International Journal for Modern Trends in Science and Technology, 6(10): 60-64, 2020

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST061011
Available online at: http://www.ijmtst.com/vol6issue10.html

Blockchain: The Essential Future of Modern Internet

Pagalla Bhavani Shankar

Department of CSE, Sri Vasavi Engineering College (Autonomous), Tadepalligudem, Andhra Pradesh, India

To Cite this Article
Pagalla Bhavani Shankar, "Blockchain: The Essential Future of Modern Internet", *International Journal for Modern Trends in Science and Technology*, 6(10): 60-64, 2020.

Article Info
Received on 17-September-2020, Revised on 02-October-2020, Accepted on 08-October-2020, Published on 11-October-2020.

ABSTRACT

This paper deals with the future of modern internet, named as "Blockchain". Blockchain is renowned as the worlds populating a type of new software platform for all kinds of digital assets. In a form of, forms of blocks data will be stored or recorded in blockchain, and emerged & protected and secured by the conceptual of Cryptography. After release of bitcoin, the "Modern Internet : Blockchain" became a high peak internet protocol , which is transforming the values of data from a node to node in a block and working in a decentralized manner. Blockchain is a state of art technology that is always associated with a great level (layer) of security and privacy In today's tremendous technology innovations, blockchain technology is not only implemented in crypto-currencies , but also in social and corporate segments too, like e-commerce, e-governance, logistics and many others.

KEYWORDS: *Blockchain, Digital Assets, Block, Node, Cryptography, Bitcoin, Crypto-currency*

INTRODUCTION

Technology is a boon and gifted to today's generations and futures too. The day ends, technology is risen at every day of our esteemed lives. Today's technology plays a vital role and be as a part with us. It simply states that, Generations are gone up – Innovations are grown up day by day. In today's world encompassing a word "internet". By using internet generations of people will search the data, store the data and retrieving the data in a secure communicative way. Simply it seems that world is stimulated around on "Data", is a collection of information. At this point of scale, securing and protection of data will be a big risky task. To overcome this kind of problems, integrating or associating the data with the language of Cryptography yields the protection and securing the data in specified manner. Storing or sharing the data in the form of interlinked blocks (nodes) associated with Cryptography, is era of today's modern internet: Blockchain.

CRYPTOGRAPHY

Cryptography is a Greek word, where as crypto means secure and graphy means writing, simply a secure writing. By using the language of cryptography [2], it converts the readable input text into unreadable output text. Cryptography is protecting the data from various kinds of intruders. Cryptography is a combine process of both encryption and decryption. Encryption is a way, the process of converting readable plain text into unreadable cipher text. Whereas, Decryption is a way, the process of converting unreadable ciphers text into readable plain text.

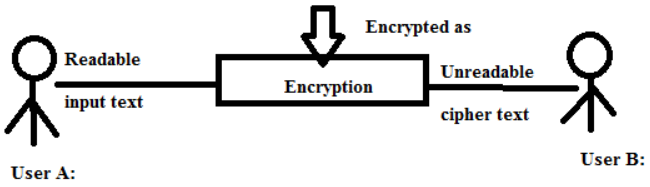

Fig. 2.1 Process of Encryption

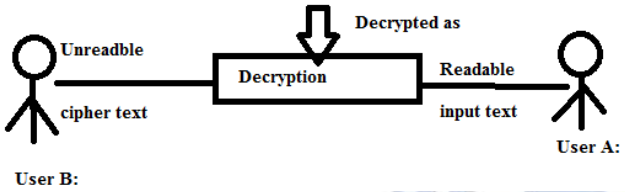

Fig.2.2. Process of Decryption

The process of both encryption and decryption yields to the fulfillment the concept of Cryptography. The process is called Cryptanalysis. Cryptography protects the data in two different ways: (a) Symmetric Cryptography, (b) Asymmetric Cryptography.

SYMMETRIC CRYPTOGRAPHY

Symmetric Cryptography [2] protects and secures the data with a unique public key or same key at the both end users of a communication. An end user uses same unique key for both encryption and decryption process, is termed as Symmetric Cryptography. Symmetric Cryptography, done or varied by two different techniques such as: substitution techniques and transposition techniques. For example, 'DATA' is a word, protecting by using symmetric cryptography with an unique key value 2. (k=2)

Process of Encryption as :

D A T A -------- 3 0 19 0

+k +k +k +k -------- +2 +2 +2 +2

(Where k = 2) 5 2 21 2

(Encrypted) ---------- F C V C

3.1. Process of Encryption using symmetric cryptography

The word 'DATA' is encrypted as 'FCVC'.

Process of Decryption as:

F C V C -------- 5 2 21 2

-k -k -k -k -------- -2 -2 -2 -2

(Where k = 2) 3 0 19 0

(Decrypted) ---------- D A T A

3.2. Process of Decryption using symmetric cryptography

The encrypted word 'FCVC' is decrypted as 'DATA', which is an input original plain text.

In the above example, "DATA" is a word, which wants to be secured and protected in an end user communication. In the process of symmetric cryptography, both end users validates and converts the message with a same key (symmetric), where k is a key and the value is 2. At 3.1. Process of symmetric cryptography user B(2.1) receives unreadable text and at 3.2. Process of symmetric cryptography user B decrypts the message with the same symmetric key, which is used by user A(2.1).

ASYMMETRIC CRYPTOGRAPHY

Asymmetric Cryptography [2] is a type of language of cryptography. In asymmetric cryptography, user A uses a key and user B uses another different key, like if one uses public key (PU) and other uses private key (PR). Examples for Asymmetric Cryptography are MD5, SHA-1, SHA – 256 and SHA – 512.

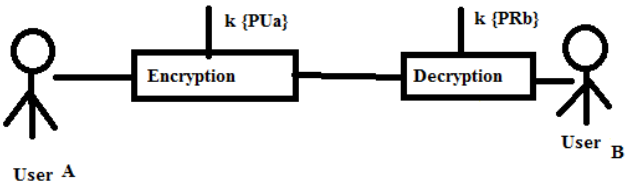

Fig.4.1.Model of Asymmetric Cryptography

BITCOIN & BLOCKCHAIN

Bitcoin is type of digital currency [1]. It is a crypto currency, simply a form of electronic cash. Emerging a spotlight on the block chain theory is due to the rapid invariant increasing the bit coin value.

Blockchain [3]is a type of form or subset of digital ledger for bit coin transactions, in and as a transparent and distributed in nature The definition of a blockchain is, "A digital ledger in which transactions made in bit coin and recorded chronologically and publicly; but a block chain is not a bit coin".

Blockchain have connective blocks and follows like linked list. Blockchain is a data structure, immutable and validated by distributed network and it have an peak level of cryptographic security.

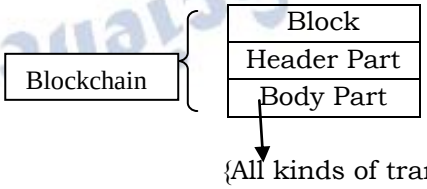

Fig.5.1. Model Representation of a Blockchain

Blockchain is a form of digital distributed ledger technology, which constructs chain of blocks, hence it is named as blockchain . A block

maintains & records the data of various assets, digital transactions and it is interlinked with the both previous and next nodes of blocks.

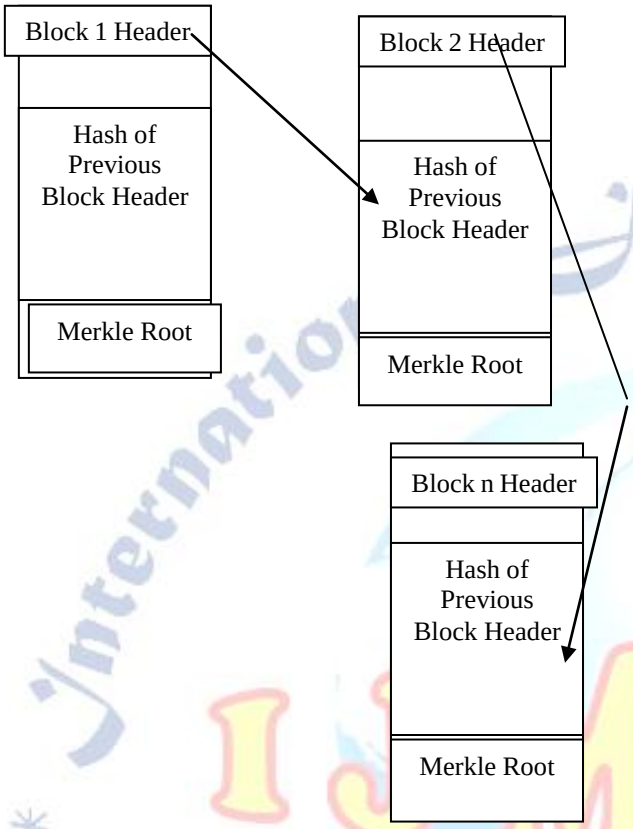

Fig.5.2. Structure of a block in the chain

Blockchain is a simply transactional pool and is a decentralized autonomy technology. In a blockchain at any block, is there anything happens at a particular block of networks, simply it happens as a whole in blockchain network under the properties of one-way, deterministic and avalanche effect in nature.

Blockchain perhaps the characteristics of immutability of data transparency, decentralization and security. Blockchain is a peer-to-peer to network [16] decentralized autonomy obeys the mutual consensus among the all network peers in a decentralized network by terms of proof of work (POW), proof of stack(POS) and byzantine fault tolerance. Consensus is a process of agreement between distributing nodes on a final state of the data. Requirements for consensus mechanism are agreement, validity, termination and fault tolerance. Considerations of consensus is duplicating results, for checking if any duplicates, uses a key termed as “nonce”. Merkle root is a kind of binary tree.

SHA-256

Blockchain is a P2P networking environment of group of minors. Minors are lenders, lends their computing power to solve complex problems. There is no central authority to manage blockchain. Anyone can join the network at any point of time. To solve the type of complex problems in the network of a blockchain, minor uses the complex algorithm is SHA-256, is a type of language (algorithm) of cryptography.

Secure Hash Algorithms (SHA) [2] was initially developed by National Institute of Standards and Technology (NIST) and published in 1993. SHA is based on the function of hashing or hash. Later NIST produced revised versions of SHA, with the hash value lengths of 256, 384 and 512 bits, known as SHA-256, SHA-384 and SHA-512.

Logic of SHA-256 : SHA-256 takes as input message with a maximum length of less than 2^{64} bits and produces as output of 256 bit message digest.

SHA Parameters	SHA – 1	SHA - 256
Message Digest Size	160	256
Message Size	$< 2^{64}$	$< 2^{64}$
Block Size	512	512
Word Size	32	32
No. of Steps	80	64
Security	80	128

VI. Comparisons of SHA Parameters

Based on the SHA-256 algorithm, complexity of problems will be solved in blockchain technology in the form of hash value of data.

SMART CONTRACT

To verify a contract digitally, facilitate, verify or enforce, judge performance of a specified project. Smartly, is named as “Smart Contracts”. The term blockchain and smart contracts will go to change the contract management in future. To be creating a smart contract, solidity and ethereum are the enough resource tools.

SoLIDITY

Solidity is a programming language and looks like object oriented programming language for writing smart contracts in various platforms of blockchain. In the year of 2014, August solidity programming was initially proposed by Gavin Wood, later it was developed by Christian Reitwiessner. Solidity and smart contract programs are run on EVM,where Ethereum [21]Virtual Machine. Solodity, Golang. JavaScript,

C++, Java, SQL, LLL(Lisp Lite Language), Viper, Serpent, Pyethereum and Go programming are the examples for to creating blockchain contracts.

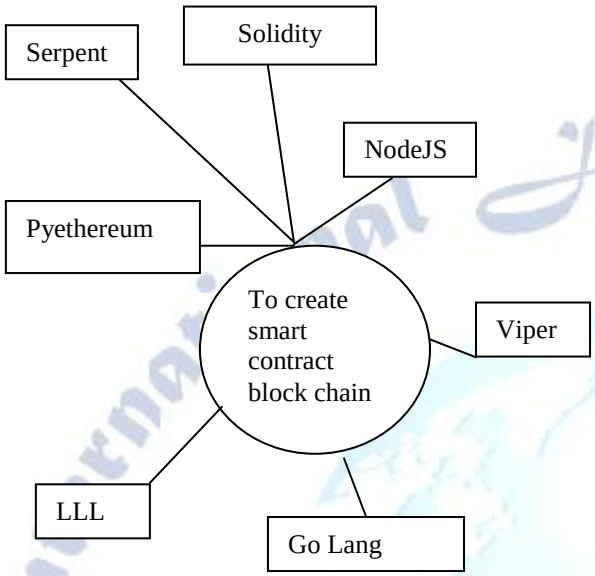

Fig.8.1.Example SmartContract – Programming Languages

The basic structure of a solidity programming language is

Pragma Solidity ^ Version
Contarct Name of the Contract
{

}

Pragma and contracts are the two keywords in solidity programming language.

To compile a program in solidity[21], user (programmer / miner) need a specific EVM compiler. Example: 0.5.14+commit.1f1aaa4,0.5.13+commit.5b0b510c , 0.5.8+commit.23d335f2----. To run a solidity program in an environment of smart contracts, minor has to install the two attributes compilers, deploy and run transactions. At the deploy and run transactions, user can select the environment, account, gas limit and value of ether. Gas is a particle, use to run the code in an ethereum environment.

Total Gas = Gas Used X Gas Price

ETHEREUM

To enable a smart contract, ethereum [21] plays a vital role in blockchain based distributed computing platform and it is publicly available as an open source. Platform of ethereum generates token called “ether”, which can be used and transferred within in the network of blockchain to mining the nodes. Ethereum executes the scripts using Ethereum Virtual Machine (EVM). Ethereum is immutable, securable and flexible in nature.

Glance of	Ethereum	Bitcoin
Block Time	14 to 15 Sec	10 Minutes
Mining	Generates new coins at consistent rate	Generate new coins at a rate that ½ halves every 4 years.
Units	Ethereum Gas Units	Fee specified in Satoshi per byte.
Transaction Fee	US $ 0.156 (in June 2019)	US $ 54(in June 2019)

IX .Comparison between Ethereum and Bit Coin

I. Applications

Blockchain is secure in tradition. Blockchain stores sophisticated and annoynmous software instructions that are too difficult for attack to manipulate the data. So, in an network platforms usage of blockchain increases rapidly by day by day.

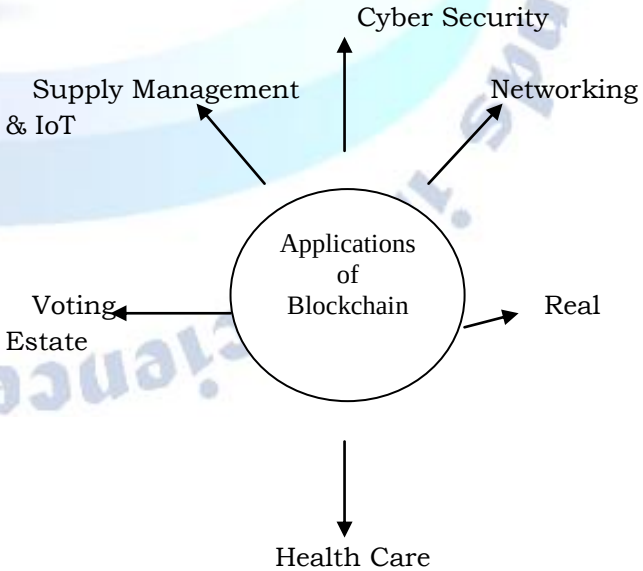

Fig.10.1. Applications of Blockchain

CONCLUSION

A Blockchain protects the data, in a decentralized environment, offers both encryption and validation. Blockchain can be private or public and virtually impossible to hack. It offers quality assurance. Blockchain ensures fast, cheap and secure transfer funds across the globe. Blockchain is well known for its traceability. Through blockchain, transactions are become more transparent. Blockchain enhances the every module of secure and transparence in modern internet: Blockchain.

REFERENCES

[1] https://www.hyperledger.org/
[2] William Stallings ,Cryptography and Network Security, third edition
[3] github.com/jpmorganchase/quorum/wikichain.com
[4] Corda.net/
[5] docs.bigchaindb/en/latest/terminology.html
[6] www.bigchaindb.com/features/bigchaindb.com/
[7] crunchbase.com/organization/bigchaindb#section-locked-charts
[8] docs.bigchaindb.com/projects/server/en/latest/simple-deployment-template/indent.html
[9] www.steelkiwi.com
[10] https://www.blockchain-council.org
[11] https://brd.com
[12] www.wikipedia.org
[13] https://blockchainhub.net/
[14] https://medium.com
[15] https://www.coindesk.com
[16] Pagalla Bhavani Shankar, "Enhancing approach to Objective Cyber Security through Digital Literacy",ISBN:978-81-936640-1-8
[17] blockchain.com
[18] investopedia.com
[19] blockgeeks.com
[20] bitcoinpaperwallet.com
[21] remix.ethereum.org
[22] remix-project.org