Network Based Adaptation of Block Chain Technology

Ch. Rupa, D. Jaya Kumari

***Abstract:** Online transactions are growing up day by day due to globalization factors. Threat victims rate also increasing due to lack of privacy protection and identity theft. The number of technologies have been using for maintaining the communication data like Torrent Technology, Databases, etc. Even though threat agents seeking new trends to attack the data. So a technology is required to do a secure transaction in the enterprise society. Recent technology, which can be played a vital role in data security, is Block chain. Once created a block lack of alter function in the block chain will helps to reduce the information attacks/forgery. This paper addresses block chain technology concepts with internal architecture and its applications along with the data communication over a network with block chain objective. The main strength of this work is simulation results with and it's analysis.*

***Index Terms:** Privacy protection, Identity theft, blockchain, security services, Database, Torrent*

I. INTRODUCTION

Currently, privacy protection is becoming a major issue in the society. All kinds of data transactions are suffering from this threat due to new trends are using the threat agents. Like, Spoofing and cloning type of threats are main causes to attacks on Integrity and Authentication security services. Also, it extends towards Phishing Attacks [1]. Day by day security issues is growing up in all the applications with the current systems by rapid growth in the technology utilization by the users. As well as the number of issues facing the users with the current application systems are like over transaction fee, double spending problems, hacking, Net fraud, etc.

Now, blockchain technology can able to reduce the threats and problems with the current system by its distributed transaction based and with a high-end secure design system. In this, every individual transaction is verified by cross-checking ledger and uses complex encoding and hashing techniques to overcome double spending problem [2]. A global network of computers uses Blockchain technology is the technique behind of crypto currency (Bitcoin, Ripple,etc). It is a data structure which designed the set of specific complex algorithm to achieve Byzantine fault tolerant state of global transaction ledger [3]. This technology helps to maintain logs transactions across the number of computers that is a distributed and decentralized digital ledger. Blockchain has to be characterized by four elements such as Cryptography, Replicated ledger, Business logic and Consensus.

Cryptography is for doing ledger integrity, authenticity and privacy of transactions and verifying Identity of the participants. Replicated ledger maintains history of all transactions. Business Logic embedded in the ledger and executed together with transactions. All transactions validate by Consensus which can referred as Decentralized protocol. Generally, It is a method to validate the order of transactions, or requests on a blockchain network.

II. BLOCKCHAIN METHODOLOGY

Blockchain has built from three technologies as shown in figure 1 which are P2P Network, Cryptography (Confidentiality and Authentication) and its program. The blockchain technology affects on two key costs such as cost of verification and cost of networking. The cost of verification related to validation of the transaction attributes with less cost. The second cost, cost of networking, is without the need for a traditional mediating, bootstrap and operate at marketplace. At regular intervals, blockchain allows a decentralized network of economic agents to agree, about the true state of shared data. This shared data can represent exchanges of currency, intellectual property, equity, information or other types of contracts and digital assets.

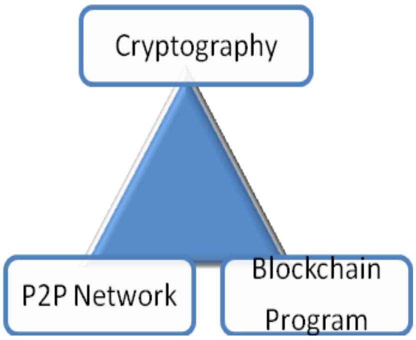


Figure 1. Blockchain Technologies

Blockchain uses private key cryptography (confidentiality) [4] to secure identities of the transaction heads and uses high-end hash functions (authentication) [5] to make the blockchain immutable. Private keys play vital role in the blockchain based distributed transactions. Mechanism doesn't need to be kept secret but the secret key (Private key) does.

The keys are mathematically related to all hash based addresses. To maintain consistency in the distributed ledger, Peer to Peer (P2P) [6] machines on

Revised Manuscript Received on July 05, 2019.

Ch. Rupa, Dept. of CSE, V. R. Siddhartha Engineering College (A), Sri Vasavi Engineering College (A) Andhra Pradesh, India
D. Jaya Kumari, Dept. of CSE, V. R. Siddhartha Engineering College (A), Sri Vasavi Engineering College (A) Andhra Pradesh, India

DOI: 10.35940/ijitee.G6317.078919

the network will help in this technology. It extends to Block-Chain program gives the blockchain protocol based on the requirement.

Blockchain is originally "**blockchain**" that is a continuously growing with the list of logs (records) which are called blocks [15]. Each block consists of the hash value of the earlier block which is nothing but a unique value generated by authentication algorithms (like SHA) to the block, which can be linking the two and form as a chain. Blocks include the collection of valid transactions which encoded into hash based Merkle tree [7]. Not possible to alter the once recorded data in the block without alteration of subsequent blocks. Hence considered Transaction data of the block (stored) is permanent. This is an iterative process with integrity confirmation of the earlier block. This technology is managed by the P2P network that is adhering to a protocol for validating new blocks. There are incentives and reward points for the latest block creators (called as Miner) to validate the transactions and creates the latest blocks by solving a complex mathematical puzzle associated with the blocks [8]. For a block to be accepted by network participants, miner must complete a proof of work which covers all the data in the block. Each block holds a hash value of the earlier block, current transactions data hash value and the nonce. This nonce is an arbitrary number which can be used only once to reduce reply attacks in authentication protocols as shown in figure 2.

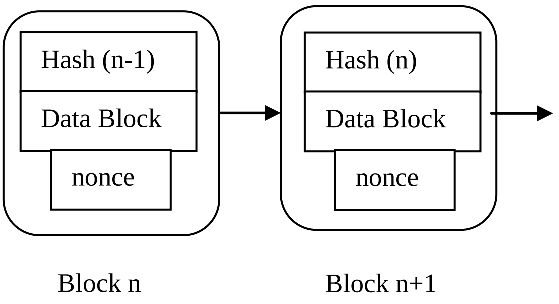


Figure 2. Process of a Block Creation

Every block has a life time that is the average time it takes to generate one new block in the chain. Ethereum is an open source, public, blockchain distributed computing platform and operating system featuring smart contact functionality. The block time of Ethereum is set to between 14 and 15 sec, while for Bitcoin is 10 min [9,10].

As a process in blockchain technology at first, if someone requests a transaction that request can broadcasted to a P2P network. The P2P network will validates the transaction using cryptographic algorithms. This verified transaction can involve in all the processing information. Verified transaction can able to combine with other transactions to create a new block of data for the ledger. Add this new block to the blockchain with the existing blocks, like this way it became permanent and unalterable. The total process is as shown as figure 3

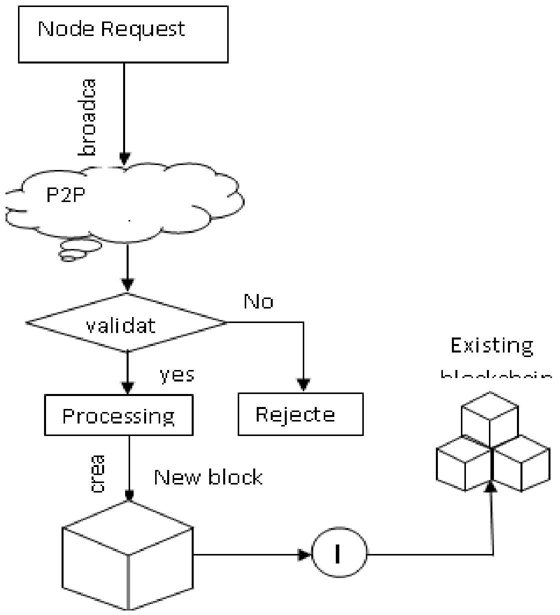


Figure 3. Process Of A Block Chain Creation

III. RESULTS AND ANALYSIS

NS2 Simulator is used to show the application of block chain technology, and also used AODV protocol for establishing the path between the nodes. The Ad hoc On-Demand Distance Vector (AODV) calculation empowers dynamic, multi-hop, self-beginning routing between taking an interest node that needs to make and keep up a specially appointed system. AODV grants versatile nodes to react rapidly to interface breakages or some other changes in organizing topology precisely. Keeping up arrangement numbers-Each passage in routing table keeps up the present data about the destination succession number and hash value of the earlier stage.

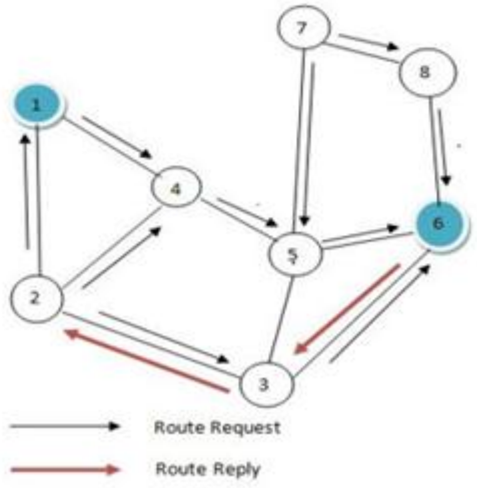
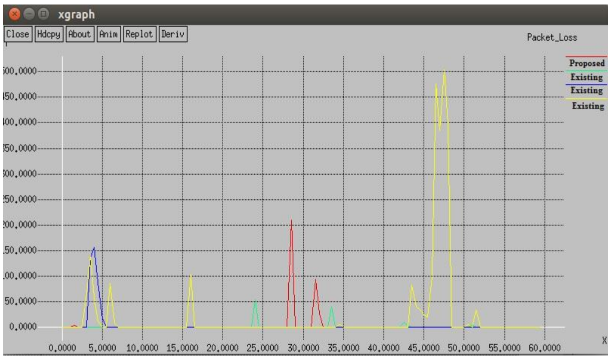


Figure 4. Simulation on NS2

Figure 4 explains the path finding process clearly. Where 'H1' considered as a initial hash value generates at node 1. By AODV routing protocol next visiting node is 2 to establish the path between source to destination.

Where 'H2' is the hash value



generated at node 2 by including earlier hash value ‘H1’. Packet loss also reduced and monitored by using blockchain technology. This feature tested results by considering MANET features has show as figure 5.

Figure 5 : Packet loss Ratio

3.1 Cost Factors Analysis

Table 1 shows that the comparison analysis among the Blockchain technology to other existing techniques such as Database and Torrent technologies. All the methods support client server architecture whether as intrinsic or extrinsic but t[1]he cost of the existing technologies are more compare to blockchain due to all the services supported by it as inbuilt should be extrinsic in the other approaches.

Table 1. Comparison Results With Existing Techniques

Methods Factors	Data Base	Torrent	Block Chain
Confidentiality	Extrinsic	Extrinsic	Inbuilt
P2P Network	Extrinsic	Extrinsic	Inbuilt
Own Protocol	No	No	Inbuilt
Redundancy	Yes	More	No
Reliability	< block chain	< block chain	More
Cost	High	High	High
Client-server architecture support	Yes	Yes	Yes

Blockchain efficiency is 90% more than that of the exiting techniques [16]. Duplicate data (Redundancy), Confidentiality, Peer to Peer network establishment factors shows more impact in the efficiency of the technologies. Modern cryptographic techniques like hash based algorithms were inbuilt by the blockchain technology which will extrinsic in others. It reduces the packet loss ration s shown in figure 5.

IV. APPLICATIONS

The main applications of block chain technologies are not only in the banking sector (crypto currency), can be used for a wide variety of applications such as Healthcare, Internet of Things (IoT), Real Estate, Voting, Low Enforcement, online music, etc [9]. Blockchain utilization has been growing up day by day due to it has owned by secure transaction management. This technology could be reduced the issues with current banking systems such as DOUBLE SPENDING problem and HIGH TRANSACTION FEE by using securely distributed ledger function [12].

Transparency of certificates can possible to improve using blockchain technology. Already some of the Governments started to utilize this technology. Recently Government of Andhra Pradesh announced that in the coming academic year onwards all the certificates will maintain through multi cloud based block chain technology only.

A World Economic Forum has reported from September 2015 predicted that 10% of global GDP would be stored on blockchain technology by 2015. Currently, IBM offers a cloud which is blockchain service based on the open source Hyper ledger Fabric project [11, 12]. Oracle has joined the Hyper ledger consortium and Oracle cloud offers blockchain cloud service based Hyper ledger [13,14]. Microsoft Visual Studio has been making the Ethereum Solidity language available to application developers [16].

As well as solutions for the main issues of integrity checking and confidentiality rating of backup versions on the cloud based environment can achieve using block chain technology. Also smart Contract using blockchain technology architecture will become an important reference in the distributed nodes based environment [17].

V. CONCLUSION

Block chain technology is becoming a good a choice for all the distributed transaction management systems. Maximum application holders feel that achieve their goals with block chain technology auditing transactions. Especially, block chain technology utilization may increase in the health care system due to its complete transparency system which helps in the audit of patient-owned personal health records. Simultaneously required to take precautions to overcome the cyber attacks in the blockchain technology based organizations by doing strengthen the Cyber Security techniques in the organizations.

REFERENCES

1. Şerafettin Şentürk, Elif yeril, “Email phishing detection and prevention by using data mining techniques”, IEEE Int. Conf on Computer Science and Engineering (UBMK), Oct, 2017.
2. Carlos Pinzon, Camilo Rocha, “Double Spending Attack models with Time advantage for Bit coin”, Electronic Notes in Theoretical Computer Science, Volume 329, no.9, pp. 79-103, 2016
3. Cristina P´erez-Sol, et. al, “Double-spending Prevention for Bitcoin zero-confirmation transactions”, e-print, IACR, 2017
4. Guegan, “Public blockchain vs Private blockchain”, HAL achieves, 2017
5. Ruiguo, etl.al, “Authentication with blockchain algorithm and text Encryption protocol in calucaltion of social network”, IEEE Access, vol. 5, 2017
6. Sergi Delgado-Segura, et.al, “Cryptocurrency networks: A new P2P paradigm”, Mobile Information system, Hindawi, 2017
7. J. A. Garay and A. Kiayias, “The bitcoin backbone protocol: Analysis and applications”, eprint, IACR, 2016
8. “Next generation smart contract and decentralized application platform”, White paper, Github, 2017
9. Gavin Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger”, EIP-150 REVISION (Founder copy)
10. Alysson Bessani, et.al, “A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform”, ACM Proceedings of the workshop on Scalable and Resilient Infrastructure for Distributed Ledgers, 2017
11. IBM-CII,“IBM White paper on Next generation supply chain powered by cognitive and blockchain”, 2016
12. Arnab Banerjee,“Integrating blockchain with ERP for a transparency supply chain”, Infosys, 2016.

13. Oraclechain, “Oracle chain technical White Paper”, 2017
14. Prisco, Giulio "Blockchain Initiative to Streamline Record-Keeping for Private Companies". Bitcoin Magazine. BTC Inc., 2016
15. Block Apps, “BlockApps Brings Ethereum Blockchain Development to Windows and Visual Studio” e-print, consensys, 2016
16. Christian, et.al, ‘Some Simple Economics of the Blockchain’, MIT Solan Research Paper, Elsevier, 2017

AUTHORS PROFILE

Dr. Ch. Rupa is working as a professor in VRSEC (A), Vijayawada. She was a senior member of IEEE and Life Member of CSI, ISTE, IAENG, IEI, IACSIT. She published more than 70 papers in various journals and conferences. JNTU kakinada has awarded her as a Young Engineer of 2010. IEI awarded her as National young Engineer of 2011 Govt of A. P and IEI by combined awarded her as Young Engineer of 2012. Her main research interests includes information security, Image Processing, Security algorithms. She has received couple of awards from IETE, IEI(I) for her work.

Dr. D. Jayakumari is working as a professor & HoD of Dept. of CSE in Sri Vasavi Eng. College (A). She was a life member of CSI, ISTE societies. She has received her B. Tech and M. Tech degrees from JNTU, Hyderabad and Ph. D from Andhra University. She has presented and published good number of papers in the reputed journals and conferences. Her main research interests include analytics and algorithms.