Bitcoin Resource: Anonymity & Challenges



Md. Ikbal Hossain 1510786042

Ibrahim Khalil 1520775042

Md. Faisal Hossan Shakib 1521156642

Abul Kawsar 1531500042

Department of Electrical & Computer Engineering

North South University

Date 22.12.19

Course – CSE499A

Instructor’s Name: MohammadAshrafuzzaman Khan

# Abstract

# In this article we tried to show how bitcoin network is working despite the fact of its anonymity. We found about a fixed number of total bitcoins which was mentioned as resource of bitcoin. But we don’t know if it is really existing or any equivalent resource to bitcoin is available or not. Thus, we can say the network system could be based on a hype where the system is still working effectively. And there is one challenging thing that, those who mine bitcoin need to solve algorithm related problems, and for that very high configuration PC is required. For this, it seems from normal computer it may not be possible to mine bitcoin or it could damage the PC if it is attempted.

Table of Contents

[Abstract 2](#_Toc485290869)

[Table of Contents 3](#_Toc485290870)

[List of Figures 5](#_Toc485290871)

[List of Tables 6](#_Toc485290872)

[1 Introduction 7](#_Toc485290873)

[2 Background 7](#_Toc485290874)

[2.1 Subheading 1 7](#_Toc485290875)

[2.2 Subheading 2 7](#_Toc485290876)

[2.2.1 First Sub-subheading 7](#_Toc485290877)

[2.2.2 Second Sub-subheading 7](#_Toc485290878)

[3 Methodology 8](#_Toc485290879)

[4 Results and discussion 8](#_Toc485290880)

[5 Conclusions and recommendations 8](#_Toc485290881)

[6 Acknowledgements 8](#_Toc485290882)

[7 References 8](#_Toc485290883)

[Appendix A: Place the title of appendix here 9](#_Toc485290884)

# List of Figures

1. Bitcoin accept product page
2. Reclaiming Disk Space
3. Bitcoin Transactions

# List of Tables

This section should begin on a new page. Microsoft Word® has an automated feature under "Insert Table of Figures." Change the caption label from “figure” to “table.” For this feature to work, all tables must have a caption. This should be one of the last pages to be completed. Some examples follow:

1. Model parameters 3

2. Fuel consumption data under nominal conditions 10

# Introduction

Bitcoin is a cryptocurrency which is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer or exchange of assets. It is an online virtual currency which is already being used based on public key cryptography, proposed in 2008 in a paper [1] written by someone named Satoshi Nakamoto as pseudonym. It is fully working from January 2009 and its broad acceptance, simplified by the presence of exchange markets allowing easy changing with conventional currencies (EUR or USD), has brought it to be the most useful digital currency.

Satoshi Nakamoto who is known as the bitcoin creator, discussed about the internet's dependence on trusted third parties such as banks and credit card companies to process electronic payments. The traditional method is still working for most transactions around the world but problems may occur when financial institutions simply the buying and selling of goods on the internet. The traditional system is used to accept a certain percentage of fraud as unavoidable. But fraud increases everyone's cost of doing business more or less. Nakamoto proposed this digital payment system that is based on cryptographic proof instead of trust.

**2. Background**

Bitcoin, first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency. Since the release of bitcoin, over 6,000 altcoins (alternative variants of bitcoin, or other cryptocurrencies) have been created. It is used to securely store and transfer any amount of value of a third party anywhere in the world. It is a decentralized digital currency without a central bank or single administration that can be sent on the peer to peer bitcoin network without any intermediaries. Over the course of bitcoin's history, it has undergone rapid growth to become a significant currency both on and offline from the mid2010.

**2.1 Fiat currency and Bitcoin**

Fiat currency is a money that is issued /printed by government and has a legal tender. The U.S. dollar is fiat money, as are the Euro, BDT and many other major world currencies. In some countries bitcoin is not fiat money like other currencies.

**2.1.1 Fiat currency vs Cryptocurrency**

There are two types of currencies either its fiat or cryptocurrency.

**Fiat** is “legal tender” backed by a “central government.” It can take the form of physical dollars or it can be represented electronically, such as with bank credit. The government controls the supply and you can use fiat to pay your taxes.

**Cryptocurrency** is not backed by a central government or bank as it is decentralized and global. Its form is more like bank credit sans the bank. An algorithm controls the supply and you can’t pay your taxes with it.

The most significance difference between fiat and cryptocurrency is that they both operates in a different way. With bitcoin the transition happens quickly and without involving of a third party but with an online fiat money exchange a some of e-money(USD,BDT,EURO ETC) is translated into an equal amount of e-value through the use of mobile wallet.

**2.1.2 Is Bitcoin a Fiat Currency?**

As stated earlier, a fiat currency is a money that is not backed by gold or any other hard asset. Its value is declared by fiat alone – the issuing government simply decrees that the currency has worth. You can’t trade a Bitcoin for an ounce of gold at a fixed price. Cryptocurrency isn’t issued by any government and there’s a fixed ceiling on how many can exist.

**2.1.3 Why Bitcoins have values?**

Bitcoin offers an efficient means of transferring money over the internet and is controlled by a decentralized network with a transparent set of rules, thus presenting an alternative to central bank-controlled fiat money.

Bitcoin and other digital currencies have been touted as alternatives to fiat money.

**But what gives any type of currency value?**

Answer: Because it is exchangeable easily and we know that the thing which can be exchangeable has values.

**2.1.4 Why Bitcoin values changes so much?**

* Like all things that have a finite supply, the value of a bitcoin is derived by the number of people that want to buy them vs the number of people that want to sell them.
* If more people want to buy bitcoins than are currently for sale (for example if a surge of people want to start using bitcoins to transfer value across borders, see more on this below) then the price goes up.
* If more people want to sell bitcoins than currently who wants to buy them, then the price goes down.
* One of the reasons that the price of bitcoin is so volatile is that many of the people buying bitcoins today are buying based on speculation(Speculation refers to the act of conducting a financial transaction that has substantial risk of losing value but also holds the expectation of a significant gain.) not because they actually want to use them.

Speculative buyers believe that in the future many people will want bitcoins (if this is true these future buyers will drive the price up) so speculators buy bitcoins now in anticipation of that future demand and price increase. However, speculative buyers are very sensitive to current events - news stories can quickly turn speculative buyers into speculative sellers. This flip-flopping of speculator sentiment is the main reason the price of bitcoin varies so wildly

**2.2 BITCOIN IS LIKE GOLD!**

Bitcoin's Perceived Value Sways

1. One reason why Bitcoin may fluctuate against fiat(4) currencies is the perceived store of value versus the fiat currency. Bitcoin has properties that make it similar to gold. It is governed by a design decision by the developers of the core technology to limit its production to a fixed amount, 21 million BTC.
2. Since that differs markedly from fiat currency, which is managed by governments who want to maintain low inflation, high employment, and satisfactory growth through investment in capital resources, as economies built with fiat currencies show signs of strength or weakness, investors may allocate more or less of their assets into Bitcoin.

**2.3 Prototype of Bitcoin**

Let us find out how the whole bitcoin thing works.

**2.3.1 How Bitcoin mining works?**

According to our research we found that there is a fixed 21million bitcoin set up by the core developers. When Bitcoin miner’s does mining (solves algorithms) they get rewards as Bitcoin from the core developers. So basically, we can see that the miners share their resources to solve algorithms and for the rewards they get bitcoins from the core developers. Then the miners store it to the bitcoin wallet to sell it or exchange it. The more people joins the bitcoin network the more difficult the algorithms become to solve. So the Miners uses a pool method to solve the problem.

**Miners:** Who uses resources to solve Algorithms/math problems by using special kind of software (CGMiner, Multiminer , BitMiner etc.).

**Resources:** At beginning the mining is usually happened by just using normal computer. But it used lots of power then they used GPU’s which was able to solve the problem faster but it was also power consuming too then a special kind of chip is made which is called ASIC.It uses less power and works faster.

**Pool Method:** A group of miners who share their resources within the group to solve more difficult algorithms then they share their rewards among them.

**2.3.2 How to Store Bitcoin:** Cold storage is an offline wallet provided for storing bitcoins. With cold storage, the digital wallet is stored on a platform that is not connected to the internet, thereby, protecting the wallet from unauthorized access, cyber hacks, and other vulnerabilities that a system connected to the internet is susceptible to.

**2.3.3 Where does the math problem comes from?**

* It was given by the core developers (As per our findings)!
* The more people joins the bitcoin network the more difficult the algorithms become to solve
* So the Miners uses a pool method to solve the problem.

**2.3.4 What is the Resources of Bitcoin?**

As per our initial finding we can say that the resource of our bitcoin is 21million BTC. Which is a fixed amount set up by the core developers who developed the bitcoin.

At first, we can say that its like gold .How?

The more people joins the network it becomes more difficult to solve the algorithms. So when they solves the algorithms they get rewards as bitcoin(gold).So more people joins in the mining, it becomes more difficult to earn bitcoin because it has a fixed amount of value as like gold ,we know that there is a fixed amount of gold in earth which is approximate of 171,300 tones ( BBC).So bitcoin is like same there is fixed amount of it when more people joins to mining the more it becomes difficult to get.

# 3 Methodology

# 4 Results and discussion

# 5 Conclusions and recommendations

# 6 Acknowledgements

This section allows authors to acknowledge contributors and other sources that are not appropriate to list in the references section. Example:

This work was conducted under Grant No. 12345, administered by X. The authors are also particularly grateful to Dr. Jane Smith for her insight into the nature of Y.

# 7 References

This is the last section of the report, prior to any appendices. The references should not be double-spaced, but single-spaced. For a technical report, use the CSE style.

[1] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. (2008)

[2] Reference 2 information.

[3] Reference 3 information.

# Appendix A: Place the title of appendix here

Provide appropriate appendices as necessary. Each appendix should begin on a new page.