Rapid Prototyping of a Mining Application for Cryptocurrency: Bitcoin

Henna Abdul Azeez
SRM University, Katankulathur,
Chennai, Tamil Nadu, India

G Vadivu
SRM University, Katankulathur,
Chennai, Tamil Nadu, India

ABSTRACT

Bitcoin is the world's first completely decentralized peer-to-peer digital currency. The main reason behind using bitcoin is that of its low transaction fee compared to any other transfers like western union, credit card transaction etc. and bitcoin transactions are transparent. So we don't have to consider about tax problems.It avoids Taxation.

Keywords: block-chain, bitcoin mining, Betweeness Centrality

1. INTRODUCTION

A software developer pseudo-named Satoshi Nakamoto published the Bitcoin Protocol (Nakamoto, 2008) which outlined the theory of a decentralized currency. This was followed in January 2009 by the release of the open-source Bitcoin software, and the mining of the first Bitcoins

Bitcoin for Business: Since its creation, Bitcoin has evolved from a mathematical proof of concept to a rapidly expanding economic network. It is now being used in business transactions around the world. Businesses big and small have shown interest in integrating the Bitcoin platform into their operations and providing new services within the Bitcoin economy. A growing number of merchants accept Bitcoin, because the transaction costs associated with the currency are generally lower than those for using credit or debit cards.

Bitcoin Mining: Instead of being made on a printing press or by a central authority, Bitcoins are generated by solving complicated algorithmic searches by powerful computers, a process known as mining. Most Bitcoin users do not mine, but purchase or trade for their Bitcoin. Mining doesn't affect the average Bitcoin user much, but is still a very important part of the Bitcoin ecosystem.

All newly mined Bitcoin, along with every transaction, are publicly recorded. This record is known as the block-chain. While the block-chain records transaction details, it does not record any personal identifying information about the senders or recipients. The block-chain is a critical feature to maintain the transparency of the Bitcoin system, and make counterfeiting or double spending impossible.

While Bitcoins are created through mining that pursuit is getting increasingly complicated and expensive, as companies and technology fans race to build the powerful computers required for Bitcoin production. There's a limit to the number of Bitcoins that can be mined. After the year 2140, no more Bitcoins will be created, and the total amount ever available is fixed at 21 million, more than half of which have already been mined.

2. LITERATURE REVIEW

2.1. EXISTING SYSTEM

So far, using credit/debit cards for a bulk amount transaction, we do have to surrender a huge amount in the name of 'tax'. Almost up to 10% roughly we pay for tax which varies for each bank. And also for each and every transaction we have to provide a record of proof stating that from where the money came?

2.2.PROPOSED SYSTEM

Our proposed system, bitcoin charges only a negligible amount as tax when compared with credit/debit. If credit/debit charges 10%, bitcoin charges 1% tax.
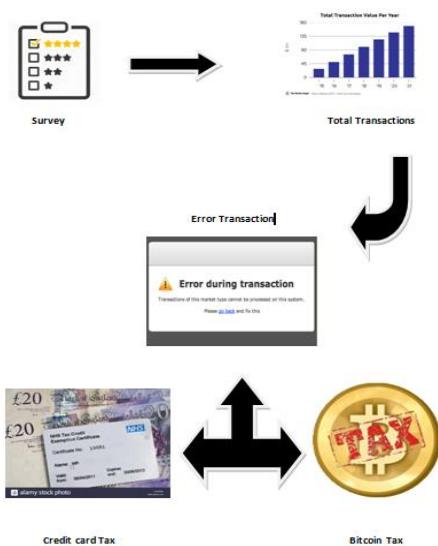
2.2.1. METHODOLOGY

Fig1: Flow Diagram

From the survey conducted, we can identify the total number of erroneous transaction from the total number of transaction.

We can able to classify the tax variation between the credit card and the bitcoin respectively.

2.2.2. NETWORK DIAGRAM

A **network diagram** is a unique kind of cluster **diagram** that represents a cluster or small structure of computers or other **networking** devices. Preidentified icons or symbols are **used** to draw **network** appliances and the style of lines between two nodes describes the type of connection

1) Erroneous Transaction Network

The Figure shows how many transactions are done through the e-commerce website and what mode of payment is used for each website.
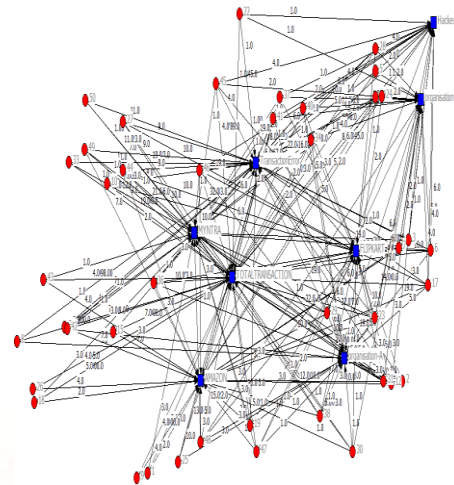

Fig2: Erroneous transaction

2) Analysis of Tax Network:

The Figure shows the Total transactions that are done using credit card, debit card and Bitcoin.
So for each mode of payment how much tax has been paid whereas for bitcoin how much tax is paid is represented in the form of network graph
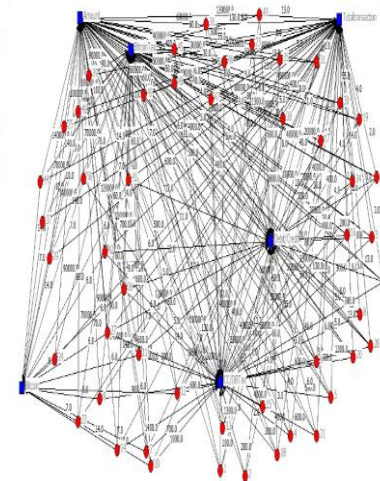

Fig 3: Analysis of Tax Network

3. EXPECTED OUTPUT
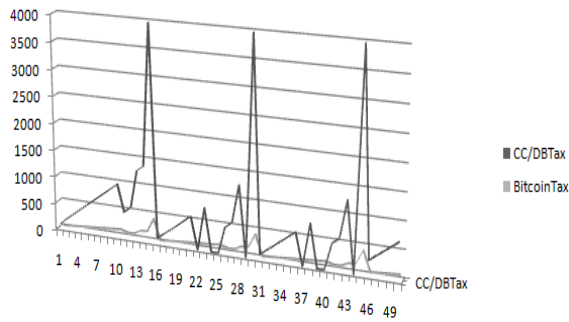
➢ Credit/debit vs. bitcoin tax

Fig4: Tax Differentiation
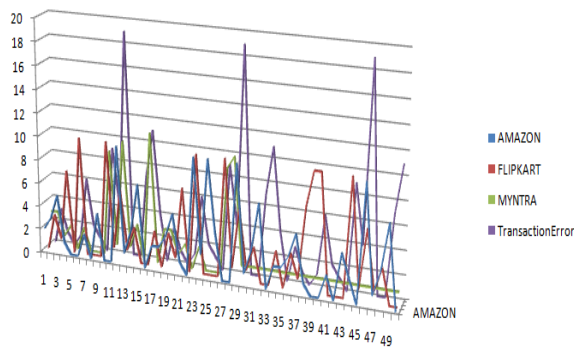
➢ Erroneous transaction

Fig 5: Diagramatic Representation of Erroneous Transaction

➢ Betweeness Centrality

In graph theory, **betweenness centrality** is a measure of **centrality** in a graph based on shortest paths.

Code:

```
> library(igraph)
> a<-sample_pa(TOTALTRANSACTION)
> betweenness(a)
[1] 0 0 0 1 0
> a
IGRAPH D--- 5 4 -- Barabasi graph
+ attr: name (g/c), power (g/n), m (g/n), zero.appeal (g/n), algorithm (g/c)
+ edges:
[1] 2->1 3->1 4->1 5->4
> plot(a)
```
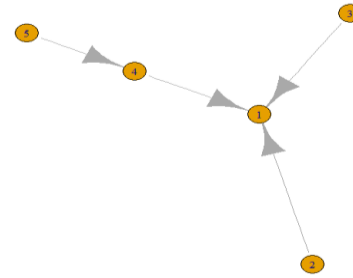
Output:

Fig 6: Betweeness Centrality Measure

Explanation

In this paper we propose the first truly scalable algorithm for online computation of betweenness centrality of both vertices and edges in an evolving graph where new edges are added and existing edges are removed.

Our method is able to keep the betweenness centrality measures up to date online.

4. CONCLUSION

This research paper points out the significance of "why bitcoin is being used". From the statistical analysis made using credit/debit vs. bitcoin transaction, we can conclude that by using bitcoin we don't have to spend a large amount on taxes. It just takes a negligible amount as tax when compared to debit/credit card.

Secondly, if a transaction goes erroneous in bitcoin, unless the recipient wills your claim goes in vain. There is no interference of third party like a bank in bitcoin.

REFERENCES

1) W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

2) H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure time stamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

3) R Vidhya, G Vadivu, Research Document Search using Elastic Search, Indian Journal of Science and Technology 9 (37), 2016.

4) T. Y. J. Naga Malleswari , G. Vadivu, Map reduce: A Technical Review, Indian Journal of Science and Technology, Vol 9(1), January 2016.

5) S. Haber, W.S. Stornetta, "How to time-stamp a digital documzent," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

6) D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

7) S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

8) K.Sornalakshmi, G.Vadivu, A Survey on Realtime Analytics Framework for Smart Grid Energy Management, International Journal of Innovative Research in Science, Engineering and Technology, March 2015

9) P.-Y. Ting, F. D. Chu, "Enhancing the security promise of a digital time-stamp", *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, pp. 342-347, 2008.

10) M. Mambo, K. Usuda, E. Okamoto, "Proxy signatures: Delegation of the power to sign message", IEICE Trans. Fundam., vol. E79-A, no. 9, pp. 1337-1354, Sep. 1996.

11) Navin, G. Vadivu, Big Data Analytics for Gold Price Forecasting Based on Decision Tree Algorithm and Support Vector Regression (SVR), International Journal of Science and Research (IJSR), March 2015.

12) "Recommendation ITU-R TF.1876 International Telecommunication Union", Trusted Time Source for Time Stamp Authority, 2010.

13) G.Vadivu, Waheeta Hopper, Ontology Mapping of Indian Medicinal Plants with Standardized Medical Terms, Journal of Computer Science, ISSN 1549-3636., Aug, 2012.

14) Protocols for public key cryptosystems. In *Proc. 1980 Symp. on Security and Privacy.*