STUDY PAPER ON BLOCKCHAIN IN TELECOM
(DLT Ecosystem for UCC and its possible Use Cases)

CONTENTS

1. EXECUTIVE SUMMARY

This white paper outlines the recently implemented Distributed Ledger Technology (DLT) by the telecom service providers in India and exploring the possibility of using this DLT system for other use cases. The paper also highlights how blockchain technology can be used by the Indian Telecom Service Providers (TSPs) in various segments of their business and to achieve operational efficiency.

Blockchain is one of the technologies which organizations, across the sectors, are exploring to find out how they can leverage this it to its true potential for the benefit of their businesses.

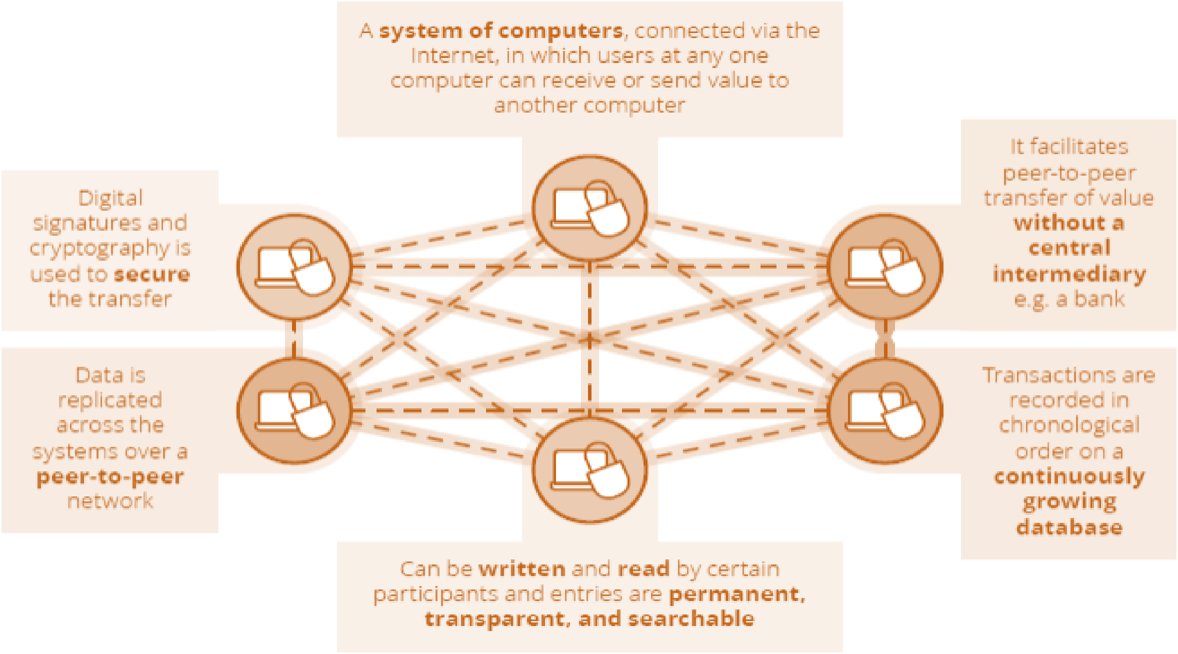
The TSPs are always in a constant transformation of their network and adopt the latest technologies to lower their cost and to increase their revenue by providing varying products and services to their customers. Blockchain is one such Distributed Ledger Technology (DLT), which, not only have the potential to improve the operational efficiency, but, also to open new revenue streams for the TSPs.

There could be multiple ideas and approaches to use Blockchain by the TSPs. One such approach has been adopted by the TSPs to implement the TRAI Telecom Commercial Communications Customer Preference Regulations, 2018 which regulates the commercial communication business and curb the unsolicited commercial communications (UCC).

The report discusses the benefits of this DLT system and how the TSPs can adopt the DLT system to improve their other business processes, regulatory compliances and a possible growth in their revenue.

2. INTRODUCTION TO BLOCKCHAIN:

Blockchain is a consensus-driven, peer-to-peer network of secure and decentralized nodes forming a distributed ledger, with each node having simultaneous access to transactions updated in the ledger.


A system of computers, connected via the Internet, in which users at any one computer can receive or send value to another computer
Digital signatures and cryptography is used to secure the transfer
It facilitates peer-to-peer transfer of value without a central intermediary e.g. a bank
Data is replicated across the systems over a peer-to-peer network
Transactions are recorded in chronological order on a continuously growing database
Can be written and read by certain participants and entries are permanent, transparent, and searchable

Source: Blockcube

Blockchain technology includes the following components to permit effective collaboration among players in a business network:

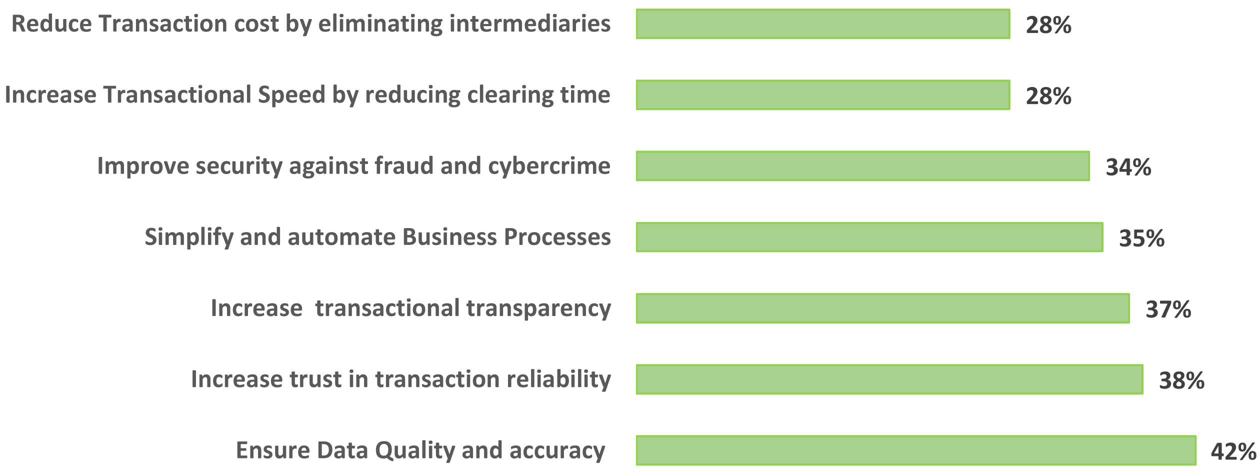
a. Shared ledger – An append-only distributed system of records shared across the business network that provides transaction visibility to all involved participants.
b. Smart contract – Business terms embedded in the transaction database and executed with transactions so that the appropriate contracts are executed when a transaction occurs.
c. Privacy – Transactions are reliable, authenticated and verifiable.
d. Trust – Transactions are endorsed by relevant participants.
e. Transparency – All participants in the network are aware of all transactions that impact them.

The blockchain architecture enables participants to share a ledger that is updated every time a transaction occurs through peer-to-peer replication. Cryptography is used to help ensure that network participants see only the parts of the ledger relevant to them and that transactions are reliable, authenticated and verifiable. Blockchain also allows the contract for asset transfer to be embedded in the transaction database determining the conditions under which the transaction can occur. Network participants agree how transactions are verified through consensus or similar mechanisms. Oversight, compliance and audit can be part of the same network.

Blockchains can help TSPs to operate much more effectively within their business network because they support consensus, provenance, immutability and finality. Potential benefits for TSPs include:

a. Time savings-Transaction time is reduced from days to near instantaneous.
b. Cost removal-Administrative overhead and cost of intermediaries are reduced or eliminated.
c. Enhanced data quality-Data accuracy is maintained during all transactions.
d. Reduced risk-Tampering, fraud, Data Privacy issues and cybercrime are addressed/reduced.
e. Increased trust-Shared processes and recordkeeping are visible to all concerned parties.
f. Reduction/elimination of disputes-Absolute transparency is established as the process executes

Globally, many connectivity service providers (CSPs) are exploring the use cases of blockchain technology. As per the survey conducted by IBM, more than one-third of the CSP executives are considering or actively engaged with blockchains, particularly, in the light of ensuring data quality and accuracy. As per this study of IBM, the below figure depicts the identification done by the CSPs regarding numerous ways that blockchain could support their enterprise strategies.

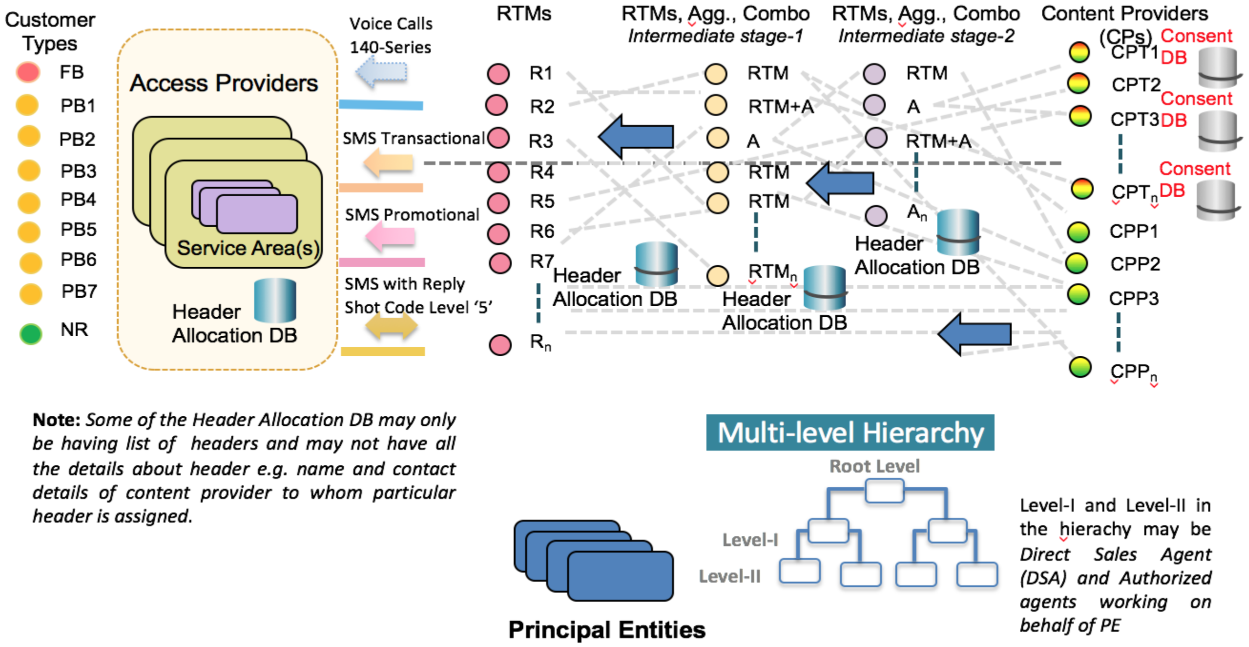


Source: IBM survey

In India, however, the very first use of blockchain is driven by TRAI defined Regulatory framework to regulate the Commercial Communication services and curb the menace of unsolicited commercial communications being received by the customers.

3. REGULATORY DRIVEN BLOCKCHAIN IN INDIA:

In 2018, TRAI decided to come out with a new regulatory framework to curb the Unsolicited Commercial Communications (UCC). UCC has become a major cause of inconvenience for telecom users and also qualifies as breach of privacy of individuals. Below is the graphical representation of the UCC ecosystem:



Note: *Some of the Header Allocation DB may only be having list of headers and may not have all the details about header e.g. name and contact details of content provider to whom particular header is assigned.*

Level-I and Level-II in the hierachy may be *Direct Sales Agent (DSA) and Authorized agents working on behalf of PE*

Source: TRAI

To curb the UCC, the Telecom Commercial Communications Customer Preference Regulations (TCCCPR) was notified by TRAI in July 2018. Following are the salient features of the Regulations:

a. Commercial Communications should take place using registered headers assigned to the senders for the purpose of commercial communications.

b. In case, any subscriber is sending commercial communication, telecom resources of the sender may be put under usage cap and if the subscriber continues sending such communications then all telecom resources of the sender may also be disconnected.

c. Access Service Providers are required to develop an ecosystem with the functions e.g. facility for registering preferences, recording consents, revocation of consent, sender registration, complaint handling mechanism etc.

d. Access Provider to provide modes e.g. SMS, calls, IVRS, USSD, Mobile App, Web portal free of cost to the subscribers to register, modify or de-register preferences.

e. Access Providers to register entities, senders, content templates, consent templates and assign the headers, header roots to the senders.

f. Access Providers to ensure that commercial communication takes place only and only through headers assigned to the registered senders.

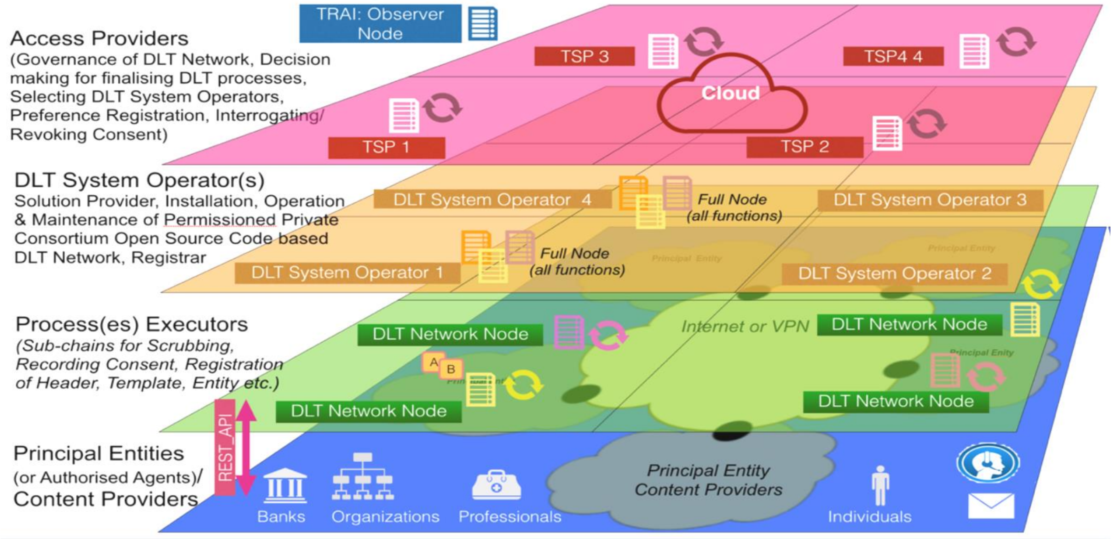
g. Access provider to deploy a system to perform functions e.g. recording of preferences, consents, complaints, to detect non-compliances and take immediate action to ensure compliance etc.

h. Access providers to adopt DLT with permissioned and private DLT networks for implementation of the systems prescribed in CoP.

i. Access Providers to establish Distributed Ledgers for complaints with requisite functions, process and interfaces etc. This system will record complaints and report any violation of regulations, to record details about the complaints (e.g. telephone number, headers, date & time of occurrence of UCC etc.

One of the significant features of this new regulation is the adoption of Distributed Ledger Technology (a Blockchain technology) to create a new eco-system for commercial communication business and to curb the UCC.

Amongst the broad spectrum of Distributed Ledger models, with different degrees of centralization and different types of access control, TRAI mandated the Access Providers to adopt the DLT with permissioned and private DLT networks. Below is the Architecture for implementing the UCC ecosystem based on DLT:



TRAI: Observer Node
Access Providers
(Governance of DLT Network, Decision making for finalising DLT processes, Selecting DLT System Operators, Preference Registration, Interrogating/ Revoking Consent)
TSP 3
TSP4 4
Cloud
TSP 1
TSP 2
DLT System Operator(s)
Solution Provider, Installation, Operation & Maintenance of Permissioned Private Consortium Open Source Code based DLT Network, Registrar
DLT System Operator 4
Full Node (all functions)
DLT System Operator 3
DLT System Operator 1
Full Node (all functions)
DLT System Operator 2
Principal Entity
Process(es) Executors
(Sub-chains for Scrubbing, Recording Consent, Registration of Header, Template, Entity etc.)
DLT Network Node
Internet or VPN
DLT Network Node
A
B
DLT Network Node
DLT Network Node
REST_API
Principal Entities
(or Authorised Agents)/ Content Providers
Banks
Organizations
Professionals
Principal Entity Content Providers
Individuals

This mandated DLT ecosystem for UCC offers a technology-driven solution to improve the regulatory procedures and delivery of the commercial communication process. It allows various stakeholders in the ecosystem to share the customer information and transaction histories in a secured manner over a distributed infrastructure. The participants in the ecosystem can be certain regarding the authenticity of the data being captured in the system. Various business entities (termed as principal entities) will also have surety regarding the safety and security of their data along the delivery chain. This system also provides capabilities to the TSPs to control and manage commercial communication more effectively and meet their regulatory obligations apart from improving the Quality of Experience of their customers by curbing the UCC. Benefits of this DLT system driven regulatory framework for various stakeholders in the UCC ecosystem are outlined below:

Customers:

a. DLT provides the capability to define categories for customer's preferences in more granular manner and allow the customers to convey their interest area along with their preferred day/time of the day to receive any promotional communications.
b. It empowers the customers to know the purpose and scope of their consents and facilitates proper verification from the customers before recording their consents.
c. It implements the choices of the customers quickly and also records their verified consent in the system in a short time period so that customers can start receiving commercial communications as per their given preferences and consents.
d. The DLT system enables faster resolution of the complaint since all the TSPs are part of the chain, it becomes easy to share and access the ledger for the complaints and hence faster resolution.

Access Providers:

a. Reduction in the financial disincentives as the solution can control the UCC from Unregistered telemarketers in more efficient and effective manner, thus, a reduced number of UCC from their customers.
b. The solution provides quick control of the participants by the TSPs in the UCC ecosystem
c. The DLT technology provides the advantage of economy of scales, thus, more participants being on-boarded in the system, more benefits for the TSPs.
d. Increase in the efficient and effective management of the tele-marketers by on-boarding them quickly and provides an opportunity to generate revenue from this process.
e. The system mitigates the chances of victimization of the customers on account of false complaints, thus avoid the loss of business opportunities.
f. It also helps in improving the overall QoE for the TSPs' customers, which is a win-win situation.
g. The DLT system also provides an opportunity to test and develop new processes around the eco-system.

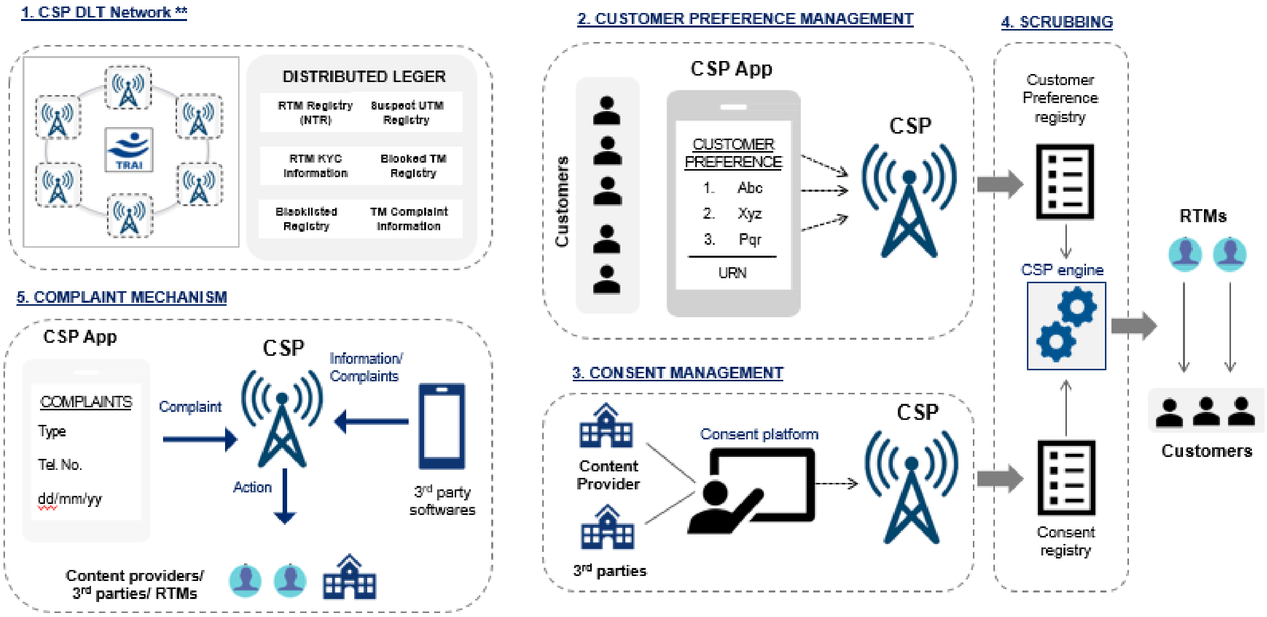
Telemarketers:

a. The new DLT system reduces the chances of flouting the regulatory provisions thus reducing the chance of blacklisting of the telemarketers (TMs).
b. It provides edge to the genuine telemarketers over those creates a nuisance for the customers as the system doesn’t leave any loopholes for such TMs.
c. It helps the TMs to enhance their business volumes since the system provides flexibility to the customers towards receipt of commercial communications and hence increase the chance of more customers opting to receive such communications in their leisure time instead of opting for fully block mode.
d. It also helps the TMs to avoid loss of business opportunities to the UTMs since the DLT system is capable to detect and mitigate the UTM activates.

Business Entities:

a. The DLT system provides a reach to the target customers thus enhancing the business opportunities.
b. The system keeps the business entity’s information safe and secure manner while sharing carrying out the activities or functions required to ensure compliance with the Regulations.
c. It enhances their brand positioning by allowing them to opt for Header of their choice which to be used to send commercial messages
d. The system connects these entities directly with the TSPs thus ensures transparency in the whole ecosystem which is beneficial for the business entities and TSPs alike.

Components of the DLT system deployed by the TSPs:



Source: Wipro

Thus, **the adoption of Blockchain technology-based Distributed Ledger System to create a new UCC ecosystem caters to the regulatory requirements and may create more transparent system. It may also enhance the business opportunities for all the participants alike apart from protecting the interest of the customers.** The completion of the eco-system based on the TCCCPR, 2018 is in its advance stage and then we would be in a position to assess the effectiveness of the DLT based solution in curbing the UCC and how it benefits the TSPs and other business entities.

4. EXPLORING THE OTHER USE CASES OF THE DLT SYSTEM:

The previous chapter highlighted the unique use case of the blockchain technology implementation through regulations and its possible benefits to various stakeholders. In this chapter, we would be exploring the possibility of using the said DLT system in other business and operational issues of the TSPs.

As discussed earlier, the DLT system adopted and implemented through the TCCCPR, 2018 is permission based private DLT networks. **One of the unique advantages of the blockchain based systems is that they are interconnected decentralized infrastructure and new modules can be added almost like in the form of plug and play. Thus, with certain modification in the infrastructure, one may think of utilizing this newly built system for other use cases**. Below are few use cases which could be achieved with certain degree of modification in this DLT system:

a) Mobile Number Portability (MNP):

TSPs have recently rolled out a revised MNP procedure as per the TRAI MNP Regulations. These MNP rules enable the customers to port out in lesser time now. A unique porting code (UPC) is required to be generated for a subscriber who requests for MNP. In the revised MNP rules, this UPC will be generated by the MNP service providers (MNPSP) only, post validation of the subscriber's account from the donor operator. During validation, several conditions have to be met. For instance, in the case of postpaid mobile connections, the subscriber has to have cleared 'outstanding dues' towards the existing telecom service provider as per the normal billing cycle. The user should be an active subscriber on the present operator's network for at least 90 days. Furthermore, TRAI notes that there should be no ongoing request for change of ownership of mobile number, nor there should be any pending contractual obligation to be fulfilled by the subscriber as per the exit clause provided in the subscriber agreement. Other pre-required regulations include the porting of the mobile number is not prohibited by the court of law, and that the mobile number sought to be ported is not sub-judice.

TRAI mandates that porting to other operator within the same circle will be executed within two working days and if porting is for another circle, it will be executed within four working days. While porting of corporate numbers, the porting request shall be forwarded to donor operator, only for the purpose of verification of the authorization letter submitted by the corporate entity, before the process is initiated. Also, there is no change in the porting timeline for national MNP i.e. porting to different service area altogether. Subscribers, who wish to cancel their port-out request, can do so within 24 hours of document submission.

The fundamental idea behind change in the MNP rules is to create a more transparent and faster ecosystem which enables the subscribers to port from one TSP to another in lesser time period. The rules enable the third party (MNPSP) to check for the eligibility criteria from the donor TSP before generating the UPC.

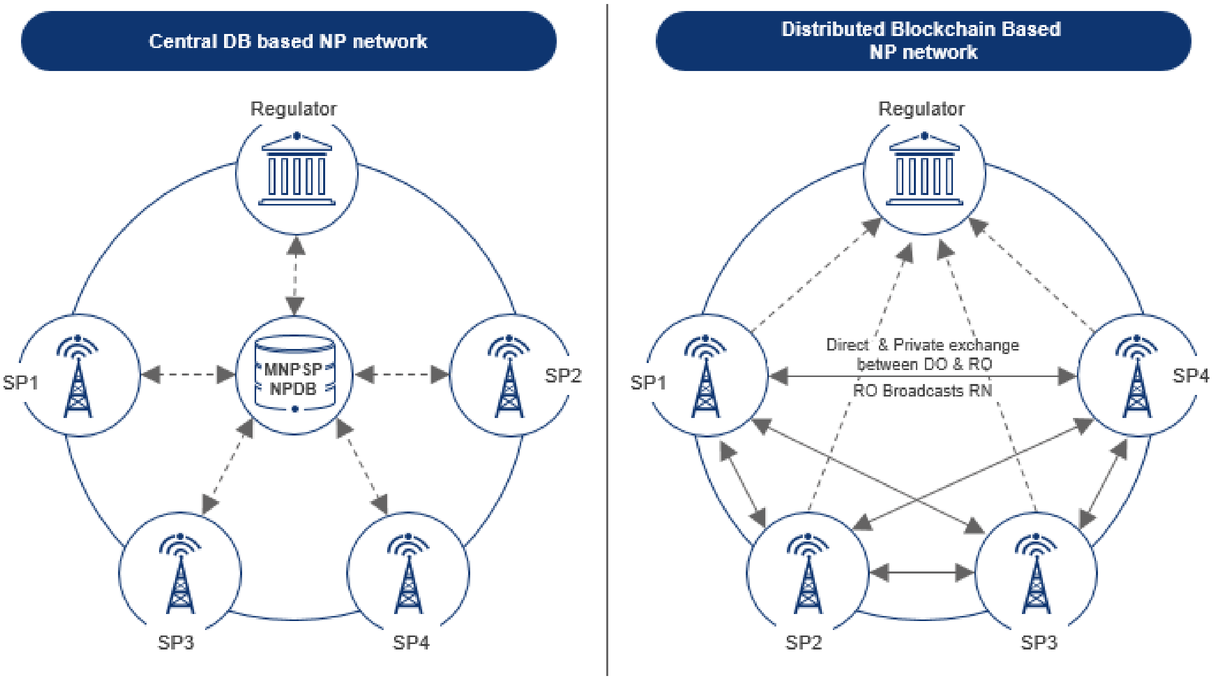
The **TSPs can extend their DLT system to cater to the MNP functionality. TSPs are already connected amongst themselves through the chain. Two MNPSPs can be made part of the DLT system and then the flow of information and procedures as mandated in TRAI regulations can be carried out through this DLT system. The advantage of permissioned blockchain is that every TSP can control the access of the data they are putting in the system to distribute**. The whole idea behind MNP is the change in the Logical Routing Number (LRN) of a subscriber when the subscriber switches from one TSP to another TSP and then broadcast this LRN to all the TSPs so that the call routing can be changed for this subscriber based on the new LRN.

Further, **the query-based mechanism where the MNPSP need to query from the donor regarding the eligibility of any subscriber for MNP can be done through this DLT system wherein the TSPs need to integrate their existing Subscriber Management System/Billing systems etc. and the entire process remains automated with the advantage of blockchain been infused into this.** Use of DLT system will give similar advantages (e.g. Transparency, safety & security of data, faster response, record keeping) as it is giving in the UCC ecosystem. Further, through the DLT, the TSPs can settle their billing with the two MNPSPs.

However, the above would require change in the MNP guidelines and also in the TCCCPR, 2018 to allow the TSPs to use this permissioned private DLT system for other services and also to create nodes for the two MNPSPs.

Further, **in future, the role of the MNPSP in the MNP ecosystem can be reduced or even eliminated altogether by using efficient blockchain technology. With blockchain technology, information and value can be exchanged in a secure and transparent manner while the porting process itself can be simplified, all without an MNPSP.** By making use of smart contracts, the Number portability process can become fully automated by enforcing contract terms and service level agreements (SLA) that the TSPs agree between them or mandated by

TRAI. This will not only help to complete the porting process faster, but a secure and transparent exchange of value such as prepaid balances, unpaid bill amounts and apportionment of charges or costs between TSPs as agreed is also possible. **The blockchain platforms can provide the secure and tamper-proof exchange of information between DO (Donor Operator) & RO (Recipient operator) to share KYC details directly with porting out user's consent. Between DO, RO, regulators and users, the process dependencies can be monitored in real-time as the process flows and statuses are registered in the ledgers and become fully auditable**. The above process can be put in with some changes in the current DLT system already deployed by the TSPs for TCCCPR. Suggested approach for the future MNP process i.e. without MNPSP is as given below:

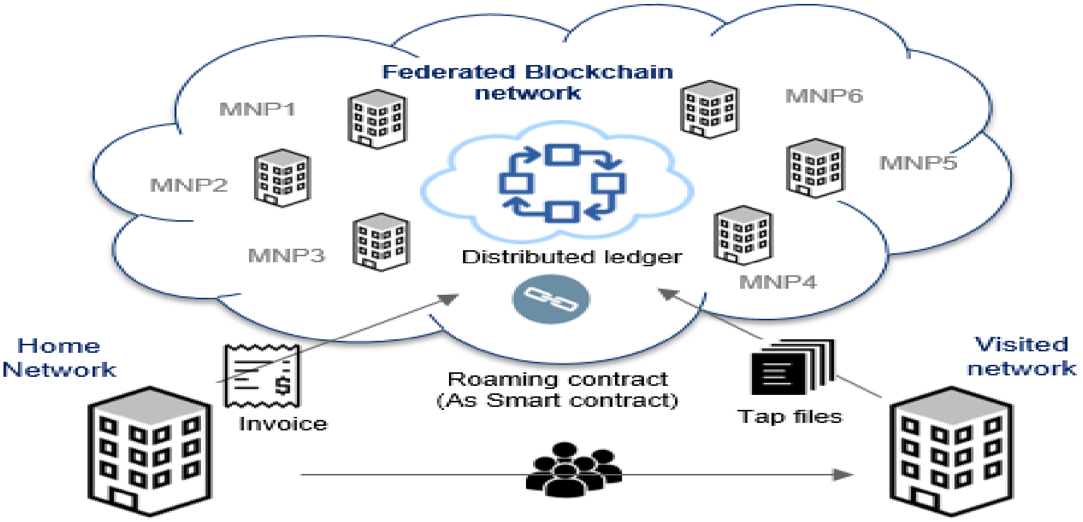


Source: Wipro

b) Roaming settlement Issues:

By creating a permissioned blockchain between every pair of the operators who have roaming arrangements, all the billing settlements and reconciliation efforts can be streamlined. While, the TSPs need to explore whether they can use the same DLT system (since all Domestic TSPs are connected with each other) and whether through varying cryptic functionality amongst two TSPs, their roaming arrangements can be streamlined through the use of this DLT system, one cannot deny the fact that the features a DLT bases system provides, can actually be utilized in roaming settlement issues.

Currently, roaming agreements and intermediaries like clearing houses increase the cost of operations that are eventually passed on to the subscriber. These agreements could be replaced with automated Smart Contracts. Based on the Smart Contract rules, the charges and payment terms & conditions are set.



Source: Wipro

Roaming settlement is done based on the records maintained by the TSPs. Call data records (CDR) are shared at varying time intervals by the network providers. But, there is always a risk of fraud and disputes from all parties involved, as well as delays and issues in payments. Roaming frauds typically are because of two characteristics:

i. The time for detection of the fraud is longer due to delays in the exchange of data between network operators
ii. The time to respond to the fraud is longer due to lack of coordination and control in the systems.

A **blockchain network, where each roaming operator would feed the details of roaming call or data session in almost real-time, could increase the efficiency of the settlement process as well as make a big dent in typical roaming frauds.** With blockchain, both the home and visited operators have a better visibility into the subscriber's usage information. **When a mobile user gets on the roaming network, the visited operator determines the user from the home operator via subscriber information exchange. The subscriber is then authenticated on the blockchain network. When a duplicate mobile user attempts to connect, the user can be easily identified and flagged during the authentication phase.**

International Roaming: Though, the current DLT system of the TSPs being used for the TCCCPR does not connect to any foreign TSP, this system can be enhanced w.r.t Foreign TSPs as well. There has been issues wherein generating and executing the Transferred account procedure (TAP) file takes time resulting in cases on fraud. This may be avoided if the agreements with foreign TSPs can also be brought in the system of DLT. Each TSPs can create their individual DLT system, having their foreign TSP roaming partners as part of the system.

Many Connectivity Service Providers across the world are exploring the use of blockchain based systems in roaming settlements. For example: Telefónica is evaluating how it can apply blockchain to roaming and believes the technology can usefully be deployed in other areas as well, including digital identity, the supply chain and tokenization. Deutsche Telekom is deploying blockchain to simplify roaming agreements. Globe Telecom, which operates one of the largest mobile, fixed-line and broadband networks in the Philippines, has already demonstrated considerable interest in blockchain technology, with a particular focus on solutions intended to address the settlement of roaming costs. This, Globe believes, could lead to settlements being conducted in real time, without needing offline reconciliation. Vodafone Group is also exploring the use of blockchain for roaming with the aim to leverage blockchain to enable more efficient, instantaneous and frictionless inter-operator processes.

Indian TSPs, with their existing DLT system in place, can explore the way they can utilize this existing system to cater their roaming settlement requirements amongst themselves and later on may explore the possibility of adding their other roaming partners (Internationally) to achieve real-time settlements without going through offline reconciliation process.

c) Wi-Fi Roaming Authentication & KYC:

COAI has proposed a Wi-Fi model to DoT which ensures interoperability between the TSPs/ISPs/VNOs through Wi-Fi roaming between service providers. Through this model, various Hotspots created by TSPs/ISPs/VNOs will be unbundled to eliminate silos and walled gardens and the existing standalone Wi-Fi Hotspots of all the TSPs/ISPs can immediately be made the part of the nationwide seamless common interoperable system. This model also envisaged that the subscriber will be able to use the data plan taken from any one of the TSP/ISP in the Wi-Fi Hotspots deployed by other TSPs/ISPs without purchasing a new plan every time to use the Wi-Fi service of other TSPs/ISPs. There will be no need for the subscriber to have Multiple interactions with the franchise, retailer etc.

In this model, two aspects are defined for the authentication and charging I.e. i) through OTP based authentication with voucher-based charging ii.) Through SIM based authentication with charging from prepaid/post-paid accounts of the subscribers. This model further prescribes for the CDR based reconciliation process between the parties.

In this case, there will be multiple ISPs and TSPs who will be under the agreement for providing the Wi-Fi roaming services and might require the clearing house for the settlement process between them. This will increase the operational cost for the small ISPs. Blockchain can work as a robust solution in this scenario, providing real time settlement between the parties and avoiding any type of Clearing House entity.

Further TSPs are already using the DLT systems for the TCCCPR, the present system can be enhanced w.r.t Wi-Fi based roaming service as well, by opening the authentication and Charging API's for the current DLT system.

d) Tower Sharing Management:

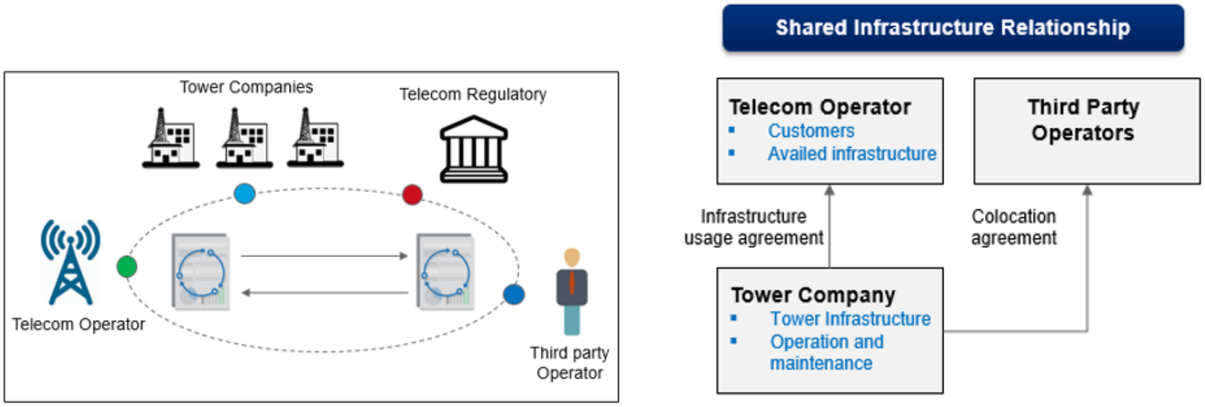
Today we see the global telecommunication market transform towards a digital, interconnected and shared economy. Telecom infrastructure is one of the prime enabler and also a barrier for the expansion of telecom services. Therefore, sharing of infrastructure by the telecom operators has become the need of hour as operators try to lower their respective investments. The intent of regulators also is to increase the mobile network coverage area within the geography and optimize the utilization of telecommunication infrastructure.

Since it is an activity that involves cooperation between the operators with infrastructure provider (Tower Company or TowerCo), a tower sharing agreement or contract is required. The TowerCo takes over ownership and operation of the passive infrastructure and assumes responsibility for the performance and maintenance. The operator purchases the capacity to use the passive infrastructure from the TowerCo on a usage or fixed capacity basis. The cost associated with re-planning existing networks requires commercial agreement, follow up on operations and tracking expenses as per tower contract. There are many associated challenges in creation, management and adherence to the contract. There are no uniform procedures and policies, and lack of implementation of central policies continue to be a challenge. In addition, reconciliation and settlement issues between tower companies & telecom operators is very common due to manual or Excel-based operations.

Further, with the TRAI recommendation (subject to acceptance of DoT) to enhance the scope of Infrastructure providers and allowing them to own, establish, maintain and work all such infrastructure items, equipment, and systems which are required for establishing Wireline Access Network, Radio Access Network (RAN) and Transmission Links, the above highlighted issues will only get inflated.

We believe that a solution based on blockchain that allows TSPs to collaborate efficiently with tower companies and build better working relationships. With the help of DLT/ blockchain solution we can achieve:

i. **Negotiation on Terms & Conditions, Approvals & Signatures captured digitally**
ii. **Workflow of contracts is captured with the timestamp by counterparties**
iii. **Commercial agreement, payment and fine terms captured as per contract**
iv. **Templatization of the tower contracts & agreements via Smart Contracts**
v. **Post agreement, digital trail of transactions, activities & expenses are captured**
vi. **The application will ensure increased speed, trust, improved visibility and auditability.**



Source: Wipro

Also**, the Blockchain process can be further enhanced to eliminate the role of any third-party intermediaries by having direct smart contract based blockchain solution between TSPs and tower companies.**

e) KYC of M2M SIMs:

As per the current DoT M2M Guidelines on KYC for issuing the M2M SIMs to entity/organization providing M2M Communication services under Bulk Category, following instructions are to be followed:

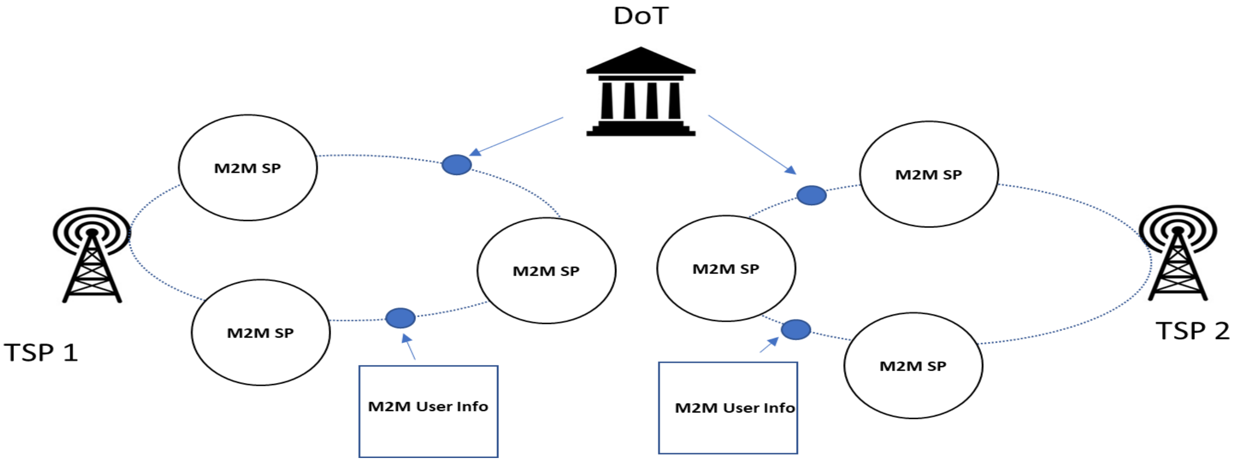
i. The details of all the customers of M2M services i.e. Physical custodian of machines fitted with SIMs, should be maintained by entity /organization providing M2M Services.

ii. Up-dated information regarding a) Details of M2M end device i.e. IMEI, ESN etc. b) Make Model, Registration No. etc of machines (i.e. Cars, utility Meters, POS etc) and c) Corresponding Physical custodian name and address should be made available online through some web interface to Licensee by entity/organization providing M2M Services.

iii. Regarding maintenance of database/records of the end-users of the SIM cards by the Licensee, the procedure as prescribed for bulk connection shall be followed.

The KYC mechanism for the M2M services can be used through the DLT system, wherein all the M2M Services can be registered by their respective TSPs providing them the M2M SIMs through the DLT system. Further, M2M service providers can put in the information about their customers on the DLT system as the real-time update. The access of the same will be to the respective TSPs while the access can also be given to DoT and the TERM cells.

KYC Mechanism for M2M SIMs



f) Cyber Security and Data Privacy:

Cyber-attacks have become increasingly targeted and complex due to more sophisticated pieces of malware being leveraged and the increasing threat of professional cyber organizations. These cyber criminals are attempting to steal valuable data, such as intellectual property (IP), personal identifiable information (PII), health records, financial data, and are resorting to highly profitable strategies such as monetizing data access through the use of advanced ransomware techniques or by disrupting overall business operations through Distributed Denial of Service (DDoS) attacks.

Blockchains could potentially help improve cyber defense as the platform can secure, prevent fraudulent activities through consensus mechanisms, and detect data tampering based on its underlying characteristics of immutability, transparency, auditability, data encryption & operational resilience (including no single point of failure).

Data Access & Disclosure: Today, if an attacker gains access to a blockchain network and the data, this does not necessarily mean the attacker can read or retrieve the information. Full encryption (hashing) of the data blocks can be applied to data being transacted, effectively guaranteeing its confidentiality, considering the latest encryption standards are followed.

Immutability: Blockchain technology can be regarded as a secure technology, from the point of view that it enables users to trust that the transactions stored on the tamper-proof ledger are valid. The combination of sequential hashing and cryptography along with its decentralized structure makes it very challenging for any party to tamper with it in contrast to a standard database. This provides organizations using the technology with assurance about the integrity and truthfulness of the data.

Right to be Forgotten: There is also need to take care of the data privacy issues, for e.g. implement the right to be forgotten in a technology that guarantees that nothing will be erased is an interesting challenge for which, fortunately, there are multiple solutions. This can be done by encrypting the personal information written in the system, to ensure that, when the time comes, forgetting the keys will ensure that sensitive information is no longer accessible. Another possibility is to focus on the value of blockchain to provide unalterable evidence of facts by writing the hash of transactions to it, while the transactions themselves are stored outside of the system. This maintains the integrity of transactions, while enabling the ability to erase the transactions, leaving only vestigial traces of forgotten information in the blockchain. This is how the DLT system is working for the TCCCPR.

Traceability: Every transaction added to a public or private blockchain is digitally signed and timestamped, which means that organizations can trace back to a specific time period for each transaction and identify the corresponding party (via their public address) on the blockchain.

No Single Point of Failure: Blockchains have no single point of failure, which highly decreases the chances of an IP-based Denial of the Service (DDoS) attack disrupting the normal operation. If a node is taken down, data is still accessible via other nodes within the network, since all of them maintain a full copy of the ledger at all times.

The above characteristics is already built in the current DLT system of TCCCPR and would also be key feature for the other use cases of the Telecom as well.

5. INTERNATIONAL SCENARIOS:

Below are some of the examples from International service providers who are exploring various use cases of Blockchain technology.

Telefonica – has associated itself with IBM to enable Blockchain in their endeavors. They are utilizing IBM's blockchain platform to log information collected by different networks when routing international calls. The intent is to improve reliability and transparency of information collected. The operators working in the routing of these calls will have an access-based authentication on a decentralized platform that will own this information. That will provide access to real-time tracing of calls to allow for correct billing processes between operators.

Deutsche Telecom – Through their subsidiary T-Systems is working on a German Blockchain Ecosystem (GBE) and will offer organizations with a platform for blockchain networks3. This will make T-Systems the first European digital service provider to launch a blockchain as a service marketplace. This digital marketplace will allow customers to map different applications using blockchain. For example – The above mentioned marketplace will allow participating organizations to map their total value chain using Blockchain. This will enable a visible digital display of an org's supply chain making operations faster, transparent and more cost effective. Inherently, this will enable trade, invoices, payments etc through the native benefits of blockchain in the 1st place. This significantly reduces fragmentation along the value chain as well.

Vodafone – This global telecom giant is part of a group of mainstream organizations working in collaboration with IBM, utilizing Blockchain to bring clarity and efficiency to transformed processes. IBM has christened this project as trust your suppliers – essentially connecting the suppliers of any organization through a common Blockchain. The supplier first will need to prove itself through background and verification checks in the Blockchain network and hence transact with the intended organization.

AT&T – similar to other players in the telecom circle, ATT is utilizing Blockchain to automate and transform their supply chain processes that impacts their products – handsets and network equipment. Any sort of product returns, upgrades/other activities that impacts the various components of the supply chain is being managed through the Blockchain route. The various suppliers are joined throughout the Blockchain network that allows security and transparency. What they are also doing is integrating IOT with the traditional Blockchain solution to customize it to suit ATT's requirements. ATT has already announced the ability of their customers to pay their telephone bills using Bitcoins.

Airtel – Telecom organizations have started to leverage Blockchain to enable micropayments for music, mobile games, and other value added services. Airtel, offers digital wallets that enable customer-to-customer payments. Through Blockchain handling the transactions, Airtel ensures that the digital wallets are more secure with ID verifications.

6. CONCLUSION:

India witnessed its very first adoption of blockchain use case driven by the regulatory framework. It has been two years since the regulation was notified by TRAI and TSPs have come a long way to understand the use of the DLT based system and are able to see the benefits of the same in the new UCC ecosystem.

While, blockchain technology is still evolving and TSPs are exploring the use cases of the blockchain to streamline their businesses and operational issues, one cannot deny the fact that the regulatory driven DLT based UCC ecosystem has opened a path for this emerging technology in the telco’s world and it is only a matter of time when the TSPs start creating the blockchain based system in their various functionality to achieve transparency, faster system, better record keeping and to manage their various contracts.

Current, blockchain system can be enhanced for using it in various use cases such as in MNP, Roaming, Public Wi-Fi Roaming, KYC of M2M SIMs and Authentication, Tower sharing Management etc.

The benefit of blockchain based systems are real and it is important to make efforts to understand the business models around blockchain system and how the same can be utilized by the TSPs in their various IT, Network infrastructure partner/vendor management and above all, to improve the Quality of Experience for their customers.

7. REFERENCES:

i. https://www.trai.gov.in/sites/default/files/RegulationUcc19072018.pdf

ii. https://www.ibm.com/downloads/cas/LQJMPYRN

iii. Telecom on Blokchain: TeLedgers CONNECTING TRUSTLESSLY (by Blockcube limited (http://blockcube.co/)

iv. https://www.accenture.com/_acnmedia/PDF-101/Accenture-Blockchain-Wheres-the-Value-for-Telecoms.pdf

v. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/ITU-Asia-Pacific-CoE-Training-on-Distributed-Ledger-Technologies-(Blockchain)-Ecosystem-and-Decentralization/TRAI%20presentation.pdf

vi. https://www.mondaq.com/india/telecoms-mobile-cable-communications/732200/the-telecom-commercial-communications-customer-preference-regulations-2018

vii. https://gadgets.ndtv.com/telecom/news/trai-mobile-number-portability-mnp-revised-process-all-you-need-to-know-2149527#:~:text=TRAI%20notes%20that%20porting%20to,for%20the%20corporate%20mobile%20connections.

viii. https://www.trai.gov.in/sites/default/files/RegulationsMNPEng13122018.pdf

ix. https://www.wipro.com/en-IN/blockchain/blockchain-applications-for-telecom-industry-and-regulatory-authorities/

x. Blockchain & Cyber Security by Deloitte