IJCSMA

Dr. Latika Kharb *et al*, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 11, November- 2017, pg. 1-8 **ISSN: 2321-8363**
Impact Factor: 4.123

BITCOINS- FUTURE CURRENCY

Dr. Latika Kharb[1], Prachi Sharma[2], Anikesh Mourya[3]

[1] *Associate Professor, latika.kharb@jimsindia.org*

[2] *Student, prachi.sharma01sep@gmail.com*

[3] *Student, anikeshmourya100@gmail.com*

Jagan Institute of Management Studies (JIMS), Delhi, India

Abstract

Bitcoin (BTC) is a worldwide cryptocurrency and digital payment system called the first decentralized digital currency, as the system works without a central repository or single administrator. Bitcoins are based on an open-source cryptographic protocol that is independent of any central authority like a Central Reserve Bank or another administrative institution. Bitcoins are created and administrated decentralized within a computer based network. The bitcoins can be used for many transactions in devices like mobile phones, tablets, personal computers and so on. Bitcoins also has economic benefits. Use of bitcoins is cheaper compared to credit card fees. This is also the reason why many merchants and traders have started using bitcoins for money.

In this paper, it has been summarized that what is bitcoin, how it evolved, its designing that includes the concept of blockchain, economy, in art, media and entertainment, how it is different from other cryptocurrencies and then finally the conclusion.

Keywords: *Introduction to bitcoins, History, Nature, Blockchain*

1. Introduction

In the beginning of human kind: food was traded for livestock, and livestock for resources like wood, or maize. It progressed to precious metal, such as silver and gold and constantly evolving our financial states.

There are various innovative money payment systems in the market today, many of which are built on platforms like the mobile phone, the Internet, and the digital storage card. These alternative payment systems have seen encouraging or even continued growth, from the likes of PayPal, Apple Pay, Google Wallet, Alipay, Tenpay, Venmo, M-Pesa, BitPay, Moven, BitPesa, PayLah!, Dash, FAST, Transferwise, and others.

Beyond payment systems that are based on fiat currency, the growing use of digital currency allows for faster, more flexible, and more innovative payments and ways in financing goods and services. One digital currency, however, stands out among the rest.
Bitcoin is one of the most well-known digital currencies today. To be specific, Bitcoin is a cryptocurrency, which is a subset of what is generally known as a digital currency. It is a new form of currency which has been constantly evolving over the past decade, developed by an unknown person and maintained by a collective group of the brightest minds in technology. It’s a new form of money that is created and held digitally, and the most important part, of course, is that no government owns it, or decides its value - the community does.

2. History

According to legend, Satoshi Nakamoto began working on the Bitcoin concept in 2007. While he is on record as living in Japan, it is speculated that Nakamoto may be a collective pseudonym for more than one person.

Fast Company recently published an article suggesting that Satoshi Nakamoto could be a group of people, including Neal King, Vladimir Oksman, and Charles Bry. Apparently, these three-people filed for a patent related to secure communication just two months *prior* to the purchase of the Bitcoin.org domain. Perhaps it's a coincidence; perhaps it's not.

Some Important Dates:

- **On August 18, 2008,** Bitcoin.org is registered! The domain was registered at anonymousspeech.com, a site that allows users to anonymously register domain names and currently accepts Bitcoins.
- **On October 31, 2008,** Nakamoto publishes a design paper through a metzdowd.com cryptography mailing list that describes the Bitcoin currency and solves the problem of double spending so as to prevent the currency from being copied.
- **On November 9, 2008,** the Bitcoin project is registered on SourceForge.net, SourceForge.net a community collaboration website focused on the development and distribution of open source software.
- **On January 9, 2009,** the first version (version 0.1) of Bitcoin is announced. It includes a Bitcoin generation system that would create a total of 21 million Bitcoins through the year 2040 and shortly thereafter, Bitcoin mining begins.
- **On October 5, 2009,** Bitcoin receives an equivalent value in traditional currencies. The New Liberty Standard established the value of a bitcoin at $1 = 1,309BTC. The equation was derived so as to include the cost of electricity to run the computer that created the bitcoins in the first place.
- **On May 22, 2010,** A programmer living in Florida named Laslo Hanyecz sends 10,000BTC to a volunteer in England, who spent about $25 to order Hanyecz a pizza from Papa John's. In today's date the value of that pizza will be in billions dollar and stands as a major milestone in bitcoin's history.
- **In January 2011,** The Silk Road, an illicit drugs marketplace is established, using Bitcoins as an untraceable way to buy and sell drugs online.
- **On February 9, 2011,** Bitcoin touches US$1.00/BTC at MtGox, reaches parity with the US dollar for the first time. By June Bitcoins is worth $31 giving the currency a market cap of $206 million.
- **On May 2, 2013,** the first Bitcoin ATM in the world is debuted in San Diego California.
- **In January 2014,** Bitcoins custodians Elliptic launch the world's first insured bitcoin storage service for institutional clients.
- **In June 2014,** The US government auctions off more than 29,000 bitcoins seized from the Silk Road, the illegal online marketplace. From this point onwards, bitcoin can no longer be considered as a currency for criminals. The use of the bitcoin blockchain means that identity of the users can often be established.
- **In December 2014, Tech giants Microsoft begins** accepting the bitcoins payments. Bitcoins can be used to buy content such as games and videos on the Xbox games consoles, add apps and services to windows phones or to buy Microsoft Software.

3. The Nature of Cryptocurrency

Cryptocurrency in its purest form is a peer-to-peer version of electronic cash. It allows online payments to be sent directly from one party to another without going through a financial institution. The network time-stamps transactions using cryptographic proof of work. The proof-of-work Bitcoin protocol is basically a contest for decoding and an incentive to reward those who participate. For Bitcoin, first participant to crack the code will be rewarded with the newly created coins. This contest will form a record of the transactions that cannot be changed without redoing the proof of work. Cryptocurrency is a subset of digital currency. Examples of the many digital currencies are air miles issued by airlines, game tokens for computer games and online casinos, Brixton Pound to be spent only in the Brixton local community in the Greater London area, and many other forms that can be exchanged for virtual and physical objects in a closed system and, in the case of an open system, exchanged for fiat currency.

4. What makes bitcoins different from other cryptocurrencies?

Bitcoin has a proven usage case as a store of value. It's instructive that most coins try to carve out some differentiation based on much smaller use cases, such as prediction markets, buying things completely anonymously or adding a decentralized name server.

Bitcoin has a large lead as a store of value over every altcoin in having existed 8 years without failure. The security of Bitcoin has been proven far more than its much younger counterparts with usage by almost every metric exceeding that of altcoins.

Further, Bitcoin is more accessible, with more exchanges, more merchants, more software and more hardware that support it. Bitcoin is far more liquid, with much larger volumes than every altcoin. Bitcoin has the largest developer ecosystem with more software and more implementations than any altcoin. Bitcoin has the most entrepreneurs creating companies around it with a lot of intellect, dedication and creativity going toward making it more useful.

When you compete with Bitcoin, not only are you competing with its much larger user base, development team and mining operation, but you're also competing against the very large ecosystem of startups, open source projects and entrepreneurs.

5. Blockchain

Before understanding Bitcoins, it is important to understand what is blockchain and how it is worked.

One can think about the blockchain as a ledger of transactions. A physical ledger is typically maintained by a centralized authority, not by market participants. The blockchain, however, is a distributed ledger which resides on each participant's device. Each individual copy is updated in real time whenever a transaction is completed. The device of each participant or user is usually referred to as a 'node,' which forms part of a network of nodes.

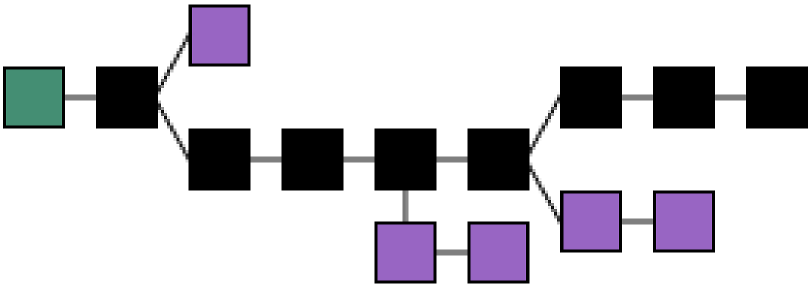

Figure 1: Example of blocks that are linked together using cryptography

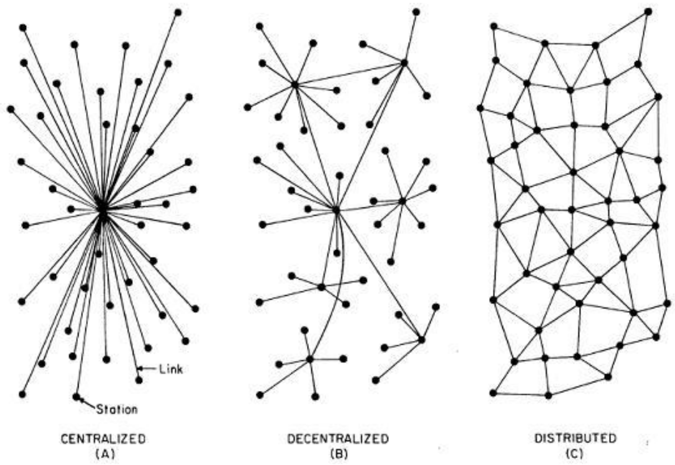

Figure 2: Different type of systems (Blockchain is distributed)

The blockchain is unique because every node must authenticate every transaction in the network. Therefore, when a new node joins the network, the entire record of transactions is downloaded onto its system (for Bitcoin, this process now takes over 24 hours). From then on, it will join the other nodes in updating the ledger as and when new transactions are authenticated. The process of authentication is based on advanced cryptography, and is widely considered to be secure in and of itself. Hence, participants do not need to rely on a third party for transparency and authenticity. The blockchain ensures the transparency and integrity of transactions purely through mathematics, and not trust.

The type of transaction varies depending on the application of blockchain technology. In Bitcoin, for instance, each transaction is a transfer of a certain value of Bitcoin between participants, and every transaction is recorded on the Bitcoin blockchain. However, the transactions could also be something like real estate title transfers.

Suppose X sends 5 units of currency to Y, it sends a transaction message, represented in computer code, to the network. To become an accepted transaction recorded on the blockchain in this case, for 5 units to be considered transferred, this transaction message must be authenticated by every node in the network.

The authentication is done on the basis of the digital signature accompanying the message. Every node possesses a public and private cryptographic key. The public key is akin to a mailing address, to enable other nodes to communicate with it (send money, sign contracts etc.). The private key is akin to a secure password that only its holder knows. Whenever a node sends out a transaction message, a digital signature is generated using its private key and the message. The digital signature enables other nodes in the network to verify that the sender is really the holder of a given private key. Digital signatures hence enable the network to verify the authenticity of messages, and prevent fraud and impersonation.

Once the digital signature of a transaction is authenticated, it gets pooled with other authenticated transactions into a ‘block.’ After the first block, a series or ‘chain’ of blocks gets formed, hence leading to the term ‘blockchain.’ This is where a second level of cryptography comes in.

Every block is encrypted using a cryptographic hash function. A block can only be read and made sense of after is decrypted. Because of the strength of the cryptographic hash function involved, a great deal of computing power is required for decryption. Every node in the network participates to work towards decrypting each block. This process is known as 'mining' and nodes doing this are called 'miners'. Incidentally, miners in the Bitcoin blockchain are rewarded for their work with Bitcoin value.

The "work" involved in mining is not manual human work, and is performed by each node's device without human intervention. In simple terms, it is large-scale trial-and-error guesswork until the correct mathematical answer is reached. Therefore, like with digital signatures, the order of transactions is decided by mathematics and not trust or third-party discretion.

Once a block is authenticated, the ledger in all nodes is updated with the new transactions in that block, and so forth.

The blockchain is likely best used when:

1. There are a series of transactions / events.
2. They need to be recorded.
3. They need to be verified.

   Verification occurs with respect to:

   a. The integrity of the information, and
   b. The integrity of the order of events.
4. There are several participants in the system.
5. Transparency is important.
6. Decentralization is important.
7. Permanence is important.

5.1 Bitcoins Creation:

New bitcoins are generated by a competitive and decentralized process called "mining". This process involves that individuals are rewarded by the network for their services. Bitcoin miners are processing transactions and securing the network using specialized hardware and are collecting new bitcoins in exchange.

The Bitcoin protocol is designed in such a way that new bitcoins are created at a fixed rate. This makes Bitcoin mining a very competitive business. When more miners join the network, it becomes increasingly difficult to make a profit and miners must seek efficiency to cut their operating costs. No central authority or developer has any power to control or manipulate the system to increase their profits. Every Bitcoin node in the world will reject anything that does not comply with the rules it expects the system to follow.

Bitcoins are created at a decreasing and predictable rate. The number of new bitcoins created each year is automatically halved over time until bitcoin issuance halts completely with a total of 21 million bitcoins in existence. At this point, Bitcoin miners will probably be supported exclusively by numerous small transaction fees.

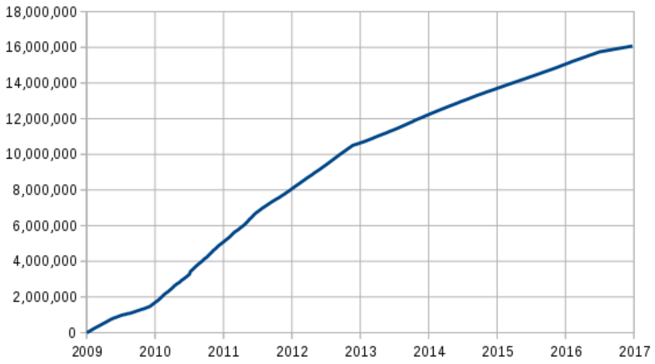

Figure 3: Total bitcoins in circulation

5.2 Bitcoin Mining:

Bitcoin is often compared with gold, and one of the chief factors of similarity it the way they're both obtained. Similarly, to gold, new Bitcoins are created via the process called "mining."

Bitcoin mining is the process of adding records of a new transaction to the Blockchain - the public ledger of all transactions that have ever taken place in the Bitcoin network. New transactions are added in batches called "blocks" roughly every 10 minutes, hence the name Blockchain (shown in above diagram). The ledger is needed for the nodes of the Bitcoin network to always be able to confirm valid transactions.

In order to become a Bitcoin miner, a person first needs a computer and mining software - like the GUIMiner. This program uses the computer's resources to perform complex mathematical calculations. When any one miner succeeds in solving their math problem, they get to create a new block and receive a certain number of Bitcoins as a reward, known as "the block reward."

Every 210,000 blocks, or, roughly, every four years, the block reward is halved. It started at 50 Bitcoin per block in 2009, and in 2014 it was halved to 25 Bitcoins per block.

5.3 Hashing:

Bitcoin uses a cryptographic hash function SHA-256 for encryption. This algorithm allows you to take data of any size and turn it into a string of a specific, predefined size. The resulting string is called a "hash," and the process of applying the hash function to random inputs is called "hashing."

It's impossible to predict what the hash of any one input will be until you actually calculate it. The goal of the miners is to keep feeding the hash function with different inputs until they get a specific hash value which is below a certain threshold, which is called the "difficulty" of network.

The difficulty is automatically adjusted every 2016 blocks - or, roughly, every 14 days - in accordance with the growing or shrinking combined computational power of the network.

If the network became more powerful over the last 2016 blocks, then the difficulty value is decreased to make it harder to find a valid hash and vice versa.

Considering the immense computational power that the Bitcoin network currently employs, it takes trillions of computer-generated guesses from all over the world until the right hash value is found by someone. And if you are the first to do it - congrats! You have just mined a block and got a reward of Bitcoins.

6. Economics

Bitcoins have three useful qualities in a currency, according to *The Economist* in January 2015: they are "hard to earn, limited in supply and easy to verify". Economists define money as a store of value, a medium of exchange, and a unit of account and agree that bitcoin has some way to go to meet all these criteria. It does best as a medium of exchange; as of February 2015 the number of merchants accepting bitcoin had passed 100,000. As of March 2014, the bitcoin market suffered from volatility, limiting the ability of bitcoin to act as a stable store of value, and retailers accepting bitcoin use other currencies as their principal unit of account.

6.1 General use

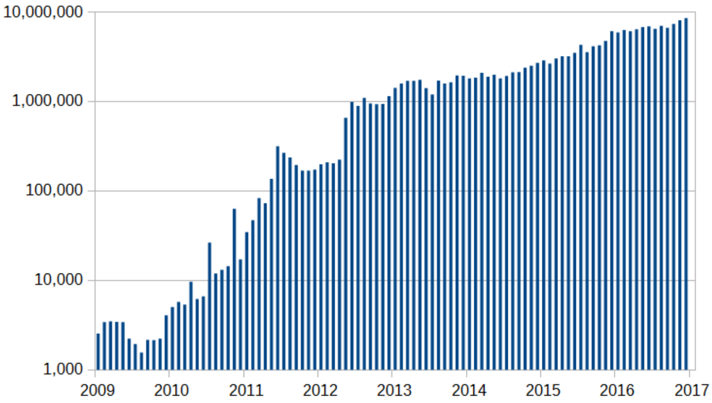

Figure 4: Graph showing the number of bitcoins transactions per month

According to research produced by Cambridge University, there were between 2.9 million and 5.8 million unique users using a cryptocurrency wallet, as of 2017, most of them using bitcoin. The number of users has grown significantly since 2013, when there were 300,000 to 1.3 million users.

Acceptance by merchants

In 2015, the number of merchants accepting bitcoin exceeded 100,000. Instead of 2–3% typically imposed by credit card processors, merchants accepting bitcoins often pay fees under 2%, down to 0%. Firms that accepted payments in bitcoin as of December 2014 included PayPal, Microsoft, Dell, and Newegg.

7. In art, entertainment and media

7.1 Films

The documentary film, *The Rise and Rise of Bitcoin* (late 2014), features interviews with people who use bitcoin, such as a computer programmer and a drug dealer.

7.2 Music

Several lighthearted songs celebrating bitcoin have been released.

7.3 Literature

In Charles Stross' science fiction novel, *Neptune's Brood* (2013), a modification of bitcoin is used as the universal interstellar payment system.

8. Conclusion

Delivering a high quality reliable product is the main focus in any software development as digital data become more prevalent, users try to secure their information with highly encrypted passwords and ID methods. Many people see similarities between the growth of the Internet and the growth of cryptocurrency and postulate that cryptocurrency is going to see exponential growth like the Internet. However, from the business perspective, the growth of the Internet has more to do with e-commerce and less to do with finance. On the other hand, with cryptocurrency, for once in the history of mankind, technology is playing a leading role in finance.

In future, one should expect a bank to be a digital or technologically savvy bank. The disruptive force has now arrived at the door step of finance and the blockchain technology is one of the solutions.

References

[1] Michael PAETAU, Bitcoin: Network Based Currency and Its Self-Organizing Emergency, 823.2

[2] Kharb L, Biometric Personal Data Security Systems: Trustworthy Yet? International Journal of Recent Engineering Research and Development (IJRERD) Volume No. 01 – Issue No. 06, ISSN: 2455-8761 www.ijrerd.com, PP. 01-08

[3] David Lee Kuo Chuen, Handbook of digital currency

[4] Kharb L, Automated Deployment of Software Containers Using Dockers International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 4, Issue 10, October (2016)

[5] https://en.wikipedia.org/wiki/Bitcoin

A Brief Author Biography

Dr. Latika Kharb – Dr. Latika Kharb is currently working as Associate Professor in JIMS, Rohini, New Delhi, INDIA. She has got work experience of more than 14 years in teaching. She is a Technical reviewer/ Editor/Board of Refree (BoR) / Chair person, member of Board of Referees/ Reviewer for numerous International Journals She has written more than 60 Research Publications besides the review articles in various International & National Conferences/Workshops/ Training Programs. She has got Nine Professional International Awards for her Academic Excellence. Her research areas include: Software Metrics, Software Testing, Artificial Intelligence, Cyber Laws, and Bioinformatics to Access Biological Database & Gene Identification, Mobile Computing, Computer Forensic Science, Nanotechnology, Cyber Medicine & Dentistry, Autonomic Software Systems and many more.

Prachi Sharma – Graduated in B.Sc(H) Computer Science in 2014-2017 from Delhi University, New Delhi, India. Currently doing Master of Computer Applications from Guru Gobind Singh Indraprastha University, New Delhi, India. Interested research areas are cryptocurrencies, new gadgets and upcoming technology. Interested in website designing, programming and blogging. Also interested in listening to music.

Anikesh Mourya – Graduated in B.C.A from Guru Gobind Singh Indraprastha University, New Delhi, India. Currently doing Master of Computer Applications from Guru Gobind Singh Indraprastha University, New Delhi, India. Interested in gaming and curious about knowing different cryptocurrencies.