3rd International Conference on Computing: Communication, Networks and Security (IC3NS-2018) ISSN: 2454-4248
Volume: 4 Issue: 3 14 – 16

Bitcoin and Blockchain: A peer to peer electronic cash system

Riya Aggarwal
Mody University of Science and Technology
Riyagg23@gamil.com

Abstract. Digital currency is a progressive technology that permits institutions or people to switch finances right away and securely in a decentralized way. The greatest benefit of digital currency is that it cannot be counterfeited and transactions cannot be reversed arbitrarily by the sender. Blockchain was introduced in 2009 and it is revolutionizing the digital world by bringing a new perspective to security and resiliency of system. When transactions are done, they are verified by network nodes through the use of cryptography and they are recorded in a public distributed ledger called a blockchain. Cryptography is a technique of storing and sending data in a specific form in order that unauthorized users aren't able to study it. Blocks in blockchain are linked and secured through cryptography. Blocks in blockchain are linked and secured through cryptography. Bitcoin is a cryptocurrency and it is created as a reward for a process known as mining. Future of cryptocurrency means permitting you to have final manipulation over your money, who you send it to.

Keywords: cryptography, cryptocurrency, bitcoin, blockchain, mining

*****

1 Introduction

Bitcoin is a distributed electronic money framework. It is a digital currency also called as the cryptocurrency. Transaction of bitcoins takes place between the users directly i.e. there is a decentralized system. The decentralized system means having a system that works without a central bank or single administrator. All transactions are recorded in a public distributed ledger called BLOCKCHAIN.

Blockchains works on a distributed computing system. Blockchain contains a list of records, called blocks. These blocks are linked and secured through cryptography.

The blockchain is a very powerful technology that enables bitcoins and other virtual currencies like litecoin, dogecoin to be open securely and pseudonymously.

This paper presents a survey on the bitcoin and blockchain, why the concept of digital currency is far better than the Indian currency (INR). Whatever remains of this paper is sorted out as follows.Section 2 presents data on cryptography and how it ensures security of bitcoins. Section III discusses about amenities of bitcoins. Section IV concludes the paper by discussing challenges faced by bitcoins globally. Finally, Section V will display the references used to get this paper ready.

The bitcoin

Bitcoin is a digital currency, also called cryptocurrency. Instead of minting coins or printing bank notes, a registration number is provided to each coin and a record of people owning them is maintained. People pay each other by transferring the registration numbers online. Bitcoins were developed by an obscure gathering of individuals under the name of SANTOSHI NAKAHOTO. Initially, they were first released on 9th Jan 2009. Peer – to – peer network is followed i.e. peers (nodes) are interconnected and they share resources amongst each other without the interference of centralized administrator. It is valued at 6500USD and according to INR 450000. Bitcoins are made as an acclaim for a procedure alluded to as mining.

Bitcoin mining is a procedure through which exchanges are confirmed and added to the blockchain and through this process, new bitcoins are released.

Indian government decides when to print paper money i.e. there is a central government who takes decisions. In contrast, with bitcoins, mmineworkers utilize extraordinary programming to take care of numerical issues and are issued a specific number of bitcoins in return. This gives an incentive for more people to mine and thus proves to be a smart way of issuing currency.

Creators Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua

A. Kroll and Edward W Felten recognized are 3 parts of bitcoin's outline that can be broke down independently. They are (1) exchanges (2) accord and mining (3) the distributed correspondence arrange.

The Blockchain

The blockchain is not a household catch word like cloud computing, internet of things, big data.

It is not an innovation that you can feel or touch like smart phones. Think of blockchain as a historic fabric beneath recording everything that happens like the exchange of value, services, and goods; digital transaction or private data. Then blockchain stitches all data in form of encrypted blocks and these blocks can never be modified. The blockchain is an open record that records bitcoin exchanges.

The blockchain is a constantly developing rundown of records, called pieces, which are connected and secured through cryptography. Each piece regularly contains 3 components (1) timestamp (2) cryptographic hash of previous block (3) transaction data. Timestamping is a process in which a record of creation time and modification time of a document is maintained. Security here means that no one, not even owner of document., is allowed to make changes once it has been recorded. A cryptographic hash characteristic is a special elegance of hash characteristic that has some positive properties which make it appropriate to be used in cryptography. It miles a one-way hash feature that maps statistics of arbitrary length to a piece string of fixed length. The input information is called message and output information is called digest.

Fig. 1. Block details

There are several issues with current banking system like high transaction fees, double spending, net frauds and account hacking. Blockchain solves this conglomerated problem. Blockchain follows decentralized system i.e. everyone who is part of a system is equally responsible for growth and downfall of the system. Everyone who is involved with the system holds some power. Leverage of utilizing blockchain is that it expels the normal for interminable reproducibility from a computerized resource. It gives a blessing that every unit of significant worth is exchanged once just, tackling the long-standing issue of twofold spending. Blockchain works as follows :-

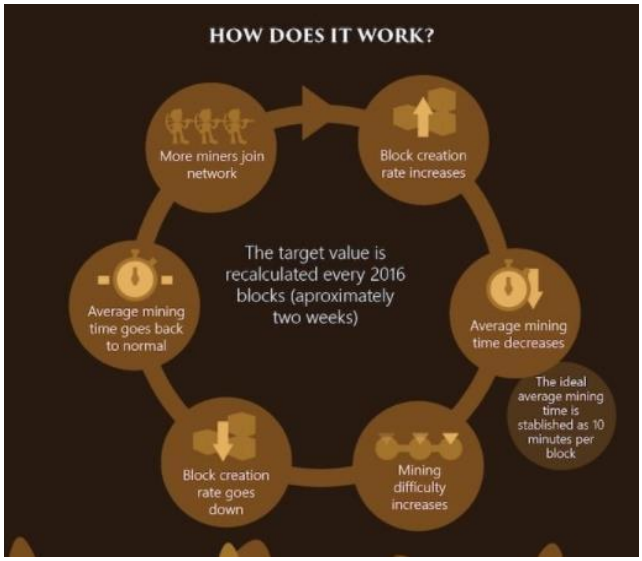

Fig. 2. Working of blockchain

Initial release – 0.1.0 / 9 Jan. 2009
Latest release – 0.15.1 / 11 Nov 2017

Studies delivered through the college of Cambridge assesses that in 2017, there are 2.9 to 5.8 million particular customers the usage of a cryptocurrency pockets.

. **Fig. 3. Blockchain wallet activity**

2 Cryptography

Cryptography is a Greek phrase and is coined by way of 2 phrases 'Krypto' that means hidden and 'graphene' which means writing.

People from ages had two inborn need i.e. to impart and share data and to convey specifically. These two needs offered ascend to the craft of coding the messages such that exclusive the planned individuals could approach the data

Safety services of cryptography

(1) **Confidentiality**- it is a safety carrier that maintains the statistics from an unauthorized character.

(2) **Data Respectability**- The data can likewise get changed by an unapproved element purposefully or by possibility. Honesty transporter affirms that whether records is in place or not.

(3) **Validation**- It affirms to the beneficiary that the records procured has been sent least difficult by utilizing a recognized and checked sender.

3 Bitcoin- Good or Bad?

Amenities of bitcoins

1) Bitcoin transactions are completely confidential unlike in payment through banks where the transactions can be tracked.

2) Paying through bitcoins provides absolute freedom. They can be sent to any person in any part of the world, no intermediate medium is required. No payment limit.

3) Paying through bitcoins is almost free. No additional amount is charged for transfer of bitcoins. Only if a person wants that his or her transaction should be processed very fast then only a amount which is very less is charged. Bitcoin transactions are very fast if compared to banking channels.

4) Most online purchases today are made via debit cards or credit cards requiring users to enter all their confidential details. However, for bitcoin transaction you only need to enter your private and public key.

4 Obstacles faced by bitcoins

Obstacles to bitcoin's mainstream adoption.

1) The buying power of bitcoin could climb or fall significantly. Most people don’t want to face this currency risks. Before the adoption of bitcoin as the basic currency, there should be stability in prices of bitcoins.
2) Bitcoins are still not user-friendly because to buy or sell bitcoins,he or she needs to open a record at a bitcoin trade.
3) Understanding the concept of bitcoin according to user's point of view is a bit complicated task.
4) There is no third party involved in transactions of bitcoin to keep track on transactions. So, many users buy illegal items. So, bitcoins became a characteristic decision for individuals who needed to purchase drugs, unlawful weapons.
5) There are numerous expense related issues like If you purchase bitcoin and after that offer it for more than you paid, you'll have to report the distinction on your charges.

Legal obstacles on the block chain

Some countries are constraining the use of blockchains because of its untraceable nature and its notoriety for being the cash of decision for criminal exercises like psychological warfare or the medication exchange as the fundamental reasons why.

Vietnam is one of the current nations to ban bitcoin exchanges. State bank of Vietnam declared all crypto currencies an illegal form of transaction and imposed fines on people who were found indulged in exchange of crypto currencies.

Bangladesh, Bolivia, Ecuador and Kyrgyzstan have restricted the utilization of bitcoin also.

It's difficult to state for certain what's on the horizon for bitcoin. Lawful rules and strategies may likewise make bitcoin-supported exchanges troublesome in a few nations. However the greater businesses include bitcoin as a legitimate price approach, the less difficult it will likely be for governments to just acknowledge digital money assume thing aside from a way to bypass banks and fund unlawful activities.

5 References

[1]. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
[2]. M. Palatinus. Stratum mining protocol - asic ready. https://mining.bitcoin.cz/stratum-mining, September 2012.
[3]. N. van Saberhagen. Cryptonote v 2.0. https://cryptonote.org/whitepaper.pdf , 2013
[4]. F. Voight. p2pool: Decentralized, dos-resistant, hop-proof pool. https://bitcointalk.org/index.php?topic=18313.0, June 2011
[5]. https://blockchain.info/charts
[6]. feature/blockchain-the-invisible-technology-thats-changing-the-world