BLOCKCHAIN'S IMPACT ON TELECOM IN INDIA

Abstract

This article describes the current telecom ecosystem's workflow for the commercial distribution of advertising messages. Here, we contrast the current telecom ecosystem workflow with a blockchain-based workflow to solve the unsolicited commercial communication (UCC) problem. Blockchain technology and its effects on telecom are explained. We are talking about the technological and legislative approaches to deal with the spam problem. The discussion is limited to the Indian context.

CS Puja Shree Agarwal
Assistant Professor
Hierank Business School
Noida
drcacspujashree@gmail.com

INTRODUCTION

One of the world's largest wireless marketplaces, India has experienced rapid expansion in the telecom sector, with more than 1 billion active subscribers. The affordable call and short message rate have made it one of the most affordable methods for achieving potential customers and selling services. However, telemarketing or bulk messages can be a reason for fraud and breach of privacy. Phone numbers of potential subscribers are leaked and used for spam.

In our telecommunication ecosystem, there are telecom operators, telemarketers, subscribers, and principal entities generating content for promotion and leveraging telemarketers to reach potential customers and the regulators.

Today blockchain technology is a revolution in various fields. However, the revolution comes with different types of challenges. In this article, we discuss blockchain technology's potential applicability to telecom laws. We specifically talk about the rising issues with unsolicited commercial communication (UCC, sometimes known as spam), which is sent by SMS and phone calls in India. When a subscriber chooses not to receive a commercial communication, it is known as unsolicited commercial communication. Even this is a big challenge for telecom operators and lawmakers despite various existing measures. Here we are focusing on the blockchain-based solution to solve the UCC problem in India which has been incorporated in the Unsolicited Commercial Communication Telecom Commercial Communications Customer Preference Regulations (TCCCPR'18) and announced on 18 July 2018. With the generalization of blockchain technology in different fields, we believe this can improve our regulatory process of telecom.

LEGAL INITIATIVE

The centralised organisation in charge of overseeing business communication is Telecom Regulatory National Do Not Disturb (NDND) registry: In 2010 this was introduced by the Telecom Regulatory Authority of India (TRAI). Mobile subscribers were allowed to register themselves for NDND. Telecom service providers had to match their data with the central database of TRAI Regulatory Authority of India for NDND. This was a 7 days long process after registration. Unless they specifically opted out by submitting their information to the DND register, all subscribers were by default opting in to receive commercial messages. There was a mandatory online registration process for telemarketers with fee charges. After registration telemarketing IDs are assigned to the telemarketer. Some fraudulent telemarketers accessed the registry data of subscribers through this process. After that TRAI fixed the per-day and monthly message limits and mandated to detection of bulk messages for telecom operators. There were higher charges for bulk messages. After registration of the complaint of the telemarketer by the customer for violation of user preferences, there was an increased security deposit required by the telemarketer for ID.

TECHNOLOGICAL INITIATIVE

Numerous smartphone apps are offered that assist in managing and filtering spam from the SMS inbox. Many of these systems employ rule-based filters that classify messages based on their textual promotional content and mark them. The use of mobile

identifying codes by telemarketers makes it possible to filter promotional messages. On the Google Play store for Android, numerous third-party programs let users manage block lists and prohibit particular SMS senders. Both Google messages and Apple's default SMS software (iMessage) offer the option to block spammers using the settings without the use of any external programs. Despite various initiatives, consumer dissatisfaction continued and complaints were not resolved.

CURRENT WORKFLOW OF PRINCIPAL ENTITIES, TELEMARKETERS, AND TELECOM OPERATORS

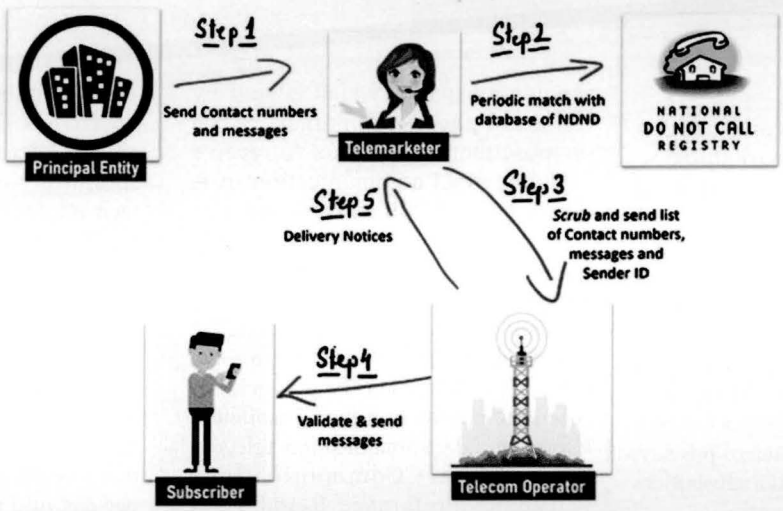
The different stakeholders in the telecom system exchange information back and forth. Restaurants, corporates, online shopping platforms, and various

The use of mobile identifying codes by telemarketers makes it possible to filter promotional messages

service providers are principal entities that create promotional campaigns with the help of telemarketers. Every principal entity should have a sender ID like the domain name of the website in the SMS system. The sender ID is displayed to the receiver SMS for brand recognition. It must be registered by a telemarketer who is a partner in the creation of the promotional campaign. As per the TRAI Regulations, it is mandatory to register six-character alphanumeric sender ID as SMS Header.

The principal entity gives the telemarketer access to the list of phone numbers of the target people for the promotional campaign. The telemarketer then scrubs (removes the DND-registered numbers from the initial list) and sends the final list and promotional message to a partner telecom operator for sending promotional SMSs under a registered sender ID. The telecom operator i.e. Original Service Provider (OSP) divides the list into regional circles as per the registration of mobile numbers and sends them to the circle operator Terminating Service Provider (TSP) for further transmission to subscribers. TSPs have the opportunity to scrub the phone numbers once more. See the following diagram for this process.

FIGURE 1



A subscriber can register the complaint of unsolicited messages with the help of the mobile application of TRAI or telecom operators' website or SMS-based system. The TSP) verifies this with the relevant National Do Not Disturb (NDND), Original Service Provider (OSP), and telemarketer. In the case of default, they have levied fines. This process takes approximately seven working days.

There are many challenges like the breach of privacy, collusion among parties of the telecom system, making matching names fraudulent sender IDs, etc., and the UCC problem is not fully resolved. The issue of UCC has persistently been difficult for controllers, versatile supporters, and telecom administrators the same. The TRAI revised the UCC guidelines in India and moved from a twofold method of setting client inclinations; for example, full block of limited time content, and negative limitations on special substance, to empowering incomplete blocks.

BLOCKCHAIN WORKING

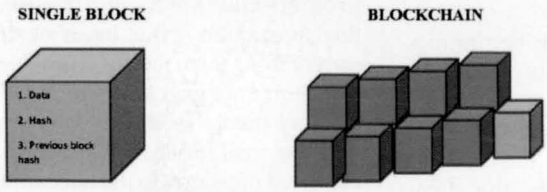
Blockchain, a revolutionary new emerging technology introduced with Bitcoin cryptocurrency, is a distributed ledger technology (DLT) that may be programmed to record and track anything of value. In this technology, all parties' transactions are shared and synchronized in this network of peers or computer nodes. The transaction information is the same for millions of computer nodes and can be verified. Hence it is called Distributed Ledger Technology (DLT) and has a higher level of transparency.

Block in Blockchain

Every block in the blockchain contains data, hash, and previous block hash. This technology records

all transaction information or transaction data in a new block with a time stamp when the transaction takes place. It means that for every transaction new block is created. Hash is a computer program containing a unique reference number like a person's fingerprint, which is unique in and of itself. The blocks in the chains are attached, storing the information of the hash of their previous block. As a result, tracking the hash code is a one-in-a-billion possibility.

FIGURE 2



As a result, anytime information in a block changes, it is not rewritten inside the block. Instead, a new block with the previous block's hash will be created. It means alteration is not possible. It is no longer the same block if the hash changes. This helps in tracking and storing the data. But the changing of hash does not guarantee full security. Nowadays, technology is very advanced, and lakhs of hashes can be calculated per second. Hence anybody can effectively tamper with the hash and technically recalculate the hashes of all other blocks to regain the validity of the Blockchain.

Proof for Security

Blockchain is a decentralized consensus technique that does not rely on a central authority or a third party for validation. Every new transaction must be approved by at least 51per cent of the network's blockchain. There are

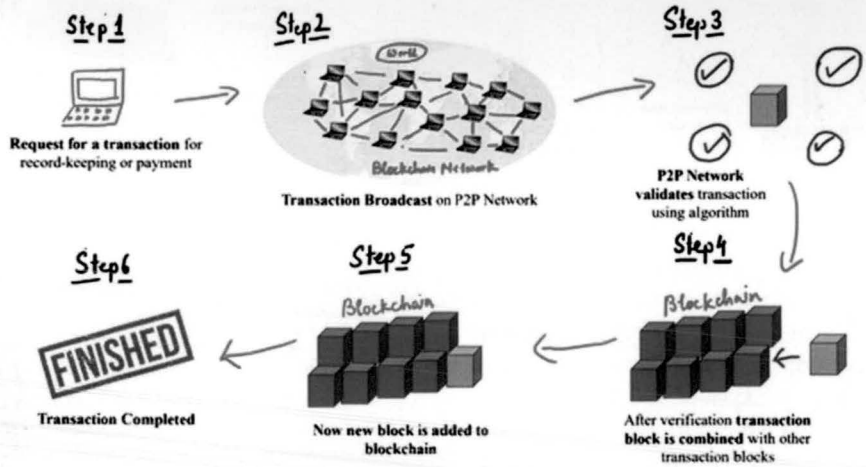
- Proof of work (PoW)
- Proof of stack (PoS) and
- Proof of validity (PoV)

consensus methods in blockchain. For the security of every block, there is a hashing mechanism with PoW in the Peer-to-Peer (P2P) network.

Hashing and PoW provide the security of blocks. It's a mechanism that makes the building of new blocks take longer. Anyone can join the blockchain's peer-to-peer network. This decentralized system is intriguing because it allows us to engage with our personal data in real time without needing intermediaries. When a new block is formed, there is a creation of a cryptographic puzzle. The puzzle is solved to check the validity of the block. If it verifies, the new block would be added permanently to the chain. If it doesn't get solved, then the block gets rejected. Therefore if anyone wants to tamper with one block, he has to tamper with all the blocks in the chain, redo the PoW for each block and take control of more than 50 per cent of the P2P network. Only then the tampered block is accepted by everyone else. That is extremely hard to achieve. Thus, it ensures reliability of the data. The data is highly secure inside the block.

FIGURE 3

BLOCKCHAIN WORKING



On a blockchain, the participants can build a distributed ledger to share information about transactions. These transactions are validated by a consensus mechanism. With communal verifiability, this technology develops trust, transparency, and accountability among the participants. A blockchain that has been given privileges to a group of entities is known as a permissioned blockchain. In this case, these entities are responsible for the governance of blockchain and verification of all transactions over the network.

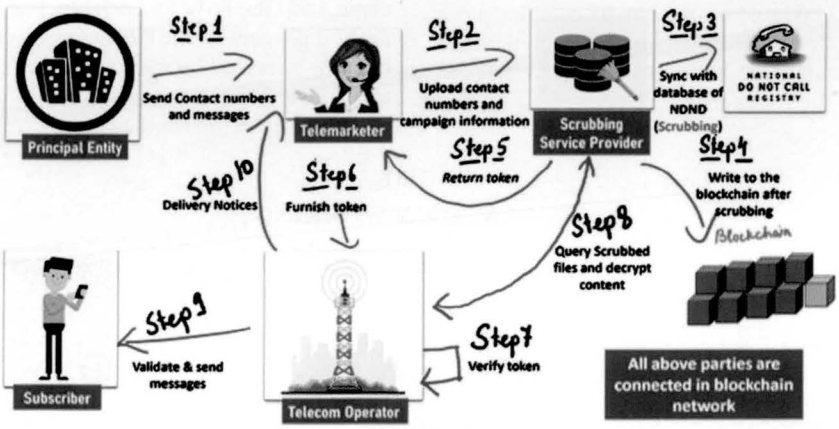
BLOCKCHAIN-BASED WORKFLOW IN THE TELECOM ECOSYSTEM

DLT-based blockchain application is viewed as a way to deal with issues including subscriber data leaks, spam messages, fraud penalties and legal infractions, among others. The register and preferences system currently in use is an example of how the regulator is involved in the day-to-day operations yet lacks traceability, enforceability for violations, etc. The block chain-based approach would plan for telecom operators to handle the majority of the duties, with the regulator simply responsible for enforcing laws. Strengthening the entire ecosystem

and bringing all participants together are the main requirements. Now there is a block chain network in the telecommunication ecosystem among all parties of the system like telecom operators, telemarketers, subscribers, principal entities, regulators and third-party service providers. With the new entry with the help of a mobile app or website or telecom operator's customer care in the NDND registry, a transaction starts in the block chain network. Every participant has a copy of the transaction on a real-time basis (the time-consuming process issue is resolved). For the security and privacy of subscribers' information in the NDND registry there is the use of cryptography and the hash technique of block chain. Information cannot be leaked to unauthorized telemarketers or parties. The block chain network manages the header registration (Sender ID) process. It keeps the record of the mapping of sender IDs with principal entities (the fraudulent sender ID issue is resolved). The telemarketer is required to register the content of the promotional message. With the help of block chain after verification and registration now principal entity has valid ownership of its brand sender ID and message content.

In this process in the beginning principal entity sends data of contact numbers and registered approved promotional message content to the telemarketer with the sender ID. Telemarketer scrubs the data independently or does this task with the help of a third-party service. This process initiates the transaction on block chain also after scrubbing of data. The third-party sends the scrubbed data in form of a token to the telemarketer. The telecom operator may receive the produced token directly from the telemarketer or through third-party services. Before sending the promotional SMSs to the subscribers in their network, the telecom operator validates the token, scans the matching list of phone numbers to send the promotional SMS, and validates the transaction status by, if desired, re-scrubbing them locally. The telecom operator(s) engaged in the message delivery finally send a delivery report with the total number of successfully delivered messages to the telemarketer who started the campaign, which can be utilized for later billing.

FIGURE 4



CONCLUSION

In the existing workflow, there are many challenges faced by all stakeholders of the telecom ecosystem which can be resolved by the implementation of the proposed blockchain-based workflow. Using block chain mechanisms will improve subscriber experiences, regulatory governance, and the telecommunication ecosystem. India is one of the largest telecom market. India has billions of subscribers requiring a smooth flow of messages without any threats and problems with the privacy and security of personal information. In the future, this can be improved over time with new challenges. This block chain-based process has been a part of our Indian regulations. Our Government has announced the requirements for the implementation of the block chain process in the telecommunication ecosystem. It is hoped that this will take place successfully. MA

References

1. *Telecom Regulatory Authority of India - Government of India. https://trai.gov.in*
2. *COAI. Cellular Operators Association of India. https://www.coai.com/about-us*
3. *True Caller. SMS Categorizer. https://support.truecaller.com/hc/en-us/ articles*
4. *Microsoft. SMS Organizer - an Android app. https://www.microsoft.com/enus/garage/profiles/sms-organizer/. Online*
5. *Bharat Sanchar Nigam Limited (BSNL). 2018. Draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/ default/files/ BharatSancharNigamLtd28062018.pdf. Online*
6. *Shefali S. Dash and I. P. S. Sethi. 2009. National Do Not Call Registry in India: A Step towards Restricting Unsolicited Telemarketing Calls. In Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance (ICEGOV '09). Association for Computing Machinery, New York, NY, USA, 335–340. https: //doi.org/10.1145/1693042.1693112*
7. *Rishi Ranjan Kala. 2018. COAI to Trai: Keep norms on spam calls on hold for now. https://www.financialexpress.com/industry/coai-to-trai-keep-norms-onspam-calls-on-hold-for-now/1248705/.*