A Conceptual Study Of Bitcoin

Rupali Chaudhary

Madhusoodan Tripathi

Vinayaka Tripathi

Abstract- Money is an integral part of society. It developed in several forms, with the growth of humanity. Cryptocurrency is latest form of money. It is possible that it will work as global money in future. Bitcoin is noted first cryptocurrency.

Keywords- Bitcoin, Digital currency, Framework, Market spread

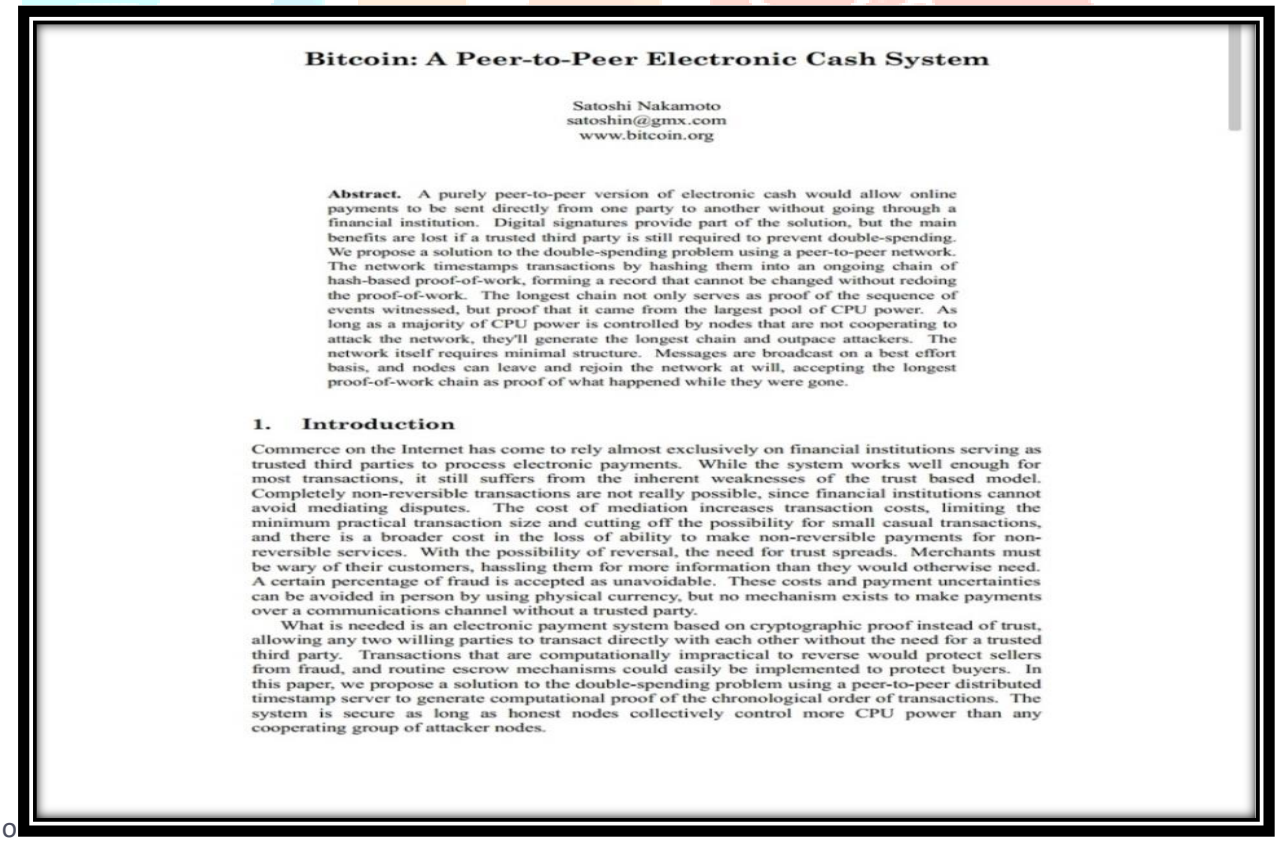
Objective- To present the concept of Bitcoin as cryptocurrency, history, framework, market share and emerging trends.

Introduction- Bitcoin is a cryptocurrency, a currency which is designed to work as money in form of payment mode outside the control of any person, group or entity. So, there is no need of third party involvement in financial transactions.

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and issue of Bitcoins is carried out collectively by the network. Through many of its unique properties, Bitcoin allows exciting uses that could not be covered by any previous payment system.

Journey of bitcoin-

Bitcoin was introduced to the public in 2009 by an anonymous developer or group using the name **Satoshi Nakamoto. *1**



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

o

Now a days Bitcoin is world's largest crypto currency by market capitalization. It has gone through several boom and bust cycles over its relatively short lifespan.

In August 2008, the domain name Bitcoin.org was registered. ***2**

Bitcoin.org from over the years: *3

Year	Bitcoin.org from over the years:
2009	Bitcoin open source implementation ofP2P currency
2010	Bitcoin Releases Version 0.3
2011	Bitcoin- A step towards censorship-resistant digital currency
2012	Bitcoin-the Libertarian Introduction
2013	The economics of Bitcoin
2014	The best places on the internet to learn about Bitcoin
2016	What is Gitian Building? How Bitcoin's security processes became a model for the open source community.
2017	Bitcoin: What's in the whitepaper?

History of Bitcoin (comparison with US dollars) for all time *4

Date	USD: 1 BTC	Summary
August 18, 2008 - January 2009	0 $	During this period, no one knew about Bitcoin. Only the bitcoin.org domain was registered and the blockchain was being developed.
February 2011 - April 2011	$ 1.00	Bitcoin takes parity with the dollar.
December 2012	$ 13.00	Grows slowly throughout the year.
December 2013	600 - 1000 $	The price dropped to $ 600, recovered to $ 1000, and fell back to the $ 500 range. Stabilizes to a range of ~ $ 650–800.
March 2014	450 - 700 $	The price continued to fall due to false reports of a Bitcoin ban in China and uncertainty that the Chinese government would seek to ban banks from dealing with digital currency exchanges.
March 2015	200-300 $	The price dropped until early 2015.
October - November 2016	600 - 780 $	As the Chinese yuan depreciated against the dollar, Bitcoin rose to $ 700.
September 2017	$ 5000	On September 1, 2017, Bitcoin traded at $ 5,000 for the first time, peaking at $ 5,013.91.
8 December 2017	$ 18,000	Bitcoin surpasses $ 18,000 for the first time at 00:28.
5 February 2018	$ 6200	Bitcoin price dropping below $ 7,000.
31 October 2018	$ 6,300	On Bitcoin's 10th anniversary, the price remains stable above $ 6,000 during a period of historically low volatility.
14 November 2018	$ 5590	Fall below $ 6,000.
24 November 2018	$ 3778	Fall below $ 4000.
29 November 2018	$ 4333	Bitcoin price has reached $ 4300.
4 January 2019	$ 3820	Bitcoin has continued to fall since the beginning of 2019.
7 February 2019	$ 3399	Lowest cost in Q1 2019.
24 February 2019	$ 4199	Bitcoin is starting to rise.

Review of Literature:

The US government has classified, what type of asset bitcoin is, which will prevent most market participants from adopting cryptocurrency-based business models (**PwC, 2015**) *5

Bitcoin transaction have become exempt from value added tax by the European Court of Justice, effectively recognizing it as a legitimate means of payment in Europe (**Perez, 2015**) *6

The combination of demand for a safe haven option and its price volatility helped Bitcoin to become the best performing currency of 2015 using the US Dollar Index (**Desjardins, 2016**) *7

The lack of trust leads to issues with investors as well. The dead pool of failed start-up has increased to 24, mostly citing "security" as the main reason for closure (**Hileman, 2016**) *8

Bitcoin transactions worth 2 billion USD happen every day and approximately over 300 million transactions have occurred till 2017. He also told If the merchant does not wait for the confirmation of the transaction, bitcoins can be double spent by attackers. **(Heston 2018)** *9

Framework:

Bitcoin is made by two words, '**Bit**' & '**Coin**'. If someone cut the information inside computers into smaller pieces, then he will find 1 and 0. These are called *bits*, coin is a form of currency.

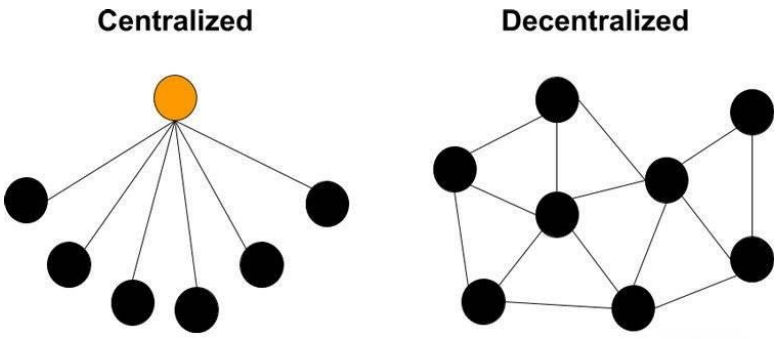
Bitcoins are just the plural of Bitcoin. **They are coins stored in computers**. They are not physical and only exist in the digital world. That's why Bitcoin is called *digital* currency.

The creator of Bitcoin made **three main concepts** for Bitcoin:

- Decentralized Networks
- Cryptography
- Supply and Demand

Decentralized Networks

When someone use internet browser and type in '*www.google.com*', then computer **starts a conversation** with Google's computers. Then, both computers start talking to each other and browser shows images, buttons, etc. If Google's servers were down for some reason, then no one be able to see these images and buttons. This is because the data is stored on a *centralized* network — **it is in one place**.



To understand the working of Bitcoin, it is essential to figure out what is **a decentralized network**. In a *decentralized* network, the data is **everywhere**. If Google used a decentralized network, someone would still be able to see the data, because it is everywhere, and not just in one place.

Cryptography

In World War II, **cryptography** was used a lot. It converted radio messages into code that nobody could read. To read it, it would need to convert back to the original message. To do that a key is required. *It was* possible through mathematical formulas.

Bitcoin uses cryptography in the same way. Instead of converting radio messages, Bitcoin uses cryptography to convert **transaction data**. That is why Bitcoin is called ***a cryptocurrency***.

Supply and Demand

Main concept of **supply and demand**: when something is **limited**, it has more value. The more people that want it, the more the price of it will go up.

Bitcoin uses this same concept. **The supply of Bitcoin is limited**. Bitcoin is produced at **a fixed rate**, which will decrease over time — *it halves every four years*. Bitcoin has a limit of 21 million coins; once there are 21 million Bitcoins, no more coins can be created.

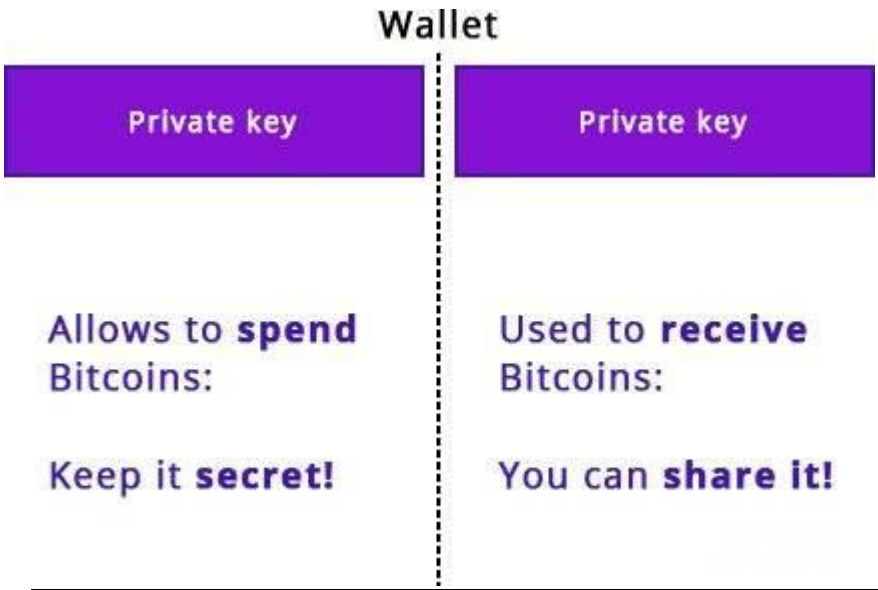
Bitcoin uses **a decentralized network**, **the Bitcoin database is shared**. This shared database is known as ***a distributed ledger*** and it is accessed using the blockchain.

Can Someone make fake sender Identity?

When a bitcoin wallet (to store bitcoin) is created, user receive a **public key** and a **private key**.

Public keys and private keys are a set of long numbers and letters; *it includes username and password*. Both are **very important** for truly understanding how does Bitcoin work.

People need receivers **public key** if they want to send money to someone. Because it is just a set of numbers and digits, nobody needs to know his name or email address, etc. *This makes Bitcoin users anonymous.*



Bitcoin transactions are grouped together and stored in *blocks*. These blocks are linked back to one another in a series. This is why it is called *a blockchain*.

Each transaction in the block has **a public key** written on it. If someone had a bitcoin, there will be a private key written on it. Because each block is connected to the block before it, no Bitcoin can be spent twice.

If someone tries to change the transaction data in one of the blocks, it will only change it on their own version, just like a Microsoft Word document that's stored on personal computer.

This is one of the key elements of how does Bitcoin work. To make the change go onto the shared database so that it's on everybody's version, they will need to control **51% of the computers in the network**.

If someone controls 51% of computer network, if someone hacked 51% of the computers in the network (*also known as nodes*), there is another layer of security that gets in their way.

To add new blocks to the blockchain, they must be **mined**. This process is called mining because the nodes that do it are rewarded with Bitcoin — like gold miners being rewarded with gold.

In mining, the nodes must process Bitcoin transactions and verify that they are real. To do this, they must solve a mathematical problem. When the problem is solved, the block of transactions is verified, and a new block is created. Each block has a new problem and a new solution for miners to find. The first node to solve this problem gets new Bitcoins. Mining uses a lot of electricity, so the miners need to be rewarded.

Bitcoin price trend:

Bitcoin has a speedy growth in its introductory years, after some years there is a decrease in its growth rate. In crypto winter wave a downfall is found in it.

Findings:

1. **Bitcoin is introduced by Nakamoto. What is Nakamoto? It is unknown. Bitcoin is wandering aimlessly in money market like orphan child.**
2. **Bitcoin concept is in its primary stage with limited quantity. Global market is humongous. It is a great challenge to spread Bitcoin in all countries.**
3. **Bitcoin is in market with developing shape. While market and economy need developed model.**
4. **Bitcoin depends on decentralised network while money and market are operated by centralized network. It is a great challenge to make a bridge between two opposite axes.**
5. **Bitcoin concept depends on liberalised infrastructure. It pays little heed to government, regulations and restrictions. But investors and participants need guidance and rules at every step. Lack of sufficient rules and regulations related to Bitcoin create fears among people and investors.**
6. **Bitcoin is global currency of coming future tunes with concept of global government.**

Suggestions:

1. **Bitcoin is a new form of currency. A global awareness campaign be initiated.**
2. **The framework of Bitcoin must be enlarged according to the size of global market.**
3. **There are many misconceptions and fears regarding Bitcoin. Suitable clarification must be produced.**
4. **There are many continents and countries in the world with distinctive developmental and monetary characteristics. According to these expectations Bitcoin concept should be modified.**
5. **More developed, specialized, regularized global version of Bitcoin must be produced under the supervision of United Nation like institution.**
6. **Bitcoin concept must be improved in light of global government of coming future.**

REFERENCE:

*1 Nakamoto Satoshi, A peer to peer electronic Cash system, www.bitcoin.org

*2 Bitcoin project. “Bitcoin is 10 years old!”

*3 Will Binns, Bitcoin.org Site Blog, 15August 2018

*4 Page web, BYTWORK.COM

*5 PwC. (2015, August). Money is no object: Understanding the evolving cryptocurrency market. Retrieved from PricewaterhouseCoopers, LLP. Financial Services Website: https://www.pwc.com/us/en/financial-services/publications/assets/pwc-cryptocurrency-evolution.pdf

*6 Perez, Y. B. (2015, October 24). European Exchanges React to Bitcoin VAT Exemption. Retrieved from Coindesk Website: http://www.coindesk.com/european-exchanges-react-to-bitcoin-vat-exemption/

*7 Desjardins, J. (2016, January 5). It's Official: Bitcoin was the Top Performing Currency of 2015. Retrieved from The Money Project Website: http://money.visualcapitalist.com/its-official-bitcoin-was-the-top- performing-currency-of-2015/

*8 Hileman, G. (2016, January 28). State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass. Retrieved from Coindesk Website: http://www.coindesk.com/state-of-bitcoin-blockchain-2016/

*9 Heston T.F., "Introductory chapter: Making health care smart", *eHealth—Making Health Care Smarter*, 2018.