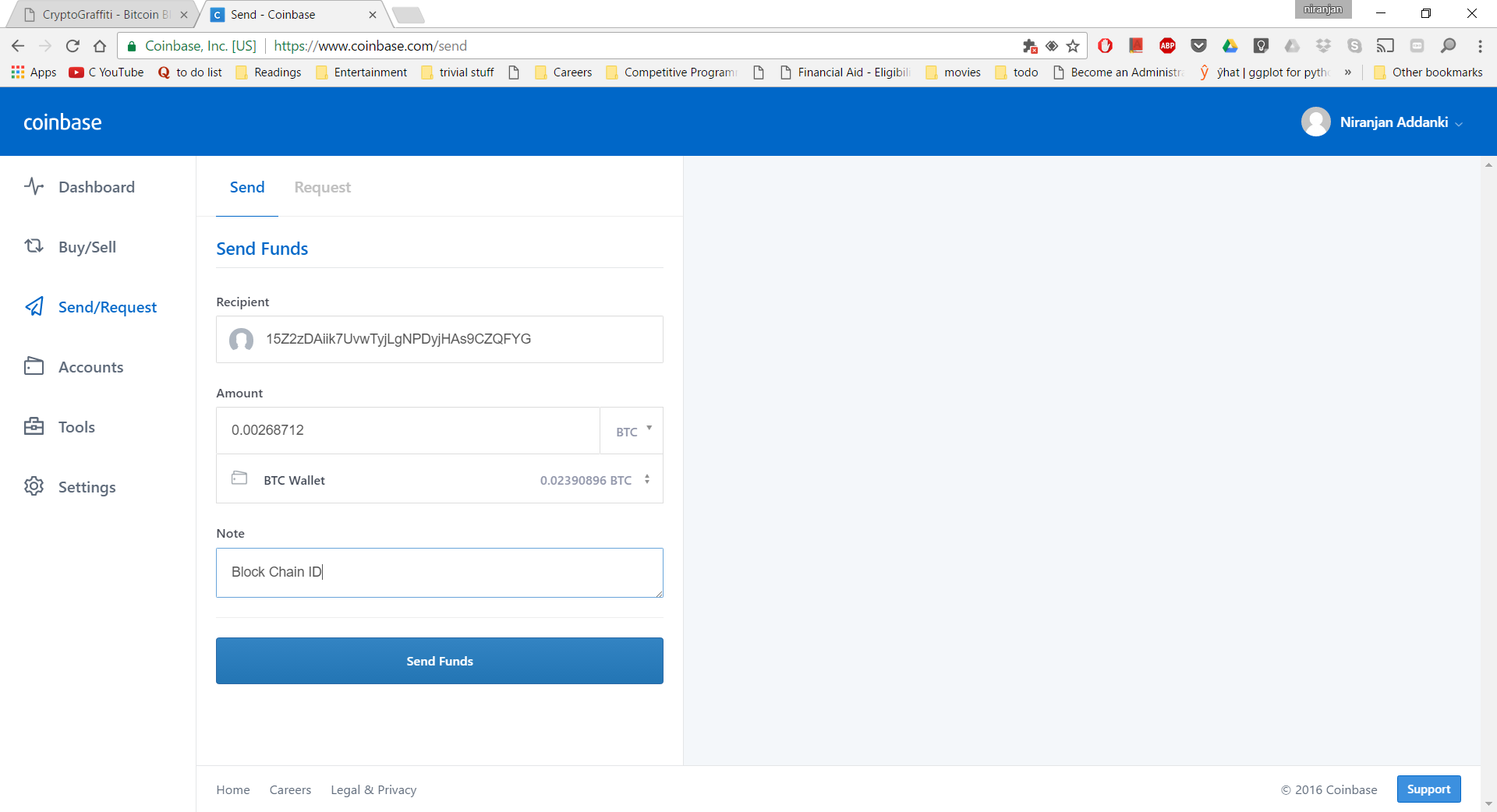


**Stamping Message on Bitcoin Block Chain:**

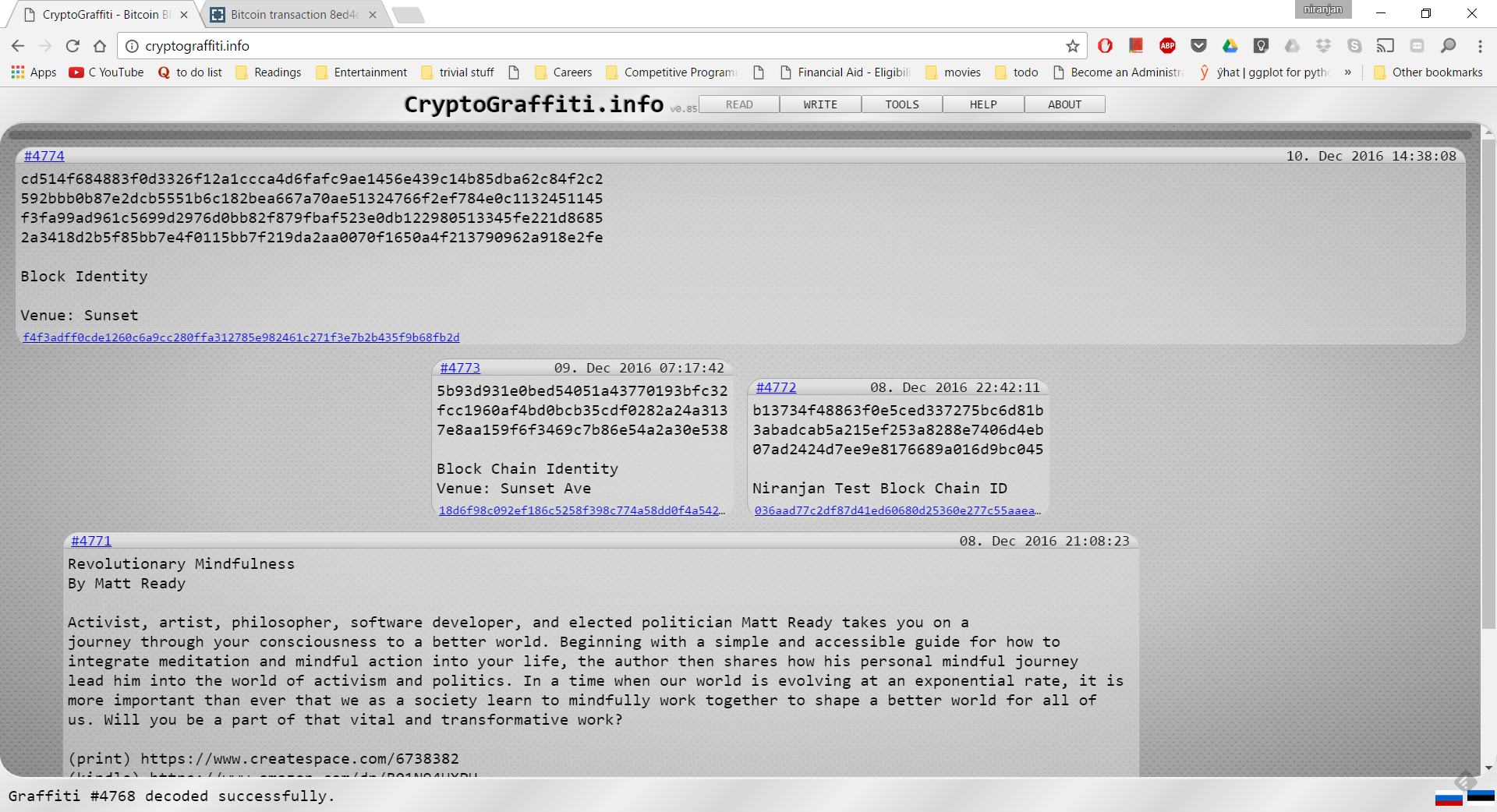




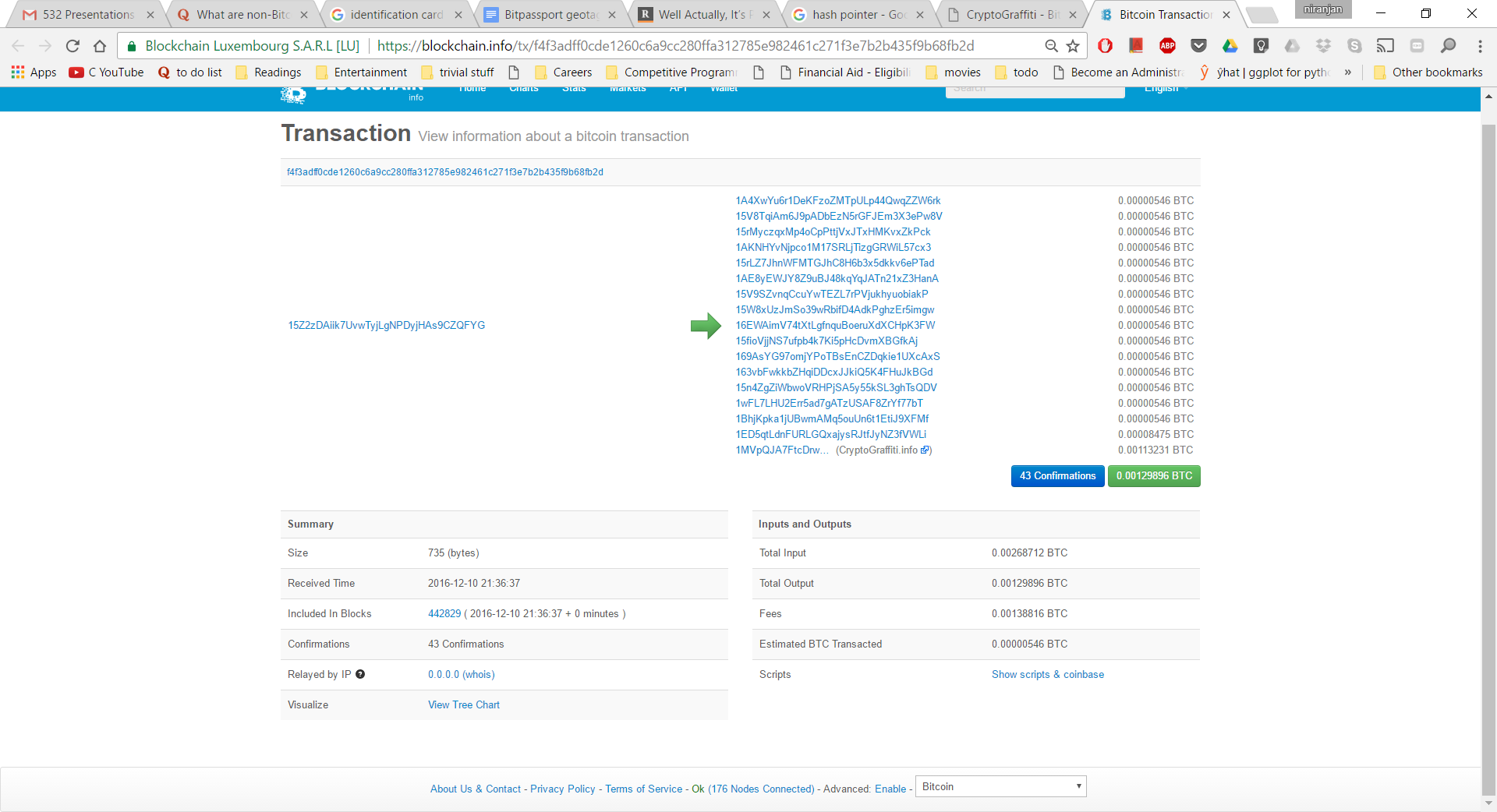
Payment to encoded bitcoin address



**Message posted on Blockchain**.

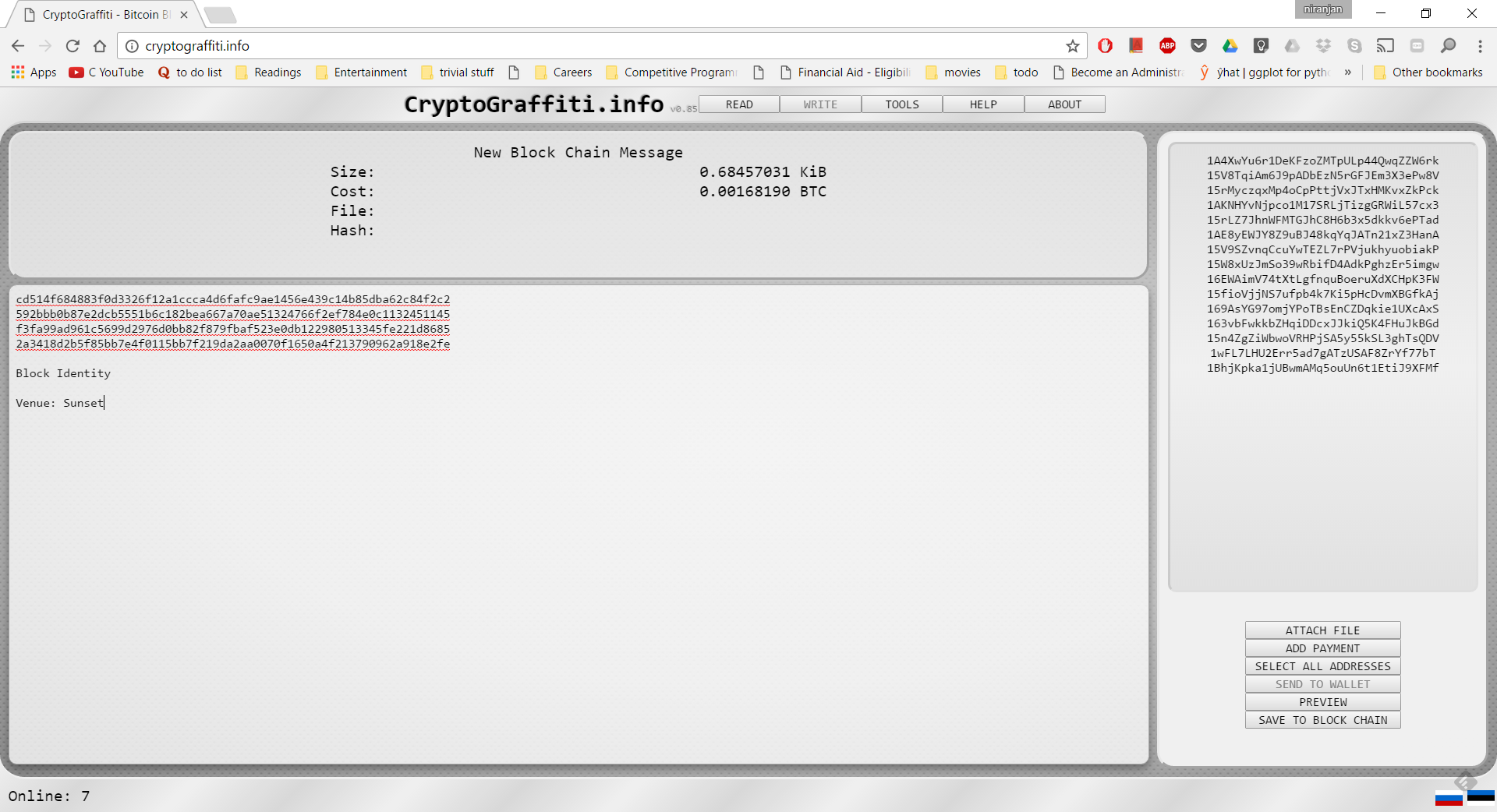


**Transaction Details**

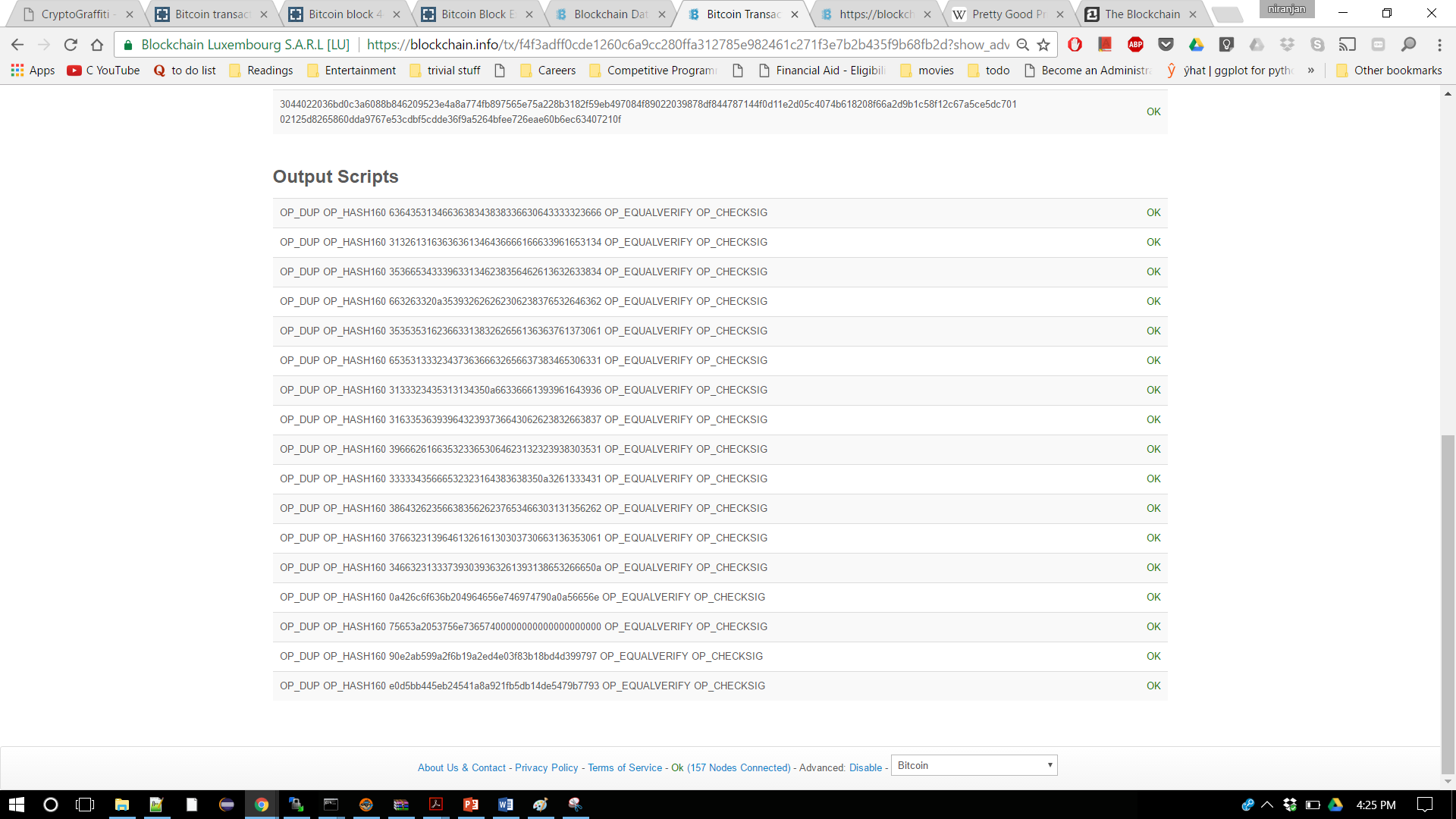


**Working of CryptoGraffiti:**

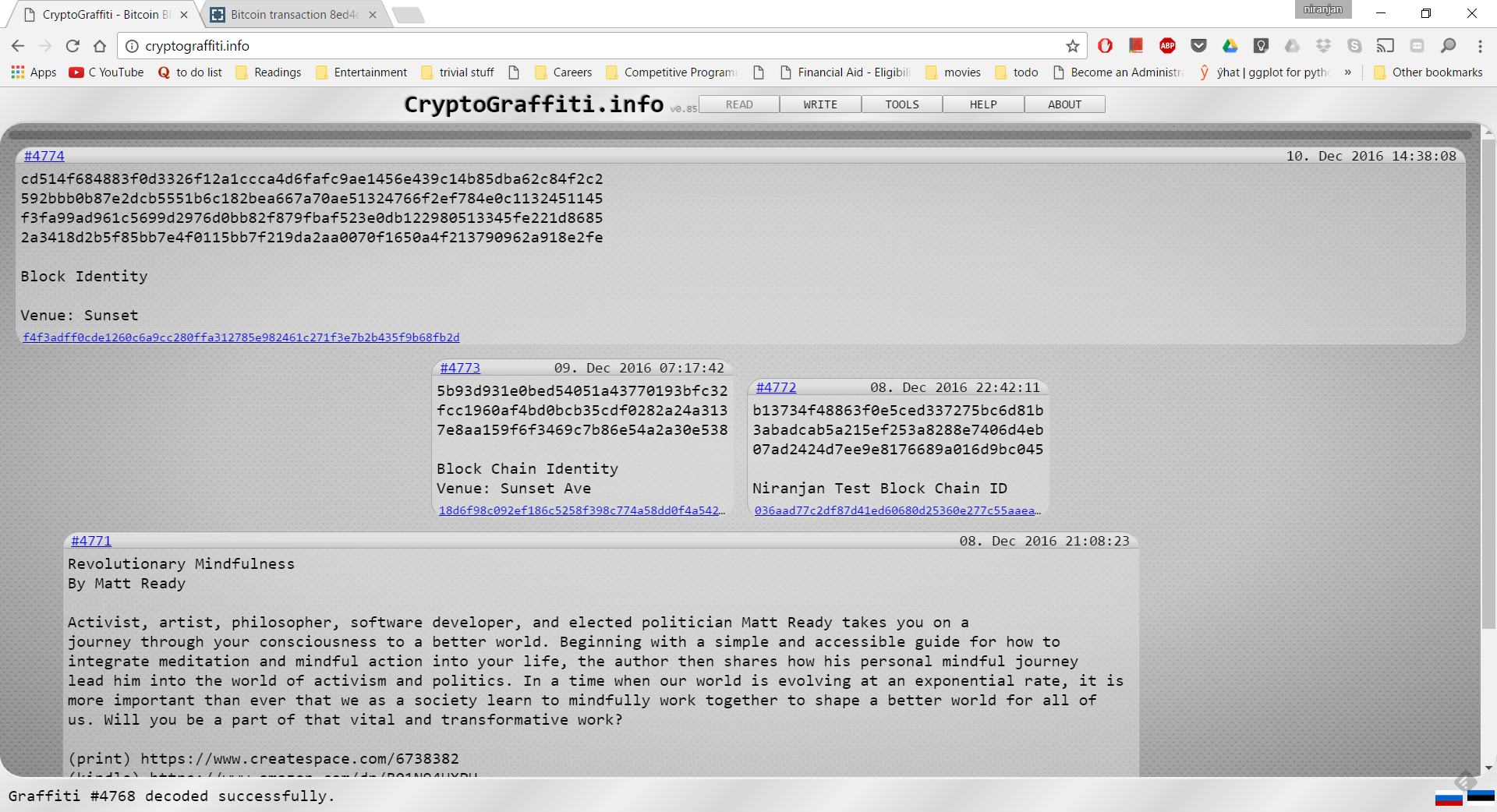
CryptoGraffiti encodes human readable message into corresponding bitcoin address. After successful transaction, transaction posted blockchain decoded into readable message that was entered.



**Encoded Bitcoin Addresses**



**Message posted on Block Chain after successful Transaction**



**Conclusion:**

Blockchain technology is evolving at rapid speed. It has applications in many areas of Our interest. When the problem is with trust and certainty, Blockchain technology provides solution it.

**Future scope of work:**

* Automate the process of creation ID.
* Maintain register/ledger like system on the block chain to track changes

**Reference**:

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies*. Princeton University Press.
2. <https://github.com/MrChrisJ/World-Citizenship>
3. <https://en.wikipedia.org/wiki/Pretty_Good_Privacy>
4. <https://en.wikipedia.org/wiki/SHA-2>
5. <https://en.wikipedia.org/wiki/Blockchain_(database)>