A DESCRIPTIVE STUDY ON BLOCKCHAIN TECHNOLOGY

Mr. Nanduri Anil Kumar,
Associate Professor,
Department of Commerce,
Avinash College of Commerce (Degree),
Kukatpally,
Hyderabad.

T. Subhashini
Student,
B.Com II Year (Honours),
Avinash College of Commerce (Degree),
Kukatpally
Hyderabad.

ABSTRACT

The research paper articulates about how blockchain technology is originated, the detailed process of blockchain, advantages and disadvantages of blockchain technology, how the blockchain technology works in Bitcoin (a type of cryptocurrency), how it is helpful for developing nations who do not have same financial structure, how it is preventing tampering, and protecting the participating parties safely without any intermediaries like middle men and traditional banking problems. The paper also discusses about how it is creating smart contracts automatically between the parties and the relation between the distributed ledger of blockchain and non- relational database. The paper also talks how the parties in transaction process are awarded with bitcoin during the dealings, the speed and ease in peer network , the decentralization of bitcoin from the government control.

KEYWORDS*: Blockchain, primary key, private. key, distributed ledger, Bitcoin.*

INTRODUCTION:

Blockchain technology was originally introduced by Santoshi Nakamoto (An anonymous person or an Organisation) foe bitcoin(cryptocurrency) in 2008. In blockchain the public key is used by a person/company who intends to spend or receive cryptocurrency. The private key is a password to access a cryptocurrency. The distributed ledger used in blockchain is many computers among the peer network each have copies of the portions of the ledger. A hash code is a part of the date and time of the transaction and the public keys of the parties. Mining means verifying cryptocurrency transaction by solving mathematical equations in order to prove the likelihood of occurrence. When blocks are mined successfully, it confirms a set of transactions and rewards the miner with cryptocurrency. Block is an encoded record of transaction. Blockchain is a string of blocks showing all transactions for the service using blockchain, usually Bitcoin.

SCOPE OF THE STUDY:

The study aims to evaluate how safest the blockchain technology is and how it works in bitcoin.

OBJECTIVES OF STUDY:

- Study and understanding of blockchain technology process, advantages and disadvantages of blockchain.

REVIEW OF LITERATURE:

P.S. Aithal, Architha Aithal &Edwin Dias(2021) stated about the current status and future research opportunities and what are the benefits and threats of blockchain technology in healthcare

Shwetha Singh, Anjali Sharma, Dr. Prateek Jain (2018) stated how bitcoin is changing the world how blockchain technology helpful in different sectors of the economy.

BLOCKCHAIN PROCESS:

Blockchain is a control system originally designed to govern the creation and distribution of bitcoin. Bitcoin is a currency that exists only in electronic form, called a cryptocurrency. Bitcoin must be "minded" in order to confirm transactions. Mining cryptocurrencies involves a person or group of people performing cryptography, which is cracking of complex mathematical equations. Through cryptography, blocks of precise number of dealings are committed at a time. The reward for solving the equation is both the receipts of Bitcoin and the validation of a new block of transactions.

A chain of blocks is attached to every Bitcoin. Each blockchain chain contains a hash code or digital fingerprint (just like Aadhar card) for each transaction as well as the hash codes for preceding and following transactions. Altering a transaction will alter the hash codes , making that hash code out of sync with other blocks in the chain. Blockchain uses distributed ledger rather than the normal accounting ledger where the ledger is related to the single company. All blockchain parties maintain a copy of entire history of all block chain transactions. When a person holding bitcoin (user) wishes to pay for a transaction with bitcoin a new transaction is requested. The user's computer storage that are involved with bitcoin which is then compared against all other copies of the blockchain for the bitcoin in the peer network. Any variances in hash codes between the user's blockchain and the other computers in the distributed ledger amount to any type of tampering. If any tampering is identified, the transaction is refused. The user's version of the blockchain is then resynchronized to match the peer network's version undoing the false alteration.

A person wants to buy a rare collection from someone in another country. Instead of using national currencies and paying exchange rate fees, the buyer agrees on a price in Bitcoin. The buyer plugs in a flash drive containing the stored record of her bitcoin and authorizes the transfer. The transaction takes about five minutes while the blockchain for the transferred Bitcoin is checked against the other copies in the distributed ledger. This validation process returns a discrepancy. Even other version of the record for that blockchain includes a transaction where this Bitcoin was already spent by the buyer, except for the version which resides on the buyer's flash drive. The blockchain control system decides that that the many records are correct, and the single discrepancy is wrong and corrects the buyer's data by making it align with the distributed ledger. It is presumed that the buyer altered or sheltered this record and no longer owns the Bitcoin in question, and the blockchain control system has reimposed that reality. The transferred Bitcoins are available for the buyer to use to pay the seller.

Blockchain technology was developed to prevent Bitcoin from being replicated and to limit its initial creation so that there is only finite number of Bitcoins. because electronic data can be easily copied and altered, the accounting system governing it must prevent the copying or alteration of the cryptocurrency; otherwise the currency may become worthless through counterfeiting. The value of blockchain is its resistance to alteration, multiparty transaction validation, and decentralized nature. Alteration is difficult because each block adds to all preceding blocks, enabling everyone to. view all blocks in the chain to the starting of the entire chain. This serves as a form of audit trail. The decentralization of Bitcoin makes it detached from government control.

The complicated mathematical processing mechanism for creating new blocks includes the public key from the receiver and the private key of the giver. This means the blockchain depends on a password to authenticate. Human beings are bad at password security and also the cybersecurity. This potential can help developing nations, which do not have the same financial infrastructure as developed nations, join the marketplace. Unfortunately, blockchain technology also aids criminals and terrorists to circumvent international laws and sanctions.

If people use companies to facilitate Bitcoin Exchanges, those companies have databases that match customers with their keys. If the exchange company suffers a data breach, the hackers will have all the keys needed to write new blocks, and the distributed ledger will view these transactions as valid. Once this happens, blockchain's resistance to tampering now makes it harder to restore bitcoin to the original owners.

Blockchain can also be used to create smart contracts. Smart contracts are those where the terms can be agreed on, executed, and verified automatically. Part of the function of notaries, lawyers, and the courts in contract law is to record that a service is complete, when payment is due, and when the payment has been received. If both the service and the payment can be observed by the blockchain peer network, then the payment can be directed by an automated process without the need to pay for the intermediary to officiate. The use of smart contracts does not replace the function of legal practitioner, but it augments, and in some cases expedites, the processing of legal documents.

A person wishes to buy an item and have it delivered to his home. A smart contract can be set up such that the buyer authorizes a payment (via Paypal, Bitcoin or electronic transfer) to anyone who delivers the item for the requested price. A fast delivery person arrives at the destination where a camera connected to the internet have the object - recognition software and can verify that the item has been delivered. The delivery fulfilment is recorded in the smart contracts blockchain peer network. Then funds are automatically transferred to the delivery person's account because the terms of the contract have been fulfilled.

The distributed ledger of blockchain is similar in architecture to nonrelational databases, a newer technology which enables faster access to a database by multiple, widely dispersed users. Blockchain could serve as backup data stored outside the database. It could represent a means to increase the speed of nonrelational databases by increasing the ability to roll back

invalid changes after beginning them. This would also promote the integrity of relational databases.

Blockchain technology is able to fill gaps in current financial technologies and able to solve traditional banking problems by being a peer technology. It also removes middle men. Bitcoins are solely positioned to solve to occur quickly in international transactions in response to an emergency thanks to speed and ease of transactions in the peer- to peer- network.

FINDINGS AND CONCLUSION:

Blockchain technology is a powerful but complex technology. It involves the algorithms those are used in blockchain applications that are used to make transactions more transparent and secure. It can take the politics out of economics by allowing buyers and sellers anywhere in the world to do the business. It doesn't allow tampering of transactions. It also removes the bank as intermediary for transferring of money. Bitcoin is safe heaven for investors because it does not lose any value due to inflation. People generally trust Bitcoin if it is legally binding, but it is not accepted by most of the nations. Bitcoin encourages illegal activities. Blockchain technology aids criminals and terrorists to circumvent international laws and sanctions. So, there are both opportunities and treats for blockchain technology (i.e; used in cryptocurrency). Presently, blockchain technology is used in Bitcoin but in future it is used for various places like healthcare, education etc.

REFERENCES:

- *" Bitcoin: A Peer- to- Peer Electronic Cash Systems"-https://bitcoin.org/bitcoin.pdf*
- *"Blockchain Technology - Current Status and Future Research Opportunities in Various Areas of Healthcare Industry" by P.S. Aithal, Archita Aithal &Edwin Dias (2021)-*
- *https://srinivaspublication.com/wp-content/uploads/2021/07/10.-Review-of-Blockchain_Fullpaper.pdf*
- *"A Detailed Study of Blockchain: Changing the World" by Shwetha Singh, Anjali Sharma, Dr. Prateek Jain(2018)-https://www.ripublication.com/ijaer18/ijaerv13n14_26.pdf*