Scalability Issues of Blockchain Technology

Hemlata Kohad, Sunil Kumar, Asha Ambhaikar

Abstract: ***In last decade crypto currencies become popular as there is no third party involvement while doing the transactions. Blockchain is the technology for using crypto-currencies. It attracts the attention of researchers and academicians , along with different features of Blockchain it is having the major issue of scalability which can be categorized into throughput , cost, capacity and networking . Improvement in Scalability affects the application of blockchain in business . Scalability affects due to some other factors like block interval time and block size which also may reduce the security . System may become vulnerable to different attacks if we blindly modify the scalability .In this paper we analyze the different ways to improve the scalability then we compare the features of blockchain with respect to different algorithms used to solve the scalability issue.***

Keywords : Blockchain, scalability, throughput

I. INTRODUCTION

In this modern Information Technology World, it is hard to store transactions in a centralized storage way, then the blockchain technology comes into existence, it provides a peer to peer connection and stores the data into a decentralized format. A lot of crypto currencies come into existence when it comes to blockchain that transaction is possible without third party involvement. The blockchain technology is capable of load balancing of the transactions of the network whereas in centralized transaction, banks or the government bodies hold all the transactions which a typical task is to manage in the cases of power failure or any other issue. Blockchain technology promotes the management of load properly using the concept of crypto currencies [3].

Various hashing algorithms are used in order to maintain the uniqueness of every transaction done. The next level of blockchain would be implement faster algorithms for the hashing so that the basic transactions can also be done with the crypto-currencies. In the Proposed Research work, we have proposed integrated model using blockchain that supports scalability so that if any block is to add in the chain, it can be easily done. The main issues that are resolved by the framework is that the security of the block is retained through various algorithms so that the data can be transmitted easily from one block to the other block and the integrity of the data can be maintained [9]

Data decentralization, transparency, security, immutability, and privacy are the Key driving principles of Blockchain Technology. Blockchain is a data structure by which digital ledger of transaction can be created, shared, or stored among a distributed network of computers. Block chain protocol controls access-manager so that it does not require trust in third party.

Revised Manuscript Received on February 04, 2020.

Prof. Hemlata Kohad, Professor, Department of Electrical and Electronics, Kalinga University, Raipur, India.

Dr. Sunil Kumar, Professor, Department of Electrical and Electronics, Kalinga University, Raipur, India.

Dr. Prof. Asha Ambhaikar, Professor, Kalinga University, Naya Raipur. Professor, Department of Electrical and Electronics, Kalinga University, Raipur, India.

Transactions on distributed ledger is based on cryptographic consensus algorithm through peer to peer network of devices [3] .Miners are the nodes in a network of computers who, together, verify all bitcoin transactions. Bitcoin protocols builds a trusted public ledger of transactions that cannot be controlled by a single entity. These transactions cannot be inspected and changed can anyone. The protocol provides enough economic incentives to the owners and operators (the miners) of the computing devices to sustain the cryptographic transactions in the distributed ledger [5].

Features of Block chain

- **Decentralization of consensus**:
  The distributed nature of the network requires untrusted participants to reach a consensus.
- **Transparency**:
  Records are auditable by a predefined set of participants, although the setcanbe open. For example, in public blockchains everyone with an Internet connection to thenetwork holds equal rights and ability to access the ledger. The records are thus transparentand traceable.
- **Security:**
  Blockchains are shared, tamper-proof, replicated ledgers where records areirreversible and cannot be forged thanks to one-way cryptographic hash functions.
- **Immutability**.:
  Blockchains function under the principle of the non-repudiation and irreversibility of records. Other non-fundamental properties of blockchains include data automation and data storage capacity.
- **Automation and smart contracts**:
  Without the need for human interaction, verification,orarbitration, the software is written so that conflicting or double transactions are not permanentlywritten in the blockchain.

We are increasingly depending on network communications. Computer based technologies impacting on information that we want to access, store and distribute. The most important use of computer-based technology is electronic commerce. The transactions that we want to do must be highly secured. Electronic payments include digital checks, credit cards, debit cards etc. this system requires protection from hackers. Security for electronic cash schemes can be achieved via digital signature. In public key cryptography based digital signature each user has a secret key and a public key [4].

Digital signature is a secret key and it is verified by the public key. Digital signature provides part of the solution for online payments to be sent directly from one party to another through the financial institutions. The main benefit of digital signature lost as the trusted third party requires double spending. Double spending problem can be solved by using peer-to-peer network [1]. In recent years a new class of accountable systems emerged. The first such system is Bitcoin which allows users to transfer currency (Bitcoin) without a centralized regulator.

Modern economy depends upon number of servers spread over the world, much

of our modern economy is digital. This modern economy must be fueled by affordable electricity. For transaction a new form of currency used called cryptocurrency. Online transaction done through bitcoin uses decentralized network [9].

Transactions on distributed ledger is based on cryptographic consensus algorithm through peer to peer network of devices. Miners are the nodes in a network which verify all bitcoin transactions. Bitcoin protocols builds a trusted public ledger of transactions that cannot be controlled by a single entity. The Miners get sufficient economic incentives for using computing devices to sustain the cryptographic transactions in the distributed ledger. These incentives are represented in the form of tokens. The token of botcoin determines circumstances under which new transaction blocks are validated before they are appended to the blockchain ledger. Miner may have a unique identification number or multiple identification numbers. This identification number is like Social Security number. All over the world computer involved in mining bitcoin work together and if the part of network fail, the system partition that piece off and continue to work.[5]

This technology basically has 4 elements.

1. **Consensus:** Provides the proof of work (PoW) and verifies the action in the networks.
2. **Ledger:** Provides the complete details of transaction within networks.
3. **Cryptography:** Makes sure that all data in ledger and networks gets encrypted and only authorized user can decrypt the information.
4. **Smart contract**: it is used to verify and validate the participants of the network.

II. CONSENSUS MECHANISMS

Whenever the transactions in Blockchain is carried out between the nodes , the block will get added to the chain after the validity . for the validity of block different consensus mechanisms are used like Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerence (PBFT), Proof of Elapsed Time (PoET), Proof of Existence(PoE),Proof of Activity (hybrid of proof of Work and proof of Stake),

In many fields like medicine , economics , Internet of Things ,software engineering the blockchain technique is used. Because of decentralized consensus mechanism of blockchain, without the need of any third-party trusted authority smart contracts allow mutually distrusted users to complete data exchange or transaction. Ethereum is the most widely used blockchain supporting smart contracts, where there are already 317,506 smart contracts and more than 75,000 transactions happened daily . Since blockchain is one of the core technologies in FinTech (Financial Technology) industry, users are very concerned about its security. Some security vulnerabilities and attacks have been recently reported. Loi et al. discover that 8,833 out of 19,366 existing Ethereum contracts are vulnerable [9]. Note that smart contracts with security vulnerabilities may lead to financial losses. In June 2016, the criminals stole around 60 million dollars by attacking the smart contract DAO [10] by exploiting a recursive calling vulnerability . As another example, in March 2014, the criminals exploited transaction mutability in Bitcoin to attack Mago, the largest Bitcoin trading platform. It caused the collapse of MtGox, with a value of 450 million dollars Bitcoin stolen [12]. The closest research work that only focuses on Ethereum smart contracts, rather than popular blockchain systems. Although a series of related attacks on smart contracts are listed in , there lacks a discussion on security enhancement [16].

One of the major issues of blockchain is the scalability. Hundreds of crypto currencies on the market currently use blockchain network for transactions, mining and maintaining ledgers. All crypto currencies face scalability issue, but the world's largest electronic payment network is capable of processing thousands of transactions per second. Proof of work technique is used for validation of transaction in case of Bitcoin and proof of Stake in case of Ethereum. In the existing blockchain systems, there are four major consensus mechanisms: PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), and DPoS (Delegated Proof of Stake). Other consensus mechanisms, such as PoB (Proof of Bandwidth), PoET (Proof of Elapsed Time) , PoA(Proof of Authority) , Selfish Mining, Ripple protocol Consensus Algorithm(RPCA),Proof of importance(PoI). and so on. The Bitcoin and Ethereum System use the PoW mechanism. Ethereum also incorporates the PoA mechanism, and some other cryptocurrencies also use the PoS mechanism, such as PeerCoin, Shadow Cash and so on [3].

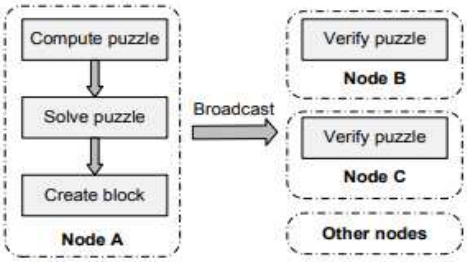

Fig.1 POW consensus Mechanism

PoW mechanism uses to find solution of puzzles to prove the credibility of the data. The puzzle is usually a computationally hard but easily verifiable problem. After validation of data by PoW node created the block and added to the Blockchain . After the PoW puzzle is resolved, it will be broadcasted to other nodes, to achieve the purpose of consensus, as shown in Fig1. Typically, PrevHash, nonce, and Tx is the information in each block of Bitcoin, Hash value of previous block is indicated by, and Txs denote the transactions included in the block. After solving PoW puzzle nonce value obtained. A correct nonce should satisfy that the hash value less than a target value, which could be adjusted to tune the difficulty of PoW puzzle.

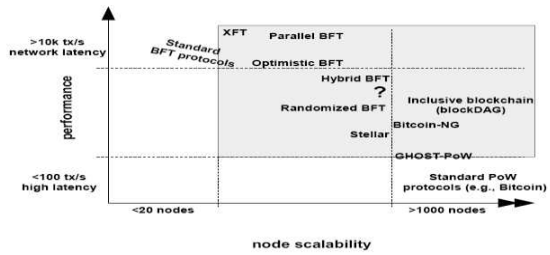

Fig. 2 Performance and scalability of different families of POW and BFT

Sompolonski and Zohar proposed the GHOST (Greedy Heaviest –Observed Sub –Tree rule [15]
Which resolves conflicts in a POW blockchain by weighing the sub trees rooted in blocks rather than the longest chain in given block rooted. GHOST offers conflict resolution strategy which improves the performance of standard longest chain rule of Bitcoin hence it increases block frequency and block size. GHOST rule is also implemented in Ethereum blockchain called GHOST-POW. In 2016 Ethereum throughput is fewer than 20,000 transactions per day i.e. about 0.2 transactions /sec [10].
Bitcoin-NG proposed by Eyal [16] uses standard POW for leader election , declaring a node which mines a block with standard difficulty (called key block) to become a leader until a new key block is mined. The leader can append microblocks in meantime , which are not subject to PoW mining but are merely hashchained together. This increases the throughput of the whole system and decrease the latency.
Lewenberg recently proposed block DAG(directed acyclic graph) instead of linear chain of blocks. Mazieres D , it allow non conflicting transactions to be initially on different forks.
Stellar proposed a protocol to increase the scalability in terms of number of nodes maintaining the other advantages over PoW.
Liu et al. proposed a novel network and node fault model called XFT that allows one to tolerate up to n/2 Byzantine nodes [10].

III. SCALABILITY ISSUE

Scalability can be categorized as throughput, cost and capacity and networking.

Throughput:

In bitcoin Blockchain 7 transactions are carried out in one second ,which is very low compared to VISA and PayPal. The time required to confirm the transaction is around 10 minutes and the size of each block is around 1 MB . 7 transactions per second is obtained by dividing the maximum size of block by an average size of each bitcoin transaction as 250 bytes.

Cost and capacity:

A large quantity of data is required to store in the Blockchain from recent block transaction to the genesis block . each node in the blockchain have limited storage capacity and resources.

Networking:

Whenever any transaction is carried out , it is first broadcast to all nodes . when a block is mined it is again transmitted to all nodes which consume slot of network resources and it increases the propagation delay. So there is a need to design more efficient data transmission mechanism.

Different applications are developed using the Blockchain , but the scalability is the major limitation . Scalability depend on the different factors : transaction per second, block size , chain size and digital signature.[18] . There are different ways to solve the problem of scalability : on chain,off-chain, child chain, interchain.

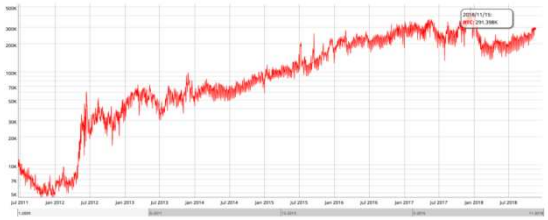

Fig. 3 Daily transaction on Bitcoin since July 2011

The number of transactions increased over one million in Jan 2018 from 3000 in Oct 2015

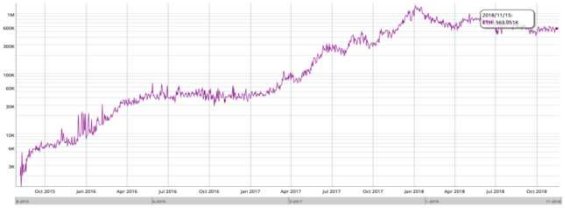

Fig. 4 Daily transaction on Etherium since mid-2015

Due to the growing number of transactions following things are observed

1) The average confirmation time for a transaction is increased.
2) Fee for the network transaction is increased
3) Difficulty to mine the block is also increased and hence computation power and resources is also increased.
4) The Block size is also increased.

As the number of transactions grow the system become slower, expensive and unsustainable.
So the scalability in blockchain become the focus area for researchers and academicians
Bitcoin processes 7 transactions per second and Etherium processes 20 transactions per second ,whereas payment by VISA is 2000 and PayPal is 200 .
Scaling can be achieved by including more transactions in a block . This can be achieved by two ways

A. On-Chain:

- Increasing Block size: In Bitcoin , blocksize is 1 MB ,Throughput increases but there is propagation delay and the forks may frequently occur which increases the cost of maintenance of chain. Thus simply increasing the block size is not the solution for the scalability of Blockchain.
  Data structure other than merkle tree to organize the data inside the Blockchain is Merkelized Abstract Syntax Tree(MAST)
- Reducing number of bytes required to represent information in each block: Information related to each transaction is stored in each block for security and verification.

- If we reduce the number of bytes required for storing information , we can achieve better throughput. We can use more efficient hashing algorithm that can generate short signature (Schnorr signature)

B. Off –chain:

Off chain solution can improve the scalability of Blockchain by processing the transaction outside the Blockchain. One of the off chain solution is lightning network.[the lightning network: scalable off chain instant payment). If any node make transactions frequently , off-chain micropayment channels are created between the nodes to handle the multi-signature transaction and only final transactions are processed on the Blockchain. Raiden network is the lightning network for Ethereum version. . But it reduces the security. Attack on off chain micropayment channel lost all the transactions performed over it.

- **Sharding : I**t is an effective method to improve the scalability of Blockchain. The nodes are divided into different shards. Each shard consist of part of transaction and there is parallel processing of transaction. Byzantine consensus algorithm verify the transaction within the shard.Elastico and Omniledger are the two examples of sharding Blockchain system. Size of shard is difficult to choose . performance of Byzantine consensus algorithm is affected by the large size of shard, small size of shard affects badly on the scalability of the Blockchain.
- **Bitcoin-NG**: improves throughput but with the compromise on security. If the leader selected is malicious double- spending attack may occur.

C. Side chain:

Rootstock and Blockstream studied the Side chain technologies , the exchange of cryptocurrency is possible .suppose I have Bitcoin which is having the disadvantage of less function, public, and slow can be use in Ethereum to use smart contract. But this can be achieve by transferring Bitcoin amount to special account for this trade and freeze it. The equivalent amount for that trade is created and after the completion of transaction remaining amount will be credited back to the Bitcoin.

D. Inter-chain:

It is difficult to choose a blockchain platform. Blockchain giving the flexibility of changing the platform using inter-chain . It serves as a bridge between public and private blockchains and can help to connect to protocols like Bitcoin and Ethereum.[17]

Table1 Comparison of Scalability with respect to different Technologies to improve scalability .

Technology	solution	Consensus Algorithm	Throughput	Cost	Capacity	Advantage	Disadvantage
On-chain	Big Block	PoW	High	Low	High	It will no longer be cheap to spam transaction	Bitcoin full nodes are forced to use more resources that don't support Bitcoin
						Fees will not be zero.	High fees may stop or reverse global adoption, investment, development, support and centralization

	MAST	PoW	-----	----	Low	More secure Larger smart contract	Not complete privacy
	Segwit	PoW	High	Low	----	High transaction speed Low transaction fees	Increases usage resources as the capacity , bandwidth increases
	Sharding	PBFT/PoS	High	----	Low	Low capacity burden Parallel processing	More protocol complexity
Off - Chain	Lightening Network	----	High	Low	Low	It may reduce traffic on Blockchain	It is designed only for small and medium scale payment
	Raiden Network	----	High	Low	Low	Low transaction fee allow to transfer tiny values	Raiden network requires some of tokens locked for life time
Child- chain	Plasma	POA	High	----	Low	Faster and less expensive	Security challenges need to be addressed to maintain immutability
Inter-chain	Atomic Swap	----	---	---	----	Worse in privacy	

IV. RESULT

The following graph plotted for 0-60000 transactions and confirmation time of transactions is in seconds

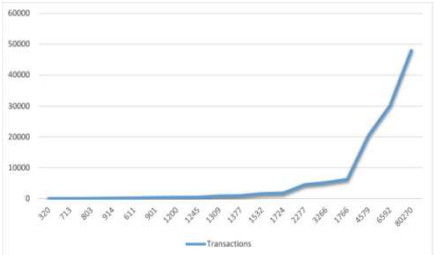

Fig 5. Transaction versus confirmation time.

From the above graph it is observed that as the number of transactions increases there is gradual increase in the confirmation time.

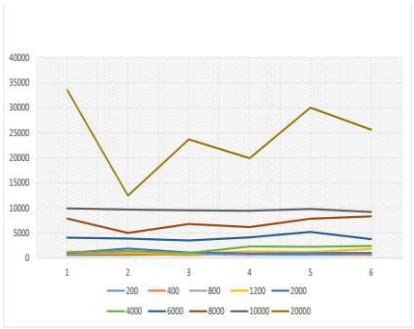

Fig 6. Transactions versus confirmation time.

In the above graph it is observed that as the transactions increases over 5000 there is drastic increase in confirmation time of transaction . As the number of transactions increases the overhead of transaction also get increased to mine the transactions in blocks , thus it increases throughput and network latency.

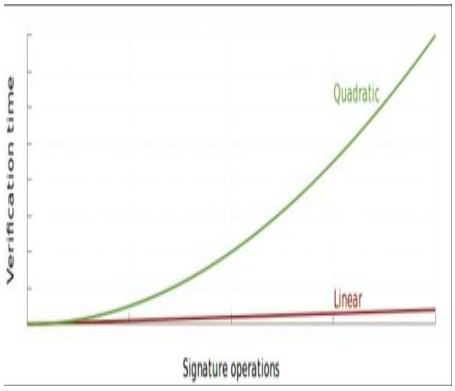

Fig 7 Signature operations versus verification time.

scalability of blockchain technology can be improved by increasing throughput is very important but only if we increase block size can cause many problems. As block size increases it cause an quadratic hashing issue so the structure of data stored in blockchain can be changed by using segwit protocol. 70 % of the block space is required to store the digital signature , Bitcoins 1-MB capacity block able to store more transactions by removing the signature data. Expected transactions per second will get increased to 20 transactions per second. If we divide the Blockchain into different parts called shard , each shard process the transaction results increase in speed of transaction . Sharding proposed to be implemented in a Etherium with Proof of Stake model in 2020.Expected transactions per second are 10,000 TPS.

V. CONCLUSION

In order to use Blockchain in business environment the scalability problem must be solved . In this article we discussed different mechanisms to solve this problem . For increasing the scalability Throughput is very important , but is Blockchain only put large amount of data related to transaction in block it causes a lot of problems. The Off-chain and Child-chain mechanisms can be used which reduce the burdon of main chain. Only increasing the block size will not solve the scalability problem, MAST algorithm solve this problem to some extent . Segwit method separate the signature so the amount of memory required to store signature will get reduced. Short signature can be generated by hashing algorithm (Schnorr signature).

REFERENCES

1. Shihab Shahriar Hazari , Qusay H. Mahmoud "A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems" 2019 IEEE
2. Marko Vukolic IBM Research – Zurich "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication" 2015
3. " Du Mingxiao ,Ma xiaofeng,Zhang Zhe,Wang Xiangwei,Chen Qijun "A Review on consensus Algorithm of Blockchain 2017 IEEE
4. Lakshmi Siva Sankar ,Sindhu M. ,M. Sethumadhavan "Survey of Consensus Protocol on Blockchain Applications" 2017 IEEE
5. L.M.Bach, B. Mihaljevic,M.Zagar"Comparative Analysis of Blockchain Consensus Algorithms" MIPRO 2018
6. " Lin Chen, Lei Xu, Zhimin Gao, Yang Lu, Weidong Shi" Protecting Early Stage Proof-of-Work based Public Blockchain 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops
7. Matthew D. Sleiman, Adrian P. Lauf, Roman Yampolskiy " Bit coin Message: Data Insertion on a Proof-of-Work Cryptocurrency System "2015 IEEE International Conference on Cyberworlds
8. Joanna Moubarak, Eric Filiol, Maroun Chamoun "On Blockchain Security and Relevant Attacks" 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)
9. Akanksha Kaushik,Archana Chaudhary "Blockchain Literature Survey "2017 IEEE conference on Recent trends in electronics Information & Communication Technology .
10. Marko Vukolic IBM Research ,Zurich ,Switzerland . " The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication" IBM research Zurich ,Switzerland Springer international 2016
11. Vitalik Buterin Plasma: Scalable Autonomous Smart Contracts August 11, 2017 WORKING DRAFT
12. Jean-Philippe Martin, Lorenzo Alvisi, and Michael Dahlin Department of Computer Science University of Texas at Austin "Minimal Byzantine Storage" DISC 2002, LNCS 2508, pp. 311–325, 2002. Springer-Verlag Berlin Heidelberg 2002
13. Liehuang Zhua , Yulu Wua , Keke Gaia,∗ , Kim-Kwang Raymond Choob "Controllable and Trustworthy Blockchain-based Cloud Data Management" Elsevier August 25, 2018
14. Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew "MedRec: Using Blockchain for Medical Data Access and Permission Management"Lippman Media Lab Massachusetts Institute of Technology Cambridge, MA, 02139, USA 978-1-5090-4054-4/16 2016 IEEE
15. Sompolonsky,Y., Zohar ,A. : Secure high rate transaction processing in Bitcoin . In: Bohme ,R .,Okamoto, T.(eds) FC 2015 . LNCS ,Vol 8975, pp 507-527 ,Springer ,Heidelberg 2015.
16. Eyal, Ittay, et al. "Bitcoin-ng: A scalable blockchain protocol." 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16). 2016.
17. Soohyeong Kim , Yongseok Kwon , Sunghyun Cho , "A survey of scalability solutions on Blockchain" 978-1-5386-5041-7/18 2018 IEEE
18. Junfeng Xie, F. Richard Yu, Tao Huang, Renchao Xie, Jiang Liu, and Yunjie Liu , "A Survey on the Scalability of Blockchain Systems "0890-8044/19 2019 IEEE

AUTHORS PROFILE

Prof. Hemlata Kohad, she has 15 years of Academic experience. She is a member of institution of engineers ,she is also have life membership of ISTE. She has published 10 research papers in national and international journals .she is editor of International journal of engineering research and applications, International journal of research and development.

Dr. Sunil Kumar, Professor and Head Electrical and Electronics Department Kalinga university ,Raipur. He is a editor of International Journal of wind and renewable Energy USA ,International Journal of mathematical modelling and physical sciences, India, International Journal of Management &Information Technology USA,Society of Engg. & Management Science, IASIR Journal, Georgia, U.S.,International journal of emerging technologies in computational &Applied sciences IJETCAS, International journal of Software & Web Sciences IJSWS,International journal of Engg. Business & enterprises Applications IJEBEA, American International journal of Research in science, Technology , Engg.,& Mathematics,American International journal of Research in formal applied & Natural sciences. American International journal of research in Humanities, Arts & Social science. He has published 39 research papers in various national and international journals.

Dr. Prof. Asha Ambhaikar, Professor and Dean Students Welfare, Kalinga University, Naya Raipur. She has also worked as a Principal in G. H. Raisoni college of Engineering and Management, Amravati (Maharashtra). She has 27 years of Academic experience. She has Guided 3 Ph.D Scholars and 8 undergoing. She has published more than 80 research papers in reputed National and International Journals. She was a chairman Board of studies and Member of Academic Council of Information Technology in Chhattisgarh Swami Vivekananda Technical University, Bhilai(C.G.). She is a member of Editorial Board and Reviewer of various Reputed international journal's and conferences. She is also the member of various professional societies like Life member of IAENG (International Association of Engineers, Hong Kong, IEEE, Indian Society of Technical Education (ISTE), Computer Society of India (CSI), IET, ASDF Computer Science Teachers Association (CSTA), Association for Computing Machinery (ACM), New York, USA, IACSIT (International Association of Computer Science and Information Technology, Singapore.

Member of SDIWC (The Society of Digital Information and Wireless Communication, USA. She has also chaired various National and International Conferences around various countries as a keynote speaker. She has also published two books by Lambert Publication Germany and two Book chapters published in Springer. She has also received a various Awards like: 1. Best Personality of India 2015 at New Delhi, India. 2. Bharat Excellence Award 2015 at New Delhi, India. 3. Outstanding Teacher's Award 2014, 2015 on 5th September, at RCET Bhilai, India. 4. ASDF Global Award for Best Dean (Academics) of the Year 2014 at Bangkok- Thailand on 30th December 2014. 5. ASDF Global Award for Best Professor of the Year 2013 at Pondicherry, India. 6. Best Research paper Award in the year 2009. 7. SPARC Europe Award 2009 for the research paper "Exploring the Behavior of Mobile adhoc Network Routing Protocols with reference to Speed and Terrain Range". She is also guiding Ph.D. Scholars in various universities, Her area of research includes Computer Networking, Mobile Adhoc Networking, Sensor Networks, Data Mining, Distributed system, information systems & security and Cloud Computing etc.