# Blockchain Technology and It's Applications in E-Governance Services

**Om Pal, Surendra Singh**

***Abstract. Blockchain Technology is one of the most popular technologies of present days. This technology has the capability to eliminate the requirement of third party to validate the transactions over the Peer-to-Peer network. Due to various features of Blockchain like smart contract, consensus mechanism, network transactions are completed securely, efficiently and timely. This technology is very useful in many areas including medical, IoT, e-Governance services, smart cities, taxation, supply chain, banking etc. In this paper, we discuss the Blockchain Technology in detail, its data structure, open source platform like Ethereum and Hyperledger, technical aspects of this technology, possible applications of this technology, challenges and limitations in adaptation of this technology.***

***Keywords: Blockchain, Bitcoin, e-Governance, Smart Contract, Merkle Tree, Hyperledger, Ethereum***

## I INTRODUCTION

Blockchain Technology is an emerging and disrupting technology which has the potential to transform the Information Communication Technology (ICT) services at next level. In this technology, transactions are approved and validated with the consensus of majority. No third party is required for validating the transactions. Therefore, it completely eliminates the role of third party. Transactions are saved in form of blocks and these blocks are joined one after another in link list form [2,5,6,7,8,10,11,13,14].

First time in year 2009, Satoshi Nakamoto proposed a digital currency called Bitcoin [17]. In proposed technology, peer members are capable to validate the ownership and expenditure of the Bitcoin digital currency and approval of controlling authority is not required to validate the Blockchain transactions. With consensus of peer members, a block is added in the Blockchain. Each block of Blockchain contains the transaction details along with hash of previous block. By doing so, the ownership and data integrity is maintained in form of block.

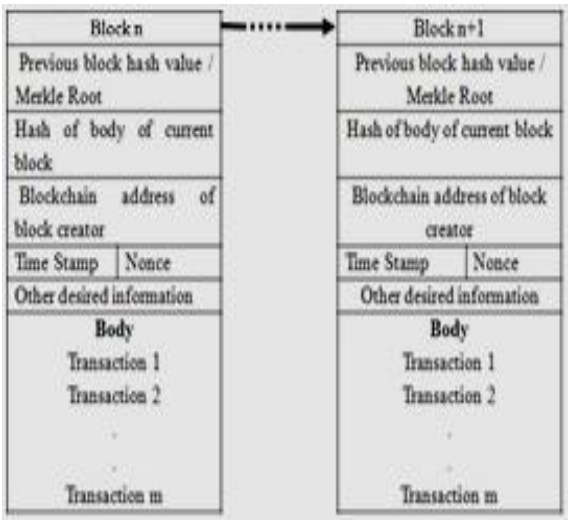


**Fig 1. Block Structure**

Basically, Blockchain Technology is not a self sustained model or technology but it comprises the Mathematics, Cryptography, Economic Model, Consensus algorithms, Peer-to-Peer network, decentralized database to validate the transactions with consensus of the majority of Peer members [3,4, 16, 18, 19]. Blockchain Technology is not a replacement of the Public Key Infrastructure (PKI) but it uses the PKI for identifying or authenticating the peer members for participating in the consensus protocols and Blockchain Technology also uses the PKI to create a new block for Blockchain with immutability [9,12,15].

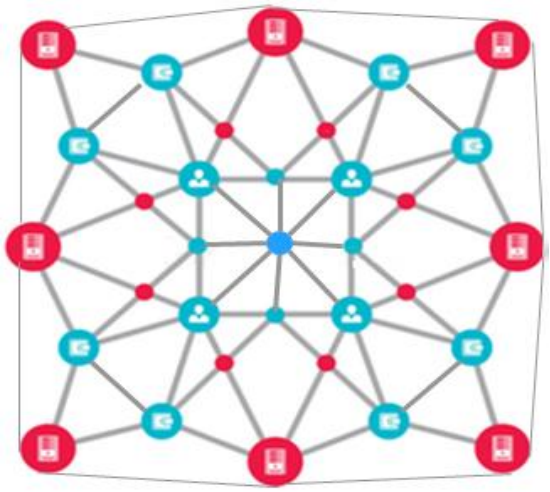

**Figure 2. Blockchain peer-to-peer network**

After success of Blockchain in field of bitcoin digital crypto-currency, now other fields like medical treatment, IoT, e-Governance services, smart cities, taxation, supply chain, e-vehicle etc are ready to apprehend the tremendous growth by use of Blockchain Technology.

**Revised Manuscript Received on November 15, 2019**

**Om Pal***, Ministry of Electronics and Information Technology, Govt. of India. E-mail: ompal.cdac@gmail.com

**Surendra Singh,** Ministry of Electronics and Information Technology, Govt. of India. E-mail: nic.surendra@gmail.com

### A. MERKLE TREE

In Blockchain Technology, blocks containing the series of transactions are connected in link list form. For verification purpose, hash of previous block is connected to the next block in the chain. To verify any transaction, one has to check the hash of the last block of the chain. In case of mismatch, one has to travel the chain in linear time complexity to find the altered block.

Merkle tree is another data structure which provides the facility to find out the altered block quickly. In other words, Merkle tree is a data structure which is used to identify the altered block of Blockchain in log2n time where n is the number of blocks in the Blockchain. Each block of the Blockchain contains the Merkle root which is used to check the integrity of the transactions. Members of the Blockchain store the Merkle tree to find out the modified block quickly. Let Ti is a set of transactions.

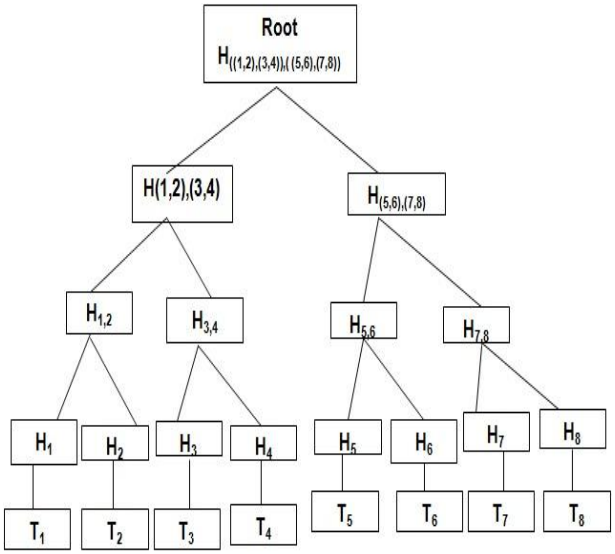


**Figure 3. Merkle Tree**

If any single detail of any transaction is changed then Merkle root would be changed. Without Merkle root it is not possible to prove that no transaction has been tempered. Merkle root is preferable over the hash chain or concated transactions. After adding of each block, Merkle root got changed. After acceptance of new block by the majority of the members of the Blockchain, creator of new block broadcast the new block with hash of the new block over the Blockchain network. After receiving new block each member of the Blockchain update the Merkle root of the blocks which were created by them.

### B. TYPES OF BLOCKCHAIN

Mainly Blockchain is categorized in to two categories: Public/Permissionless Blockchain and Private /Permissioned Blockchain.

(1) Public/Permissionless Blockchain: In this kind of Blockchain, there is no restriction on entry and participation of any anonymous member. Any anonymous member can join the permission less Blockchain with the consensus of the existing members and can participate in the consensus mechanism of adding a new block in the Blockchain. Ethereum is an open source and public Blockchain.

(2) Private/Permissioned Blockchain: In this kind of Blockchain, there are restrictions on entry and participation in the consensus mechanism. In this, head authority is defined in advanced and it may be multi-layered had-authority to manage the Blockchain at multiple layers. In this Blockchain, higher privileges are given to upper layered nodes. Based on the consensus of lower layered nodes, higher layered nodes take the decisions and report to the central authority. Final decisions are taken by the central authority based on the consensus report received from lower level.

### C PROTOCOLS

In distributed environment, the fundamental problem among the network members is to agree on a single data value. To achieve the overall reliability and to intact the integrity of common decision, consensus protocols play a major role in the distributed environment. A consensus algorithm is a process to achieve the agreement on a majority data value among the members of the distributed network. For example, whether all or majority of distributed process agrees to commit a transaction to database or not. In this case, commitment of the transaction to the database is fully dependent on the consensus of the majority. There are various consensus protocols which solve different kind of network issues, some of these are:-

(1) Paxo Protocol
(2) Byzantine Paxo Protocol
(3) Byzantizing Paxos by Refinement
(4) Raft Protocol
(5) Chandra-Toueg Protocol

It is possible that some of the network members may be faulty or unreliable or some members do not have updated local database then fault tolerant consensus algorithms identify these kinds of issues and correct these issues with consensus of the non-faulty members. A fault tolerant consensus algorithm must satisfy the following properties:-

(1) **Termination**: Every member should decide some value.

(2) **Validity:** If majority of members propose the same value 'v' then all members decide 'v'.

**(3) Integrity:** Every member decides at most one value, and if it decides some value then it must have been proposed by some members.

**(4) Agreement:** Every process must agree on the same value.

As discussed above, there are many consensus protocols and these are used according the need of application. In this section we describe Paxo Protocol-

**Paxo Protocol:** Paxo Protocol is one of the basic consensus protocol for distributed environment. In this protocol it is assumed that members do not lie, collude or attempt to subvert the protocol. To overcome the limitations of Paxo protocols there are many other protocols like Byzantine failures and Byzantine Paxos etc. Paxo protocol makes the progress using 2n+1 members where n is the number of members in the network. Protocol survives as long as no more than n number of members fails simultaneously in the network. In Paxo protocol four kinds of roles are assigned to the members. Any member may play more than one role however it depends on the protocol implementation.

Following are the members' roles and other properties of Paxo's protocol:-

**(1) Client**: Any member who requests to the distributed system for an action and waits for a response from the distributed system is called a Client. For instance, a write request of transaction in a distributed database server.

**(2) Acceptor** (Voters): Acceptors or in other words members of the network are divided into groups and each group is called a Quorum. Each Quorum contains at least n+1 members where total number of members in the network is 2n+1. Any message which is sent to acceptors for voting must be sent to each member of at least one of the Quorum. Response of any acceptor is considered only if response of each member of the Quorum is received.

**(3) Proposer:** Proposers are the members of the network and these members advocate the client's request to other members of the network and attempt to convince the acceptors to agree on the client's request. In case of any conflict, proposers play a role of coordinator to resolve the conflict.

**(4) Learner:** Learners are the members of the network and these learners execute the action on client's request in response to agreement made by the acceptors on the proposal. There may be more than one but definite number of rounds before reaching the agreed value. Based on the agreement of acceptors, learner executes the request and sends the response to the client.

**(5) Leader:** Among the proposers, one is called a leader or distinguished proposer. Leader is chosen through voting mechanism and in case of failure during the consensus, another leader is chosen.

**(6) Proposal Number & Agreed Value:** Each proposal has a unique proposal number and attempts are made to define a value v for the proposal which may be accepted or may not be accepted by the acceptors.

**(7) Safety and liveness properties:** In Paxo protocol, following three safety properties are defined and these safety properties are always held regardless of any kind of failures.

- Non-triviality: Only proposed values can be learned by the learners.
- Safety: Two different values cannot be learned by different learners. Same value must be learned by all learners.
- Liveness: If a value is proposed by proposers and a majority of members are non-faulty then learners will learn some value.

Rest of the paper is organized as follows: in section 2, we discussed the Open Source Platform for Blockchain, in section 3, we discussed the Blockchain Technology Use Cases, in section 4, we discussed the challenges and solutions, in section 5, conclusion is given and in last the list of references is given.

## II OPEN SOURCE PLATFORM FOR BLOCKCHAIN

### A. ETHEREUM

Blockchain networks such as Ethereum use 'smart contract' (also known as e-agreement) in lieu of physical agreement among the parties. These e-agreements are executed automatically when specified conditions in e-agreements are met. Blockchain uses digital signature provided by Public Key Infrastructure (PKI) and consensus algorithms to maintain the trust in the network while executing the smart contracts.

To save the business cost, smart contracts can play a major role, for example- Let insurance companies, hospitals, banks and funeral departments all are connected through a Blockchain network then after death of any person, claim settlement can be processed quickly through smart contracts instead of generation and approval of documents at various stages in funeral department, hospital, insurance company etc.

Ethereum is a Blockchain Technology based open source platform which facilitates the development and deployment of decentralized applications. Ethereum is a permissionless and distributed public platform for Blockchain Technology. There are many programming languages which are used to write smart contracts to run on Ethereum platform. Solidity is a high level language which is used mostly to write smart contracts for Ethereum Blockchain.

When smart contracts written in Solidity language get complied then it is converted in to Ethereum Virtual Machine (EVM) byte code. This is like the world of Java where on compilation, byte codes are generated and generated codes run in the Java Virtual Machine (JVM).

### B. HYPERLEDGER

To support the development of Blockchain-based distributed ledger, Linux foundation had started an open source Blockchain project in December 2015. The aim of this umbrella project was to develop the Blockchain-based distributed ledger and its tools to support the business transactions, e-Governance services, supply chain services etc through Blockchain Technology. The major objective of this project is to cross-industry collaboration for development of distributed ledger to enhance the efficiency in terms of performance, reliability, trust etc of various domains like health care system, e-Governance models etc.

**(1) Hyperledger Fabric:** IBM and Digital Asset designed a permissioned Blockchain infrastructure termed as Hyperledger Fabric. Hyperledger architecture facilitates the execution of chaincodes (called Smart contracts in Ethereum), configurable membership services, assignment of roles among the members, access of ledger data and configurable consensus services etc. In this architecture, network members are divided in to two categories (i) Peer nodes and (ii) Ordered nodes. Peer nodes are responsible for execution of chaincode, interface with applications and endorsing of transactions. Ordered nodes are responsible for assignment of roles, authenticity of network nodes, consensus protocols, consistency of the system, delivery of endorsed transactions, resolving of disputes, and management of overall Blockchain structure.

**(2) Hyperledger Composer:** Hyperledger composer is a browser based interface which provides the facility to support the existing Hyperledger Fabric Blockchain structure by assigning the roles to participants, defining the assets which are exchanged among the members, defining secure access of the distributed ledge, defining the Blockchain transactions etc through browser based interface

## III BLOCKCHAIN TECHNOLOGY USE CASES

Blockchain Technology has the potential to transform the existing e-Governance services to a next level. There are many e-Governance services like, agriculture services, banking sector, land record management where the Blockchain can be used as a disruptive technology. The control flow diagram in Blockchain application is as under:

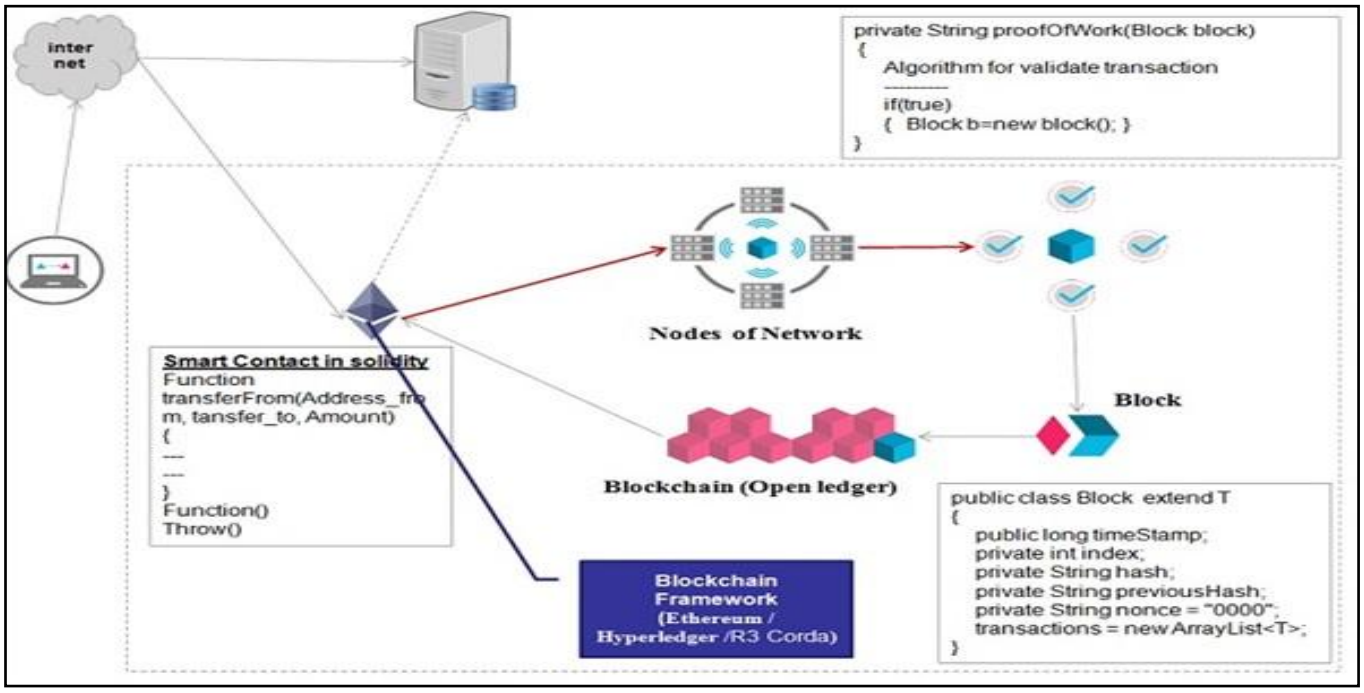


**Figure 4. Control flow diagram for Blockchain application**

To understand the implementation of Blockchain Technology in various sectors, we are going to explain the implementation of Blockchain Technology in e-Tendering process through simple steps.

**e-Tender through Blockchain:** E-tender (electronic tender) is an internet based complete tendering process wherein publishing /advertising tender, receiving bids, submitting tender-related information and opening of the tender after defined timeframe are done online. E-Tender enables firms to be more efficient as paper-based transactions are eliminated and it facilitates for a more speedy exchange of information. E-Tender solution enables the bidders to participate in bidding process at anytime and from anywhere. There is no dependency on the newspapers, couriers and banks therefore; it reduces the efforts and cost of bidding. In e-tendering solution, the bids for various tenders are published on the web site.

In present, in most of the e-Procurement processes the bidders have to enroll themselves on the website by using Digital Signature Device Certificate (DSC) in the form of smart card/e-token etc. The bidders are be able to see the status of the tenders at various stages for which they have submitted quotes and are being also be informed of the status by E-Mail. But in the present bidding process, the bidder does not have an active role in the bidding process. Whole data of bidding process is stored in the central server, therefore it is the expectation of bidders such that bidding data should be stored with honesty, with confidentiality, in hands of trustworthy management, no access of data to any one before opening of the bids etc. Therefore, it is required that e-Tender process must be transparent and trustworthy.

Blockchain Technology is very useful for e-tendering process because its features perfectly suit to enhance the efficiency, trustiness etc of online bidding process. Blockchain Technology enables a company or government entity to share the huge amount of information with large numbers of players in the most efficient, secure and transparent way. Due to transparent feature of Blockchain Technology, the possibility of corruption is nearly eliminated.

By incorporating the Blockchain Technology in the present e-tendering process, various social, technological and process orient benefits may be achieved.

Some of the key advantages of incorporating the Blockchain Technology in bidding process are-

- Ensure that all participants have the same information
- Automate and make more transparent the process (publishing, opening, closing, bid analysis based on defined criteria)
- Quick Publishing, reviewing, auditing, closing and communicating the decisions
- No need to organize Pre-bid conference physically
- No need to call participants physically to open the bid
- No alteration in submitted bids is possible
- Cost saving by doing the process automated
- Speedy execution of bidding steps
- Identity of bidders and the bidding entity is proven with consensus of majority

To ease the incorporation of Blockchain Technology in e-tendering, we divide the process in to the following steps:
(1) Preparing and publishing of the tender documents and other information
(2) Pre-bid conference
(3) Amendments after pre-bid conference
(4) Submission of the bid by the bidders
(5) Opening of the tender
(6) Bid evaluation and award of contract

**Step wise flow process of the e-Tender module is as under:**

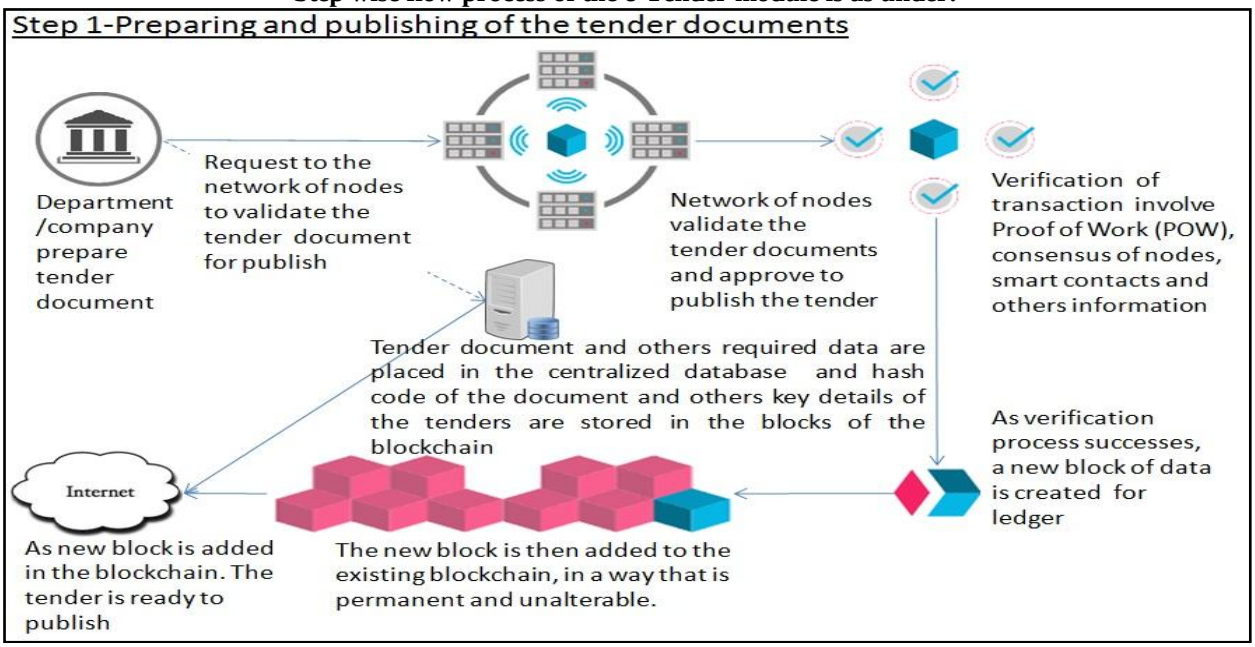


**Figure 5. Step -1**

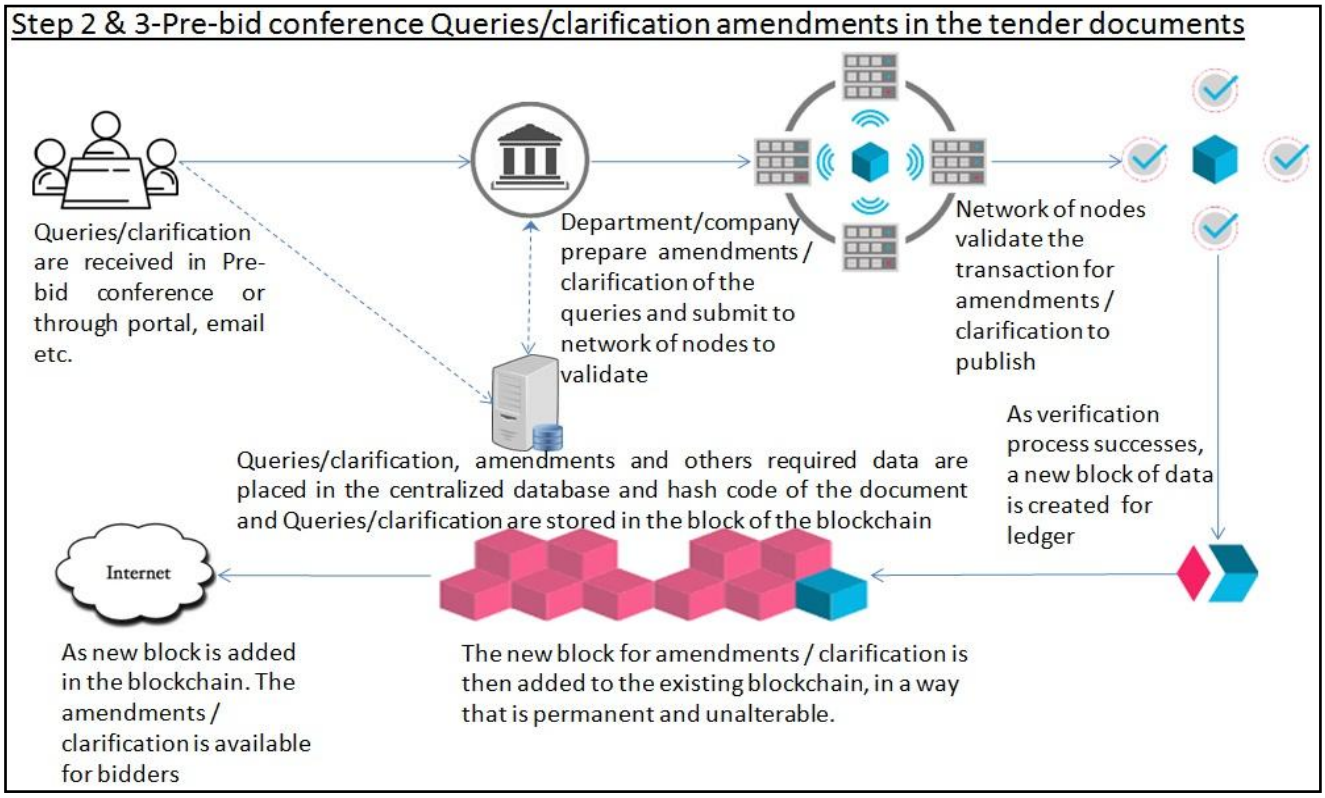


**Figure 6. Step 2 and 3**

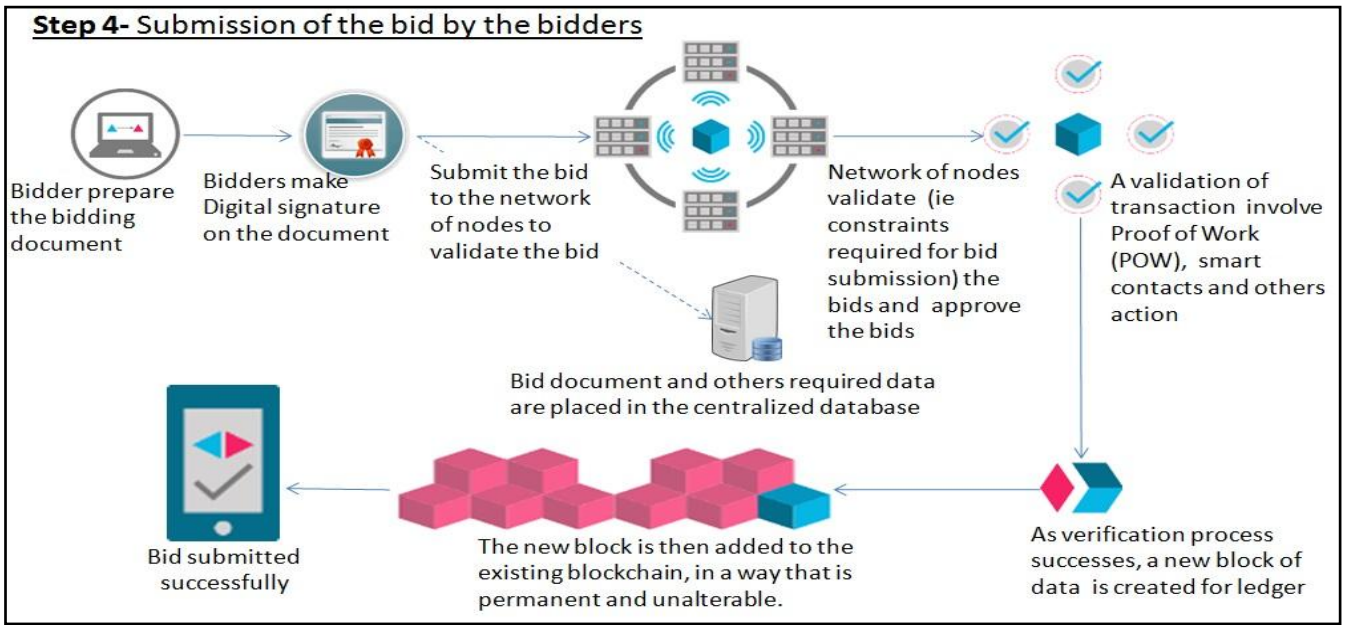


**Figure 7. Step 4**

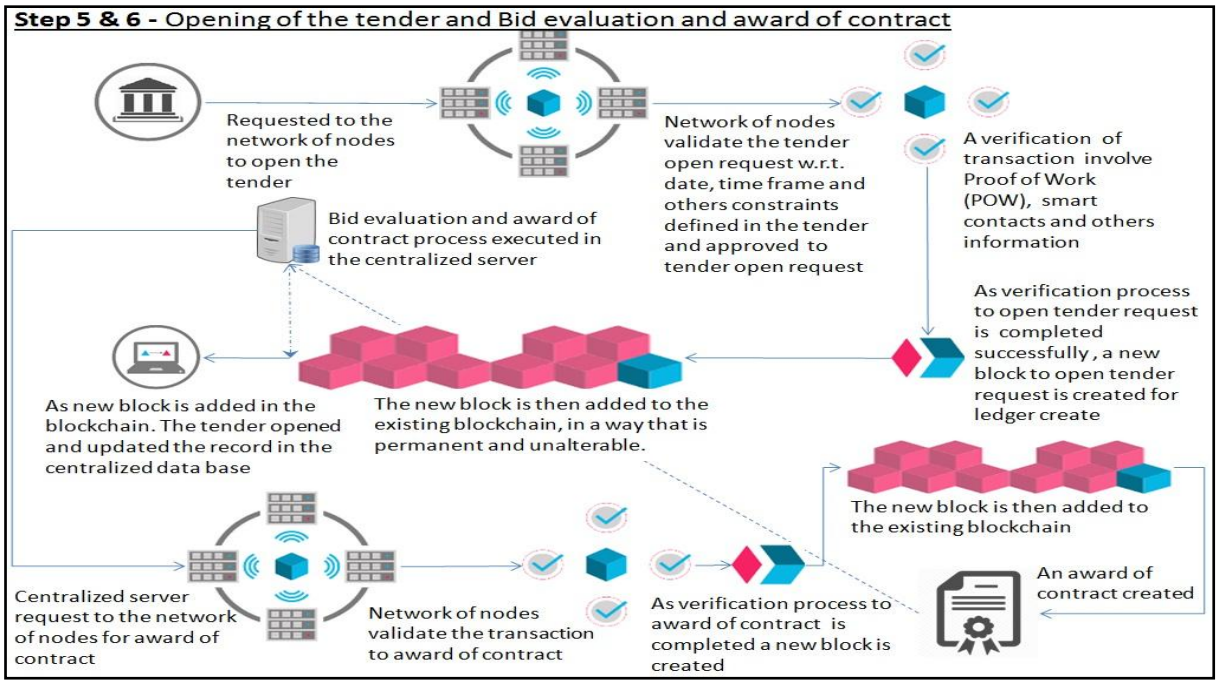


**Figure 8. Step 5 and 6**

**Publishing of Tender:** The firm prepares and uploads the tender documents on online portal for bidding and submits a request to publish the tender. To publish the tender, the request to validate and to approve the received tender is forwarded to all nodes in the network. The nodes in network validate the tender documents and provide the consensus for publishing the tender. Based on the received consensus as per defined criteria for publishing the tender, the tender document is published. After consensus of majority, a transaction to add the new block in the ledger is executed. This new added block contains the hash detail of the uploaded tender document. Subsequently after addition of the new block in the ledger, the tender document is published. Permissioined Blockchain framework suits to the e-tendering process, floating of the tender request to existing nodes, execution of the transactions and publishing of the tender are taken care by existing consensus protocols of the permissioned Blockchain

**Pre-bid conference:** If there are any pre-bid queries from the possible bidder's side then they have to register themselves as a node in the network and subsequently they can raise the pre-bid queries online. After receiving pre-bid queries, network's ordered nodes resolve the queries through consensus protocols and new blocks are added in the ledger.

**Amendments after pre-bid conference:** After pre-bid conference, amendments are done in the publish tenders by adding the new blocks in the ledger. After completion of amendments, bidders are invited to submit their bids online.

**Bid submission:** In this step, bidder prepares the bid documents, makes the digital signature on it and submits it to any ordered node of the Blockchain network.

Majority of the nodes validates the submitted bid and after successful consensus, a new block is added in to the ledger and finally submitted bid is treated as a successful submission.

**Opening of bids:** For opening of the tenders on specified date and time, the concern officer submits the request to nodes of the network; nodes validate the bid opening request with respect to conditions specified in the tender document. New block for bid opening request is added in the ledger.

**Bid evaluation and award of contract:** Opened bids are visible to every node of the network. According the terms and conditions specified in the published tender, bids are evaluated. After evaluation, results are uploaded on the network for the approval of other nodes. After approval by the majority of the nodes, contract is awarded to the winners and transactions are saved in the ledger.

## VI. CHALLENGES AND SOLUTIONS

Every new technology has its own benefits as well as its limitations. Blockchain Technology has also various implementation challenges, limitations, security challenges, economical, regulatory and political challenges. Blockchain Technology is not such a technology which can be adopted without proper precaution.

Security is one of the major challenges in consensus phase of the Blockchain Technology. However, it can be handled smartly if there is proper mechanism for ensuring the confidentiality of the transaction data over the consensus phase of the Blockchain Technology.

On implementation of Blockchain at a large scale, managing the forking issue of the Blockchain may be a major challenge. For example, land records, public services offered by Government, Government policies for hospital, policies of educations all are recorded in form of Blockchain. Now it is possible that new Government advocates the major changes to reform the policies, economic model, service policies then system may need to modify the Blockchain protocols if majority of users have agreed to update the protocol or update the Blockchain software with new agreements among the nodes. In this scenario, problem of forking may arise. However, the forking issue is manageable if majority of nodes agree to update the Blockchain software. After updation of Blockchain software, nodes follow the new consensus rules for adding the future blocks in the Blockchain.

In general, we can categorize the Blockchain challenges in following categories-

(1) Security Challenges and attacks
(2) Efficient implementation and selection of Consensus Protocols
(3) Fork problem
(4) Scaling problem
(5) Regulation and Blockchain Standards

Scaling is one of the challenge in Blockchain Technology. Proper scaling strategy must be planned in advanced as day by day size of data, messages among the nodes for synchronization may be increased. Due to addition of new nodes and new services in the Blockchain network, complexity of the system is increasing day by day.

In Blockchain Technology, a lie becomes truth if majority of the nodes are faulty in the system. This attack is called a '51% attack'. If more than 50% nodes are agree to commit the malicious transactions then there is no solution to stop this attack in the permissionless Blockchain. However in permissioned Blockchain this kind of attacks may be resolved by upper level nodes or central authority. In permissioned Blockchain, upper level nodes or central authority is not bound to execute the consensus of the lower level nodes.

There are various consensus protocols, according the need of the system, a proper consensus protocol must be selected. Regarding regulation problem, a regulatory mechanism may be set up to encounter any regulation kind of issue.

## V . CONCLUSION

In this paper we discussed various features of Blockchain Technology like its data structure, smart contract, open source platforms for Blockchain, consensus mechanism, network transactions etc. We discussed various application areas of this technology where it can be applied and we also discussed the implementation mechanism of Blockchain Technology in e-tendering. Further we discussed various challenges and limitations in adaptation of this technology. Finally we conclude that Blockchain Technology has huge potential to transform the existing digital services in to new era where efficiency of services, customer satisfaction, trust, security, privacy, cost saving etc may be enhanced un-doubtfully.

## REFERENCES

1. A. Lei, Cruickshank, H. Cao, P. Asuquo,. P. Chibueze, A. Ogah, And Z. Sun, "Blockchain-Based Dynamic Key Management For Heterogeous Intelligent Transportation Systems," Ieee Internet Of Things Journal, 2017.
2. I-C. Lin, And T-C Liao "A Survey Of Blockchain Security Issues And Challenges," International Journal Of Network Security, Vol.19, No.5, 2017.
3. C. Fischione, "Lecture Note On Consensus Algorithms", Royal Institute Of Technology –Kth Stockholm, Swedene.
4. Paxos Consensus Protocol (Https://En.Wikipedia.Org/Wiki/Paxos_(Computer_Science)).
5. S. T. Aras, And V. Kulkarni "Blockchain And Its Applications – A Detailed Survey," International Journal Of Computer Applications (0975 – 8887), Volume 180 – No.3, 2017.
6. S. Huckle, R. Bhattacharya, M. White, And N. Beloff, "Internet Of Things, Blockchain And Shared Economy Applications," International Workshop On Data Mining In Iot Systems, Sciencedirect, Procedia Computer Science, 2016.
7. J.H. Park "Blockchain Security In Cloud Computing: Use Cases," Challenges, And Solutions, Symmetry, 2017.
8. A. Azaria, A. Ekblaw, T. Vieira, "A. Lippman: Medrec: Using Blockchain For Medical Data Access And Permission Management," Presented In Proceedings Of 2nd International Conference On Open And Big Data, 2016.
9. R.H. Hsu, J. Lee, T. Quek, And J. Chen ,"Reconfigurable Security: Edge Computing-Based Framework For Iot, [Cs.Cr], 2017.
10. The Future Of Public Service Identity: Blockchain, Report Of M/S Accenture, 2017.
11. I-C. Lin, And T. C. Liao, " A Survey Of Blockchain Security Issues And Challenges," International Journal Of Network Security, Vol.19, No.5, 2017, Pp.653-659.
12. S. Huh, S. Cho And S. Kim, "Managing Iot Devices Using Blockchain Platform," Presented In Icact2017, 2017.
13. Survey On Blockchain Technologies And Related Services, Nomura Research Institute, Japan's Ministry Of Economy, Trade And Industry (Meti), 2016.
14. Z. Zheng, H.N. Dai, And S. Xie, " Blockchain Challenges And Opportunities: A Survey," International Journal Of Web And Grid Services, 2017.
15. T. Salman, M. Zolanvari, A. Erbad, R. Jain, And M. Samaka, " Security Services Using Blockchain: A State Of The Art Survey," Ieee Communications Surveys And Tutorials, 2018.

16. G. Zyskind, O. Nathan, And A. Pentland, "Decentralizing Privacy: Using Blockchain To Protect Personal Data," Presented In Proceedings Of Ieee Cs Security And Privacy Workshops, 2015.
17. S. Eskandari, D. Barreray, E. Stobertz, And J. Clark, "First Look At The Usability Of Bitcoin Key Management," Arxiv:1802.04351 [Cs.Cr], 2015. Http://Dx.Doi.Org/10.14722/Usec.2015.23015.
18. N. Fotiou, G. Polyzos, "Decentralized Name-Based Security For Content Distribution Using Blockchains," Ieee Conference On Computer Communications Workshops (Infocom Wkshps), San Francisco, Ca, 2016, Pp. 415-420.
19. O. Pal, B. Alam, V. Thakur, Surendra Singh "Key Management For Blockchain Technology", Ict Express Journal, August 2019. Doi: Https://Doi.Org/10.1016/J.Icte.2019.08.002

## AUTHORS FROFILE

**Om Pal** received MS by Research degree in field of Cryptography from Indian Institute of Technology, Bombay and Ph.D. in field of Cryptographic Key Management from Jamia Millia Islamia, University, New Delhi. Presently he is a Scientist in Ministry of Electronics and Information Technology, Government of India. His research interest include Blockchain Technology, Cryptology, Network Security, Quantum Computing and e-Governance. One can contact to Dr. Om Pal at ompal.cdac@gmail.com

**Surendra Singh** received B.Tech in Computer Science & Engineering from Bundelkhand Institute of Engineering & Technology (BEIT) Jhanshi (UP). Presently he is a Scientist in Ministry of Electronics and Information Technology, Government of India. His research interest include Blockchain Technology, Big Data, AI, IoT and e-Governance. One can contact to Mr. Surendra Singh at nic.surendra@gmail.com.