Telechain: Bridging Telecom Policy and Blockchain Practice

Sudheesh Singanamalla
sudheesh@cs.washington.edu
Microsoft Research India
Bengaluru, Karnataka, India
University of Washington
Seattle, USA

Apurv Mehra
apmehra@microsoft.com
Microsoft Research India
Bengaluru, Karnataka, India

Nishanth Chandran
nichandr@microsoft.com
Microsoft Research India
Bengaluru, Karnataka, India

Himanshi Lohchab
himanshi.lohchab@tanla.com
Tanla Platforms Limited
Hyderabad, Telangana, India

Seshanuradha Chava
anuradha.chava@tanla.com
Tanla Platforms Limited
Hyderabad, Telangana, India

Asit Kadayan
asit.kadyan@gmail.com
Telecom Regulatory Authority of India, Government of India
New Delhi, India

Sunil Bajpai
sunilbajpai@gmail.com
Telecom Regulatory Authority of India, Government of India
New Delhi, India

Kurtis Heimerl
kheimerl@cs.washington.edu
University of Washington
Seattle, WA, USA

Richard Anderson
anderson@cs.washington.edu
University of Washington
Seattle, WA, USA

Satya Lokam
satya@microsoft.com
Microsoft Research India
Bengaluru, Karnataka, India

ABSTRACT

The use of blockchain in regulatory ecosystems is a promising approach to address challenges of compliance among mutually untrusted entities. In this work, we consider applications of blockchain technologies in telecom regulations. In particular, we address growing concerns around Unsolicited Commercial Communication (UCC aka. *spam*) sent through text messages (SMS) and phone calls in India. Despite several regulatory measures taken to curb the menace of spam it continues to be a nuisance to subscribers while posing challenges to telecom operators and regulators alike.

In this paper, we present a consortium blockchain based architecture to address the problem of UCC in India. Our solution improves subscriber experiences, improves the efficiency of regulatory processes while also positively impacting all stakeholders in the telecom ecosystem. Unlike previous approaches to the problem of UCC, which are all *ex-post*, our approach to adherence to the regulations is *ex-ante*. The proposal described in this paper is a primary contributor to the revision of regulations concerning UCC and spam by the Telecom Regulatory Authority of India (TRAI). The new regulations published in July 2018 were first of a kind in the world and amended the 2010 Telecom Commercial Communication Customer Preference Regulation (TCCCPR), through mandating the use of a blockchain/distributed ledgers in addressing the UCC problem. In this paper, we provide a holistic account of of the projects' evolution from (1) its design and strategy, to (2) regulatory and policy action, (3) country wide implementation and deployment, and (4) evaluation and impact of the work. While the scope of the work presented in this paper is in the context of the UCC problem in India, we believe that the approach can be generalized to adopt blockchain based solutions to improve regulatory processes in other contexts and countries. We hope this account will serve as a useful case study for the stakeholders of the telecommunications ecosystem and regulators, and motivate countries across the world facing similar challenges to consider the viability of the technology, be convinced to establish it, continue efforts at addressing active research challenges, and scale the technology from our experiences.

CCS CONCEPTS

• **Applied computing** → *Computing in government*; • **Social and professional topics** → **Governmental regulations**; *Computing / technology policy*.

ACM Reference Format:
Sudheesh Singanamalla, Apurv Mehra, Nishanth Chandran, Himanshi Lohchab, Seshanuradha Chava, Asit Kadayan, Sunil Bajpai, Kurtis Heimerl, Richard Anderson, and Satya Lokam. 2022. Telechain: Bridging Telecom Policy and Blockchain Practice. In *ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies (COMPASS) (COMPASS '22), June 29-July 1, 2022, Seattle, WA, USA.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3530190.3534820

COMPASS '22, June 29-July 1, 2022, Seattle, WA, USA

ACM ISBN 978-1-4503-9347-8/22/06.
https://doi.org/10.1145/3530190.3534820

1 INTRODUCTION

Despite several efforts by telecom operators, Internet businesses, operating system and application developers, regulators, the problem of spam in communication networks (Internet and cellular) continues to be a global challenge. India has seen tremendous growth in the telecom industry with more than a billion active subscribers (1197.87 million) making it one of the largest wireless markets in the world [9, 74]. The low costs for short message service (SMS) (0.085 INR/SMS for bulk advertisers or 0.001 USD/SMS [17]) and calls has made it one of the most cost effective ways to reach potential customers and sell services and products using telemarketing.

More than 30 billion SMSs are sent in India every month which contributes a monthly gross revenue of approximately 2 billion dollars for all the telecom operators in the country. There are 12639 legally active and authorized telemarketing organizations in India with some large telemarketers sending up to a billion SMSs on certain days. While the cost effectiveness of the scale has made it easy for businesses to reach out to their target audience, telemarketing has brought with it a serious invasion of privacy and has become a major irritant to mobile subscribers in addition to possible frauds [59]. The issue is rampant across the world with the Federal Communications Commission (FCC) in the United States of America mentioning that more than half the calls received by subscribers in 2019 are spam [28, 66]. Research efforts have shown that the growth of legitimate bulk messaging traffic in the recent years degraded the performance of spam detectors resulting in increasing number of spam messages passing through the established content based filters [61]. Prior research in Pakistan has indicated the growing role of SMS messaging for financial inclusion but highlighted and attempted to address the growing concern of fraudulent SMS [58]. A growing body of work has studied the role of security in global development, and the various factors influencing security and privacy of people in developing regions, while identifying the important role that national and international policy could play in influencing and improving the security practices [2, 83].

"The SMSs appear like regular text messages sent by banks. However, they are sent by fraudsters and contain a link which installs a malware allowing access to the phone" - Cybercrime investigation officer [59]

To curb the menace of Unsolicited Commercial Communication (UCC), the Telecom Regulatory Authority of India (TRAI) introduced a regulation in 2010 allowing mobile subscribers to register themselves to a National Do Not Disturb (NDND) registry [13, 69]. The NDND registry behaves as a preference portal where the subscribers can block all communication or selectively block communication from a predefined set of seven preference categories (Banking, Real estate, Education, Health etc..,). Currently, the NDND registry, since its inception in 2010, holds preference information of more than 230 million subscribers who have exercised their choice and opted out from receiving promotional content. Additionally, the government mandated that each telecom service provider (TSP)/carrier in the country implement a *common* procedure for complaint registration and resolution in their networks. So far, more than 2 million complaints have been registered which resulted in the active block-list of 460000 numbers and disconnection of approximately 1.4 million phone numbers for violations and instances of consumer courts levying fines on telecom service providers [23].

Despite the introduction of monetary dis-incentives, preference registration, and complaint resolution and tracking facilities by TRAI there have been new efforts taken by violators to gather phone numbers of potential subscribers from various data leaks in the country [18, 19, 22], and reach customers using unauthorized commercial communication channels without regard for the customers' preferences. The implementation of the NDND registry came with its own set of challenges. The first involved all the telecom service providers to "sync" their operational databases with the central database hosted by TRAI. This considerably slowed down the process and resulted in a customer's preference being acknowledged and effective only *seven days* after the registration. Additionally, complaint resolution processes currently take up to seven days from their registration because of the heavy need for collaboration among telecom service providers who are generally reluctant to share subscriber information or telemarketer activity.

Motivated by the economic importance of telemarketing, keeping in mind the problems faced by subscribers and the need to improve collaboration, transparency, and accountability in the entire process, this paper describes an architecture that uses consortium blockchains to record customer preferences and extends it to capturing subscriber consent. The solution tackles challenges around data sharing between telecom service providers and processes to improve operational efficiency of current business processes. These suggestions have been incorporated in the latest release of the regulations for unsolicited commercial communication in India by TRAI in July 2018. In addition to detailing the design of the system, we present the journey towards the realization of the design, its country wide deployment, and challenges faced. Finally, we evaluate the success of the proposal with one year of real world data since the usage of the implemented system from telecommunications operations in India.

We make the following contributions: (1) detail key business processes, operational practices, and challenges faced by the Indian telecommunications ecosystem [§3], (2) engage with regulatory bodies and stakeholders; design, propose [§4], and implement a viable solution addressing performance, security, and privacy challenges with minimal operational impact [§5] resulting in the TCCCPR'18 regulatory amendment, (3) identify practical challenges during deployment [§6], (4) evaluate the impact of the deployed system [§7], (5) lay out practical challenges, and limitations of the currently deployed system [§8], and (6) present a discussion [§9] and detail potential future efforts [§10].

2 BACKGROUND & RELATED WORK

Previous efforts to tackle spam or forms of unsolicited communication fall under two categories, 1) regulatory initiatives taken by the governments to manage spam and 2) technological initiatives and tools built to handle and manage spam. Below, we look at these initiatives & solutions proposed in the past.

2.1 Regulatory Initiatives

The first major regulatory initiative to curb spam was enacted by the United States Congress as the Telephone Consumer Protection

Act of 1991 (TCPA 1991), and Telemarketing and Consumer Fraud and Abuse Prevention Act (TCFAPA 1994) which regulate the use of automatic dialers, robocalls (prerecorded calls) & introduces the national do not call lists [65]. Additionally the TCPA'91 mandates that written consent be taken from the customers and that the customer can only be reached out to if they meet a strict opt-in requirement. This meant that the customers are by default opted out of any commercial communication until an explicit consent is provided. Different states in the United States have laws that affect SMS messaging and sales communication which on violation result in serious fines.

In Europe, the Privacy and Electronic Communications Directive 2002 known as the ePrivacy Directive (ePD) established an opt-in approach where any commercial email can only be sent to an individual with a prior agreement or consent [12]. In the United States, the CAN-SPAM Act of 2003 mandates that all commercial messages sent to a cell phone need to be disclosed as an advertisement and must provide a way to opt-out from receiving future messages while ensuring that they comply with the national do not call list [81]. Similarly, in the United Kingdom, Schedule 2 of the Data Protection Act of 1998 introduces mandatory opt-in for any commercial communication and allows consumers to sue for compensation for receiving spam messages [54].

Compared to the CAN-SPAM act, TCPA, and TCFAPA in the United States aimed towards email and spam in telecommunication networks, EU General Data Protection Regulation (GDPR), and Canada's Anti Spam Law (CASL) include laws with much heavier monetary penalties ranging between 1 million dollars (CASL) per violation to 22 million dollars (20 Million EUR). Despite the long term existence of spam prevention regulations, it has only been recent for businesses in the telecom industry to face extremely heavy penalties. The EU GDPR, since its adoption, has penalized telecommunications operators with 69 penalties across different countries in the EU with companies like Telecom Italia and Vodafone Italia facing the largest fines totaling over 30 Million EUR [41, 42, 57].

The first regulation to tackle unsolicited commercial communication in India was released in 2007 introducing the implementation of the national do not call/disturb (DND) register [13], mandating every telemarketer to respect the preference of the subscribers and introducing a mobile identifier code for telemarketers [70]. As a default setting all subscribers were opted in to receiving commercial communication unless explicitly opted out by adding their information to the DND register. The regulation also mandated the registration of telemarketers and introduced monetary dis-incentives to curb the problem of spam in the country.

Current regulations mandated worldwide only provided economic dis-incentives for the telemarketers and resulted in banning telemarketers for continued violations [33]. These acts and regulations have been criticized for increasing the amount of spam by having merely provided guidelines for spammers to spam legally [46, 68]. The CAN-SPAM Act was poorly enforced and the economic dis-incentives were not strong enough a deterrent for spammers resulting in increasing email spam [33]. For example, in India and many other countries, violators gamed the system of consent by using fine-print on raffle or lucky draw coupons and additionally used leaked phone numbers from databases. Another reason for higher levels of spam could be the default "opt-in" approach taken for advertising in India compared to the default "opt-out" in Europe and the US. However, the voice call based spam continues to be a global nuisance. This brings in a need for a system that can capture unique consents and map the consent of the customer with the required business entity while ensuring the ability to revoke them as needed. Suggestions were made to revise the act to include long prison sentences [30]. In a response to similar regulations in Malaysia, researchers have prescribed *self-help*, *opt-in & opt-out* as strategies to address the spam problem which are now adopted by various governments as do not call lists & mandatory requirement of consent [29]. However, our experience presented in this paper supports the statement by prior research efforts that legislation alone will not be able to eliminate spam [46].

2.2 Technological Initiatives

There are a variety of mobile apps available for smartphones which help manage and filter spam from the SMS inbox [44, 78]. Many of these systems use rule based filters which categorize the message based on their promotional nature of text and flag them for review by the user. The usage of mobile identifier codes for telemarketers ensures that the promotional messages can be filtered by using a rule based approach. Other approaches like *SMSAssassin* use a combination of crowd-sourcing and bayesian learning which can be trained over time to identify spam [87].

Additionally there are many third party applications on the Google play store for android which allow users to maintain blocklists and ban specific SMS senders. Narayan *et al.* studied the top twelve SMS spam filtering apps and conclude that most of these apps are ineffective and propose a new 2 level stacked classifier approach to detect and classify spam [47]. Apple's default SMS application (iMessage) and Google messages both provide the option to block each sender using the settings without the need for any third party applications [3].

Previous work by Jiang *et al.* tries to analyze SMS spam in large cellular networks and indicate spatial correlations using text clustering tools over reported spam SMS data [25]. Similarly other techniques focus on identifying SMS spam during possibly legitimate bulk messaging by senders [61]. Systems like Greystar leverage the fact that SMS spammers target random phone numbers and employ statistical models based on their footprints through a grey space (e.g. data only numbers) essentially behaving as *honeypots* to detect spammers and block them out of the networks [24]. Such systems have been implemented and used by the telecom operators in India to detect and fine violators using a random set of regularly changing honeypot phone numbers.

Unfortunately, none of the existing technology solutions by themselves have been effective in completely curbing spam. As long as the cost of sending an SMS remains low, there is huge motivation from the spammer to get around the filters and find new ways to continue to reach the consumer. To avoid such a problem, in this paper we propose a proactive approach to prevent spam by bringing together infrastructures to record consent, and preferences of the customer, rather than reactive approaches to spam taken by default messaging applications today. The technological approaches described address the "user end", or target a specific stakeholder of the ecosystem, in an effort to solve the problem of spam but does

not address the overall challenge it poses at the ecosystem level. In our work, we attempt to address the challenges throughout the ecosystem with existing individual solutions complementing our efforts.

2.3 Use of Blockchain in Government

A blockchain allows a set of participants to create a shared and tamper resistant ledger of transactions that are validated by a consensus mechanism among them. Such a network decentralizes trust among mutually untrusting participants by creating transparency and accountability through collective verifiability [56]. A permissioned blockchain is one in which the write privileges are granted to a consortium of entities. These entities govern the policies of the blockchain and are responsible to propagate and verify transactions in a network. Such a blockchain could have a public read privilege or maybe granted only to auditing agencies. Hyperledger Fabric [1] & Ethereum consortium [15, 86] are some popular blockchain frameworks that enable creation of consortium blockchains.

Smart contracts are protocols which make contractual clauses partially or fully self executing and self enforceable. Governments have begun to experiment with blockchain for the various strategic, organizational, economic, informational and technological benefits it brings [51, 56]. For example storing land records in distributed ledgers prevents manipulation and reduces corruption [32]. The government of Estonia, has implemented an X-Road system using blockchain transparently and easily allowing citizens to access their data and control data access [76].

To effectively leverage the advantages of blockchains they need to be guided by *governance*. In this paper, we describe an approach where the regulatory bodies embraced blockchain as a technology to combat the problem of unsolicited commercial communication but eventually saw possibilities to govern other areas with the same technology.

We believe that UCC has unfortunately acquired a negative connotation as spam but instead can be viewed as a problem of bridging the divergence between ex-ante expectations of regulators and telemarketers and the ex-post perceptions by the recipients (subscribers). Spam is therefore very subjective since its a nuisance for those who explicitly choose to exercise their option to not be disturbed but could also take shape of graySMS. GraySMS, like graymail is a situation where an originally interested consumer who opted into receiving the messages, eventually is no longer interested and marks the same message as spam.

3 UNDERSTANDING OPERATIONAL PRACTICES IN INDIAN TELECOM INDUSTRY

India is the world's second largest telecommunications market with over a Billion active subscribers and has the lowest call, message, and Internet data pricing in the world enabled by nation scale hypergiant telecom operators. In this section, we present the detailed view of the telecom ecosystem prior to our intervention, and the operational practices put in place then for addressing the challenges of UCC.

3.1 Stakeholders in the Telecom Ecosystem

The telecom ecosystem essentially comprises of the following entities:

(1) *Telecom operators* are telecom service providers who provide telephony and access to data services.
(2) *Telemarketers* are marketing agencies or personnel who solicit customers through phone calls, SMSs & auto-dialers either directly or on behalf of an organization which shares their (potential) customer details with the telemarketing organization.
(3) *Principal entities* are organizations which generate content and leverage telemarketers to reach out to potential customers. These are businesses which use telecommunication services to interact with subscribers.
(4) *Subscribers* are the mobile consumers who use the network services provided by telecom operators and are potential customers to the principal entities.
(5) *Regulatory authorities* are typically government entities that make policies and enforce incentive structures that ensure fairness among participants.

3.2 History of Regulatory Amendments to UCC in India

Since the effect of the Telecom Commercial Communications Customer Preference Regulations (TCCCPR) in 2010, TRAI in the 6^{th} amendment introduced a SMS header format (AB-XXXXXX) where *AB* corresponds to the telecom provider and region and *XXXXXX* corresponds to the alpha numeric code for the business entity sending the promotional SMS. The amendment to the regulation clearly defined *promotional & transactional* messages in addition to demarcating special phone number sequences which begin with *+91-140* for telemarketers to use during promotional phone calls [71]. A *promotional* SMS is used to send offers, discounts or promotions to new or existing customers which may have not been solicited by the recipients and can only be sent between 9AM and 9PM. A *transactional* SMS is used to send one time passwords, informational messages, booking information or order alerts to registered customers and should not be intended for marketing.

The 2010 regulatory mandate also involved an online registration process for telemarketers starting 15th January 2011 by paying 1000 INR (approx. 13.5 USD), and 9000 INR (approx. 120 USD) as customer education fee. Once validated, the telemarketers are immediately assigned a telemarketer ID, and issued a registration certificate for beginning operations [50]. Malicious telemarketers found ways to register small fraudulent entities and paid the low registration cost of 10000 INR (approx. 133.5 USD) to access and obtain numbers from the national registry. The malicious telemarketers then use personal phone numbers to send promotional SMS content mimicking the standard peer to peer (P2P) messages which are treated differently than business messages (Note that business messages or bulk ads are 8 times more expensive than P2P SMS). These operations are extremely hard to detect without privacy invasive checks on all customer communications and the telecom operators therefore resort to reactive approaches such as investigation procedures when affected subscribers file complaints with the operator or with the regulatory body. These telemarketers are classified as unregistered

telemarketers. In response to increasing cases of fraud and telemarketing from unregistered telemarketers, TRAI capped the number of SMSs that can be sent in a day to 100 per day and limited to 3000 per month for mobile subscribers which was later amended to 200 per day. In the 10^{th} amendment of the regulation, TRAI mandated the usage of *signature solutions* by telecom operators to detect bulk messages having similar string or their variants, specifically those without any specific information of the subscriber. Additional improvements in the amendment included guidelines for block-listing or throttling specific numbers, introducing higher tariffs for bulk messaging, and a web based complaint registration system. In the 13^{th} amendment, the regulation introduced financial disincentives to telecom operators and telemarketers for complaints registered about violations of users' preferences and increased the security deposit needed to be made by the telemarketers to be registered. A recent summary by Tu *et al.* identifies the various techniques currently in use to curb UCC due to robocalls in the United States and similar systems implemented and adopted across the world by various telecom operators [79].

Despite incessant measures taken to mandate the use of the NDND registry and regulating the usage of specific number series and SMS header, customer dis-satisfaction continued, indicating the increasing challenges faced by the ecosystem, hinting towards the possible need for revising the regulatory framework.

3.3 Regulatory Processes and Authors Engagement

The main responsibility of the regulators at Telecom Regulatory Authority of India (TRAI) is to help market function. The regulatory change process starts with the initiation of an open consultation to address an identified problem in areas over which the regulators have jurisdiction. The problems are identified through stakeholder feedback, audits, complaints, and active efforts at problem identification. The process starts with a clear presentation of the problem and defines specific issues on which the authority democratically invites comments from the public.

The responses could be made by stakeholders mentioned in §3.1 including active engagement from organizations providing services to the stakeholders, and individual citizens. The responses obtained are openly published in the first stage and an opportunity is given for anyone to submit counter comments. Thereafter, the authority almost invariably chooses to hold one or more open house discussions to hear all points of view in person. The inputs received are summarised, and considered while deciding upon the nature of intervention. This may be a regulation, a recommendation to the government, a direction to the licensees, or a combination of these measures [72, 73, 75]. The regulations are accompanied by an explanatory memorandum that sets out the reasoning behind the rules.

The authors in this work engaged with TRAI's initial call for consultation to evaluate the potential feasibility, need, and analyzing the impact of blockchain technologies in the formulated problem setting of spam. These collaborations continued in the public process where inputs were obtained from various stakeholders during the multiple rounds of public comments (and counter comments), and open house events, with the pilot solutions and their feasibility

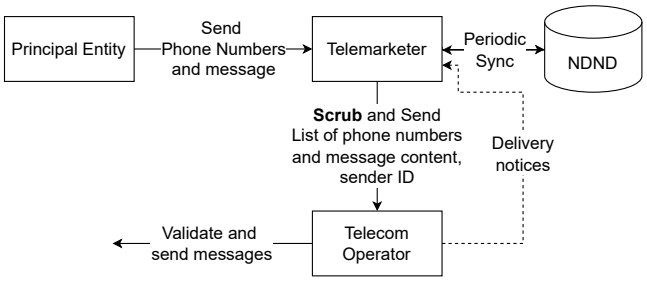


Figure 1: Current Interactions between Principal Entities, Telemarketers, and Telecom operators

demonstrated publicly [4, 5, 7, 8, 10, 11, 16, 20, 21, 27, 31, 34, 35, 39, 40, 55, 60, 62–64, 82, 84, 85]. The draft regulation for TCCCPR 2018 was published and invited for a second round of consultation after which some changes were made based on stakeholder input resulting in the updated version of the regulation and an explanatory memorandum was issued addressing the concerns of the stakeholders.

3.4 Current Workflows

The telecom ecosystem comprises of back and forth communication between the various stakeholders. Principal entities (e.g. online shopping platforms, ride hailing services, restaurants etc..,) partner with a telemarketer with whose help they create a *promotional campaign*. The telemarketer is responsible for the registration of a sender ID for the principal entity which is used in the header format that is displayed to the recipient on their mobile device. Sender IDs allow principal entities to set a recognizable name which helps recipients recognize the brand instantly. Sender IDs/Headers which are equivalent to the domain names in the SMS world need to be registered by the partnering telemarketer who would be running a promotional campaign on the principal entity's behalf. TRAI regulations mandate that the SMS headers for business entities in the countries be of 9 alpha numeric characters of the format *AB-XXXXXX* where *A* corresponds to the letter assigned to the telecom operator, *B* corresponds to the telecom operators' regional circle followed by a - *(hyphen)*. It is mandatory to register a 6 character alpha numeric SMS header. While similar to Internet domain-name registrations, the current process for header registration involves verification of the documentation of the business entity and registering a unique header ID for the same. These registrations need to be shared across all telecom operators and resulted in operational latencies of a few days before the registered header was assigned and made usable to the business entity.

Today, The principal entity provides the telemarketer with a list of phone numbers who are the target of the promotion either as a file or via an API provided by the telemarketer. The telemarketer then removes the numbers registered with the DND service from the original list in a process known as ***scrubbing*** and proceeds to send the final list and promotional message to the a partner telecom operator to be sent under a specific sender ID or a generic sender ID for promotional SMSs registered to the telemarketer. The telecom operator who receives the task, known as the Originating

Service Provider (OSP), further splits the list provided into regional circles based on the registration of the phone numbers and delegates the task of sending the SMS to the telecom operator at a given circle, known as the Terminating Service Provider (TSP), who then sends the required promotional SMS. The TSPs optionally scrub the phone numbers again before sending the SMS. We present these interactions in Figure 1.

To register or update preferences, a subscriber logs into a centralized web based portal provided by TRAI or a portal provided by their respective telecom operators. In the current system, the preferences are sent daily as an update from each telecom operator to the national do not disturb registry. The registry updates are then periodically synced by the respective telecom operators and the telemarketers. The existing system takes more than 24 hours to register the preferences of the user and requires up to seven days to enforce the revised preferences at the TSPs [74].

A complaint can be registered for an unsolicited commercial communication by a mobile subscriber using the mobile apps provided by TRAI or via their respective telecom operators' web, IVR or SMS based systems. Once a complaint is registered by the subscriber, the TSP verifies the registration status of the complainant in the National DND registry and compares the information provided using semi-automated procedures in the logs to identify the OSP, and telemarketer who have initiated the process. The parties involved along with TRAI verify the complaint and present required proofs of SMS being sent and the content in a specific promotion. On confirmation of UCC, the telecom operator and the telemarketer are levied fines. The total turn around time for a complaint to be addressed in the current process is close to 7 working days and involves heavy coordination between the telemarketer, and the telecom service providers (TSPs, OSPs) involved in SMS message flow. The problem further intensifies due to customer data privacy and can only be addressed by nodal officers of the respective telecom operators from each circle.

3.5 Challenges with Current Workflows

The problem of UCC has continuously been a challenge for regulators, mobile subscribers and telecom operators alike. The National DND registry which consists of all the phone numbers of the customers and their corresponding preferences is stored in plain text and can be accessed by all registered telemarketers who create periodic local copies for scrubbing purposes. TRAI amended the UCC regulations in India and moved from a binary mode of setting customer preferences i.e. *full block of promotional content*, and *no restrictions on promotional content*, to enabling *partial blocks*. Using the partial block features, the subscriber can partially block content from seven predefined set of categories which are as follows: 1) Banking, insurance & financial products, 2) Real estate, 3) Education, 4) Health, 5) Consumer goods & automobiles, 6) Communication, broadcasting & entertainment & 7) Tourism. The introduction of this resulted in the need for telemarketers to classify the principal entities under one or more of the respective categories. Mobile subscribers blocking a specific category due to the UCC generated by a specific principal entity also end up blocking principal entities who they would have otherwise been interested in. This opens up a need for nesting the categories to multiple levels of sub-categorization.

A major problem for unsolicited commercial communication is due to possible collusion between malicious and unregistered telemarketers. The availability of all phone numbers for a small registration fee and security deposit to TRAI allows malicious telemarketers to leak phone numbers and collude with unregistered telemarketers or entities to violate the guidelines set of telemarketing and send out SMS or make calls from phone numbers which are registered for personal use. Therefore there is a need for storing the numbers in the DND registry in a privacy preserving format which the telemarketers can then scrub their phone number lists across the DND service protecting user privacy, instead of periodically downloading the data present in the NDND registry for scrubbing.

The current registration of the SMS headers/sender IDs for the principal entities opens up tremendous opportunities to *spoof* customers with sender IDs which sound and look very similar. For example, a leading bank in India, the State Bank of India (SBI) might be registered as *STABAN*. However, another malicious entity under the name of *SBI Banquets* can register themselves as *SBIBAN* and send out fraudulent SMSs posing as the bank. Additionally, many principal entities might not have a 6 character name for e.g. *Ola, Uber* (popular ride sharing services) which makes telemarketers register them with additional characters such as *OLACAB, UBERCA*. Similar issues exist with principal entities whose names are much longer and cannot be abbreviated to six characters. Many of the large organizations in India have multiple businesses in different sectors which makes it hard to establish a brand identity with a flexibility of six characters. Additionally business entities use multiple telemarketers and SMS gateway APIs as a fallback in case of failure thereby making it hard for the user to associate the message with the brand. For example, SMSs from the bank stated above might be received on the subscribers' mobile phone as *VM-STABAN*, *AD-STABAN* etc.., which appear under different SMS inboxes for the mobile subscriber making it difficult to keep track of all the SMSs from a specific principal entity in a common place. These challenges provide us with an opportunity to implement national header registration features similar to domain name systems and their registrations for the web [45]. Being able to track and verify the message flows between principal entities, telemarketers, and telecom partners, it becomes possible to enable mobile subscribers to efficiently manage their SMS inboxes through improved flexibility in display of the sender ID.

The current processes for a subscriber to register their preferences and for them to come into effect can take up to seven working days due to synchronization delays. Similarly, a registered complaint can take up to 7 days to be resolved and needs to be resolved manually in most cases with extensive collaboration between the different telemarketers, telecom operators, and subscribers. This opens up the need to simplify the operations and automate the way in which data is shared and used by the respective stakeholders. During complaint resolution it also becomes very difficult for the principal entities and telemarketers to prove acquisition of consent. In many cases these proofs are presented as paper documents, screenshots with insufficient information or database entries made across a subscribers' record with no way to verify the validity of the claim. This brings in a need for a verifiable and digital way of acquiring, storing and using consent from the customers while giving the customers an accessible way to revoke it.

Since the introduction of the complaint registration procedure over 2 million complaints have been registered by consumers with an average of 40000 per month. As a result, telecom services to more than 1.4 million phone numbers have been disconnected and 460000 numbers have been blocked so far. Despite so many disconnections, levy of huge fines and blocklists of unregistered telemarketers & violators, the UCC problem is still not fully under control. Motivated by these challenges (summarized in Table 1), we propose a blockchain based solution aimed at addressing various privacy, security, and operational challenges.

3.6 Design Goals

With the understanding of the current workflows in the telecom ecosystem described in §3.4 and the various challenges they pose described in §3.5, we outline below the design goals, summarized by the grouped categories shown in Table 1. We set out to achieve our goals with the proposed solution in §4.

(1) **Real time or Near Real time operations**: Subscribers, and principal entities both face significant challenges due to the long operational times involved in critical operations. Subscribers face lengthy times for the registration of their preferences (1-7 days), and for them to take effect. This is due to synchronization challenges between the telecom operators, and the TRAI operated NDND preference registry. Principal entities face similar challenges with the registration of headers to send promotional messages. We aim to reduce these multi-day latencies to real time, or near-real time latencies when operating at scale.
(2) **Improving Security and Privacy**: Telemarketers and telecom operators periodically obtain the plain text information of subscribers in the NDND registry and their preferences for promotions. Malicious telemarketers obtain the information of these subscribers and use personal devices to perform telemarketing operations. We aim to prevent the usage, and sharing of plaintext phone numbers, and prevent risks from malicious attackers compromising and leaking the subscriber phone numbers, and preferences in the NDND registry.
(3) **Improved Compliance and Flexibility**: Subscribers register complaints for UCC through various means such as through the official mobile app managed by TRAI [48, 49], with the telecom operator providing them the services through a web portal, IVR, customer complaint ticket. The registered complaints are usually addressed within 7-14 working days. We aim to reduce these latencies, improve the compliance of telemarketers to adhere to subscriber preferences. Successful intervention of the proposed system would result in a reduced number of complaints from registered telemarketers. We aim to design the solution to be easily extensible allowing future fine grained preferences for customers, improved header registrations, and protect brand reputation through fraud prevention.

4 PROPOSED SOLUTION - TELECHAIN

The most common approach today in India, and other countries, to the problem of UCC, is to investigate spam after a violation is detected or a complaint is filed by the subscriber. In contrast, our solution helps establish ex-ante compliance for each message or call sent to the mobile subscriber – thus effectively ensuring that all the promotional messages sent to a particular user are consistent with preferences and recorded consent of that user.

Our choice of a consortium blockchain in the design of Telechain is motivated by our goals described in §3.6 to have secure and near real time exchange of data between the various stakeholders. In addition, the pro-active approach to policy enforcement and transparency based on collective verifiability and smart contracts enabled by blockchain makes it a compelling design choice.

4.1 Components of the proposed system

4.1.1 ***Blockchain network.*** A consortium blockchain network is created between the participating entities i.e. telemarketers contributing physical nodes in the blockchain, telecom operators, third party service providers and a regulatory authority. Any update of the customers' preferences in the NDND registry via the mobile app, web portal or via telecom operators customer care systems (described in §4.1.8) is encoded as a transaction in the system. Each one of the participants in the network maintains a copy of the blockchain state including the DND register which gets updated in the servers of the participating entities thus making each update of preferences by the subscribers near-real time and reduces the time from almost seven days to a matter of minutes. The usage of blockchains and establishing the network addresses the current latency challenges and issues due of data staleness (R1-R5), improves policy adherence by ensuring strong accountability and transparency addressing the S5, A1, A3 challenges, facilitates the necessary registrations of headers, templates, and consent (F2, F3) presented in Table 1.

4.1.2 ***Improving privacy of NDND Registry.*** To improve privacy and security, subscriber information shared on the chain is always hashed and cryptographically signed by the respective nodes originating the update. The use of blockchain changes the maintenance of the DND registry from a centralized setting to a decentralized and replicated setting. While standard access control measures prevent leakage of information to unauthorized telemarketers, the existence of hashed information prevents a malicious telemarketer from leaking actual phone numbers to an unregistered telemarketer who carries out advertising through personal cellular devices or a telecom operator poaching subscribers addressing the challenges S1, S2, and S3, presented in Table 1. Each number present in the DND registry is mapped to the name of the telecom operator and relevant metadata.

While this approach allows large telemarketers to make their operations more efficient in sending promotional SMS, it makes it harder for smaller telemarketers who cannot afford to dedicate a server on their behalf to participate in the network. Previously, smaller telemarketers filtered the list of customers from the do not disturb registry by downloading the entire data of the registry and possibly manually checking the customer preferences for each promotional campaign. However, this approach would no longer work with the new solution since the hashed information provided to the telemarketers is not usable with their current operations. To resolve this problem, we introduce *scrubbing nodes* on the blockchain

Table 1: Challenges faced by different stakeholders grouped by design goals and deployment status. (●: Completely deployed, ◐: Partial deployment)

#	Stakeholder	Challenges	Addressed by
Real time			
R1	Subscribers	Lengthy time for preference registration to take effect. (7 days)	● [§4.1.1, §4.1.7]
R2	Subscribers	Lengthy time for complaint resolution. (7-14 days)	◐ [§4.1.1, §4.1.7]
R3	Telemarketers	Ensuring the usage of the latest data for scrubbing phone numbers	● [§4.1.1, §4.1.3, §4.1.7]
R4	Operators & Telemarketers	Quick update and maintenance of user preferences	● [§4.1.1, §4.1.7]
R5	Operators	Coordination with telemarketers	● [§4.1.1, §4.1.3, §4.1.7]
Flexibility			
F1	Subscribers	Unavailability of fine grained control of preferences	◐ [§4.1.5]
F2	Principal entities	Registration of longer/shorter SMS Header/Sender ID	◐ [§4.1.1, §4.1.7]
F3	Principal entities	Brand identification irrespective of mediating links	● [§4.1.1, §4.1.4, §4.1.6]
Security & Privacy			
S1	Telemarketers	Avoiding usage of plain text phone number sharing	● [§4.1.2]
S2	Operators	Ensuring data privacy and protecting consumer data	● [§4.1.2, §4.1.3]
S3	Subscribers	Prevent access of phone number data by unregistered telemarketers	◐ [§4.1.2]
S4	Operators	Prevent unregistered telemarketers from sending promotional SMS/calls	◐ [§4.1.8]
S5	Principal entities	Protection from spoofing attacks due to similar sounding sender IDs	●[§4.1.1, §4.1.7]
Automation & Usability			
A1	Operators	Validating complaint registrations & root cause analysis	◐ [§4.1.1, §4.1.4, §4.1.7]
A2	Subscribers	Avoiding inbox clutter due to multiple sender IDs	◐ [§4.1.8]
A3	Auditors & Regulators	Consent request & acquisition is unverifiable	◐ [§4.1.1, §4.1.4, §4.1.6, §4.1.7]

network providing scrubbing services for a minimal fee. Larger telemarketers, telecom operators and infrastructure operators provide scrubbing services to smaller telemarketers.

4.1.3 ***Scrubbing Nodes***. The scrubbing nodes have read only privileges to the blockchain network and are responsible for providing scrubbing services for a small fee. The result of the scrubbing would be a token that's furnished to the telemarketer and the proposal of a transaction to the blockchain while following a specification that's agreed upon by the participants in the network. The telemarketer can submit this token along with the promotional SMS, registered header, and template IDs, directly to the telecom operator who can retrieve the scrubbed file and send the promotional SMSs to the list of valid subscribers. The design decision to return a token instead of the scrubbed result $S = \mathbb{L} - \mathbb{C}$, where $\mathbb{L}$ corresponds to the set of subscriber identities and $\mathbb{C}$ corresponds to the set of subscribers in the NDND registry, is intentional to prevent probing attacks where telemarketers aim to identify subscriber preferences by sending one request at a time. The scrubbed result at its simplest binary preference level is represented by the set difference S. The scrubbing nodes coupled with the blockchain network ensure the recency of the data being operated upon, easy interoperability with existing telecom operators, prevent unauthorized access to the subscribers' consent and preferences and protects their privacy addressing the challenges R3, R5, and S2, presented in Table 1.

4.1.4 ***Header & Content Template Registry***. The blockchain network handles the registration of headers (sender IDs) and maintains the ownership mapping between the principal entities and the headers registered by the entity. The telemarketer operating the promotional campaign on behalf of a principal entity is required to register the content of the message(s) used as a part of the campaign. The content registration is also allowed on the system as *templates* which are message strings that have placeholders and can be replaced by specific information related to the subscriber when the SMS is sent. Here is a sample content template.

"*Dear <%..%> Head to the nearest <%..%> store and avail a flat <%..%>% off using coupon code <%..%>.*"

The registration of headers and templates by the principal entities however need manual verification by the telecom operators for business compliance. Once verified and registered into the blockchain, it provides principal entities ownership of their brand header and verification to operators and telemarketers after the correct scrubbing process about the correctness of the message delivery addressing F3, enabling easier complaint tracking (A1), and establishing auditability of the actions (A3).

4.1.5 ***Preference Registry***. A challenge in the existing system was the long duration needed for a customer preference to take effect. With the introduction of the blockchain, a mobile subscriber can login via their respective telecom operators self-help portals or the mobile apps to update their preferences and either block/unblock specific promotional categories and sub-categories. The changes are proposed as a transaction by the telecom operator, or TRAI enabling the dashboards after successful user authentication. The transaction on successful validation is used to update the database records of each of the participants with the new preference information set by the customer effectively reducing the time needed for the preferences to be in effect *improve from seven days to a few minutes*. Additionally, the flexibility of the scrubbing services

and its integration into the blockchain enables the preference registry to support fine grained preferences addressing the challenge F1, and enabling fine grained preference control.

4.1.6 ***Consent Registration & Acquisition.*** To overcome the problem of unsolicited commercial communication by telemarketers to potential customers, it becomes highly important to have an electronic registration of consent of the customer. This process is made in two independent phases, the first phase involves the registration of a *consent template* by the principal entities which maps it to their registered headers. The registered message will contain the link to privacy policy, terms and conditions, message frequency and request the customer for approval before being contacted for any promotional purposes. The second phase is the *consent acquisition* phase where the registered consent template is sent over SMS to the mobile subscriber along with a one time password or a custom web link. The subscriber can read the conditions and choose to either provide the principal entity with the OTP or click on the link and go through the necessary steps to provide consent to the principal entity. This provides a digital trail of actions (addressing A3) and SMS interactions that resulted in the verifiable informed consent being acquired by the principal entity (addressing F3) for their customers.

"*Thank you for shopping with <%..%>. Please click on the following <%link%> if you'd like to receive updates regarding offers & promotions. Terms & privacy can be found here. You may receive up to 4 sms/month. Your consent OTP: <%..%>*" - sample consent template.

While consent reflects on an explicit preference, the exercise of preferences does not imply consent. For example, a subscriber consenting to receive promotional offers from a restaurant is only restricted to that specific restaurant and not to the overall preference for receiving promotional offers from *any* restaurant.

4.1.7 ***Smart contracts & agreements.*** Smart contracts are programmatic expressions of business workflow conditions which help in pro-active policy enforcement without the need for a third party. The developed contracts are audited by the participants of the network and across a correctness test suite which implements the various conditions described above such as the *header, content & consent registrations, scrubbing requests* and are validated by the participants of the network. These are programmatic encoding of business logic which are critical and facilitate the operations on the blockchain network.

4.1.8 ***End user applications.*** Each of the participating nodes (telecom operators, telemarketers, scrubbing nodes) in the blockchain network expose interfaces for their existing business processing systems to interact with the blockchain infrastructure. These include web portals, mobile apps, Unstructured Supplementary Service Data (USSD), and SMS services provided by telecom operators where a mobile subscriber can register complaints, update preferences, and in addition can see a detailed list of consents provided by the customer. Similarly, there are supporting applications provided for smaller telemarketers where the promotion campaign can be registered on behalf of a principal entity which allows the telemarketers to obtain a token to be furnished to the telecom operator in addition to also providing them an easy way to request a telecom operator to run the promotional campaign. End user applications such as messaging apps can continue to implement local spam and aggregation filters to avoid inbox clutter addressing A2 while applications like TrueCaller installed on client mobile devices can block unregistered telemarketer SMS and calls.

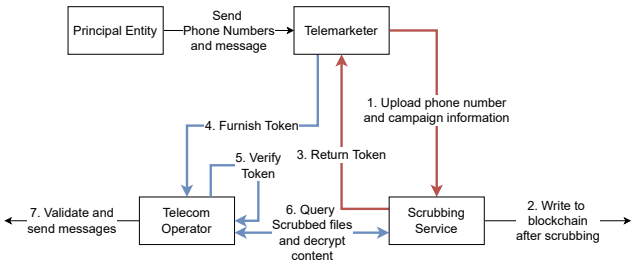


Figure 2: Figure showing the new workflow among stakeholders involving generation of a scrubbing token and the usage of scrubbing services. The solid red lines indicate the scrubbing service workflow. The scrubbing operations can be performed through any registered blockchain participant providing the scrubbing services. The solid blue lines indicate the post-scrubbing workflow which is modified from the workflow presented in Figure 1 for final message delivery.

4.2 Decentralized Workflows

Keeping in mind the business workflows detailed in §3.4, and the desire to create minimal disruptions to existing business processes, we design a new decentralized workflow leveraging the components presented in §4.1 to tackle the challenges summarized in Table 1 and §3.5. The registration / on-boarding of each of the components involved in the workflows are as follows:

4.2.1 ***Telemarketer Registration.*** Telemarketers register with TRAI using the existing application process, pay the required one time fee and a security deposit after which they receive a telemarketer ID. The telemarketer ID along with the payment information is stored in a database provided by TRAI to which the *read-only* credentials are shared over the network. Telemarketers willing to participate in the blockchain network can create a server and request to connect to the blockchain network by furnishing their a self signed cryptographic identity along with the telemarketer ID and payment receipt numbers as a transaction. The information corresponding to the telemarketer ID is verified by each of the participants according to the policy of the network. On successfully validating the information on the network and ascertaining the identity and signature, the server node is added to the network as a participant in the blockchain. The telemarketer node then reconstructs the blockchain by fetching information from the peers in the network and validates them before finally reaching a state consistent *global state* matching the other participants in the network after which the added node can participate in the network by issuing new transactions.

Telemarketers who do not participate in the network as direct participants delegate their registration to the network via any third party services, detailed later in the paper, which create a local

authentication system for the telemarketer, maintain their cryptographic credentials and register them by creating a transaction in the network.

4.2.2 ***Principal Entity, Header & Content Registration***. Principal entities are registered along with the *header* registration processes via *third party services* or telemarketers offering header & content registration services. Similar to domain name registration, a principal entity registers the headers of their choice which appear as sender ID to the mobile subscribers. The registration of the principal entities is done using their business name while mapping it to the chosen header(s) as a transaction on the blockchain. These entities are granted access to their information using the authentication on the third party services.

The principal entities after confirmation of their header registrations delegate/configure the ownership or access of their registered headers to any of the registered telemarketers by using the telemarketer ID or searching for the same via the web interface provided by the third party service for the same. This allows the partner registered telemarketers to create campaigns on behalf of the principal entity. The access delegation of a header to the telemarketers by the principal entities is recorded as a transaction over the blockchain. Once delegated, the telemarketers can register promotional content templates or the complete content of the promotion against the header of the principal entity by signing the one way hash of the templated content and the header used as the message. A transaction is issued on the blockchain by the principal entity with ownership of a specific header proxied through a blockchain participant offering content registration services. A *content token* is provided to the telemarketer which is furnished to the partnering telecom operator along with the template and the *scrubbing token* for message delivery as shown in Figure 2.

4.2.3 ***Customer & Consent Acquisition***. During customer acquisition and storing the contact information of the customer (for eg. at the point of sale counter), principal entities can use the APIs provided by their partner telemarketer or the services offered by third party consent registration and maintenance services to trigger a one time password (OTP) along with mandatory information as described previously in §4.1.6. The trigger of the consent acquisition SMS based on a registered consent template as described in §4.2.2 is recorded as a transaction on the blockchain. Similarly, the grant of the consent either based on OTP or a provided web link to the customer is recorded on the blockchain as a transaction which on successfully being validated adds the consent mapped to the header and the customer for future promotional campaigns by the principal entity.

4.2.4 ***Third Party Services***. Third party services are value added services offered by nodes participating in the network which can offer any of the following services. The services include 1) registration of telemarketers, principal entities and headers, content and consent, 2) authentication to third party services, scrubbing as a service using preferences and consent for principal entities, and 3) execution of promotional campaigns and forwarding the requests to the telecom operators. The third party service providers create and register identities for the telemarketers and provide them an authentication system for further usage of the system. These nodes behave as proxy nodes for their users to interact with the blockchain and provides the necessary web applications or API services.

Scrubbing is a mandatory business process for sending out any promotional SMSs with failures to comply with the mandate resulting in heavy penalties including ban of operations. The scrubbing process can be performed by the telemarketer nodes participating in the blockchain on their respective server machines. Telemarketers not actively participating in the network can use third party scrubbing services which are participants on the network. The scrubbing operation takes in an input list of phone numbers, the telemarketer ID, content template ID and the header of the principal entity. After validating the ownership of the telemarketer ID with the header ID, and the content ID with the header ID, the service creates a one way hash of each number and validates the preferences and the consents listed across the entry of the particular phone number from the current global state of the blockchain. If the user has either consented to receiving promotional content from the principal entity or has the category of promotion as a valid preference, the number of the user is stored in multiple files of valid phone numbers where each file contains the numbers corresponding to a specific telecom operator. Similarly, the rest are stored in corresponding invalid files.

Each one of these files based on the telecom operator are encrypted using the public key of the telecom operator and the corresponding links to the file locations for each telecom operator is provided along with a signed digest of the respective files thereby proving immutability and allowing access to only the intended parties. In addition the transaction includes a signed token and current hash of the global state which is issued to the blockchain network. The participants of the network validate the contents of the transaction by verifying the digests of the encrypted files and corresponding signatures. The telecom operators after validation take the corresponding token issued in the transaction and queue it to the pipeline of promotional campaigns to run. The token and the transaction ID proposed by the scrubbing node is presented to the telemarketer who requests the telecom operator(s) to begin the campaign by furnishing the token and signing it with their cryptographic identity. The request to initiate the campaign is recorded on the blockchain and the promotional campaign takes effect with each telecom operator changing the status of the promotional campaign to *completed*.

The business workflows post registration of the telemarketers, principal entities are illustrated in Figure 2 where the process starts with the principal entity partnering with a telemarketer. Similar to the current process, the principal entity sends a list of phone numbers and the message content, and a registered template ID to the telemarketer who scrubs the data across a third party scrubbing service or on their own while initiating a corresponding transaction on the blockchain. The generated token from the scrubbing process is furnished to the telecom operator directly or via third party services. The telecom operator validates the token, reads the corresponding list of phone numbers to send the promotional SMS and validates the transaction status by optionally re-scrubbing them locally before sending out the promotional SMSs to the mobile subscribers in their network. The telecom operator(s) involved in the message delivery then eventually attach a delivery report to the telemarketer initiating the campaign indicating the total number

of successful messages delivered which can be used for subsequent billing purposes.

4.3 Challenges addressed

With the implementation of the proposed system using the components introduced in §4.1, we addresses many of the challenges posed in Table 1.

By hashing the information available in the centralized NDND registry [13], replicating, and decentralizing it using blockchain, we ensure that the preference registration and any *updates are instantly in effect across all the participants in the network* removing the periodic synchronization in favor of distributed consensus protocols which are critical to blockchains [6, 67]. This reduces the complex and time consuming process in the current approach where the data is periodically downloaded and synchronized by various stakeholders. The proposed system and format of hashed data storage *protects sensitive and personally identifiable consumer data* (phone number) from being leaked. Malicious telemarketers and colluding unregistered telemarketers can no longer make sense of the downloaded hashed format.

The usage of the blockchain is ideal for the given problem as it *automates the coordination between various stakeholders* and their corresponding cryptographic identities on the system. The mandatory need for scrubbing ensures that the telemarketers do not ever know a *filtered* list of phone numbers which could help malicious entities collude with unregistered telemarketers. The segregation of the files by the scrubbing operations into respective files for telecom operators *greatly simplify the operations* and the need for the partner telecom operator to share data with other telecom operators for executing the promotional campaign. Throughout the entire process, the phone numbers and other sensitive information is shared in a hashed manner thereby *protecting the privacy of the subscribers*.

The availability of all the registered entities, their categories of operation and recursive sub-categories are now available to each of the nodes participating in the network. This information enables scrubbing service providers and preference registry systems to give users *much more fine grained control of their preferences* than the coarse categorisation into seven categories. It also allows any mobile subscriber to clearly view, manage and revoke the consents granted by them to various entities from a single location. Principal entities because of the new header registration process and the removal of the six character limit can now clearly establish their brand identities. Apps installed by mobile subscribers on their devices now can organize their message inboxes by the name of the business entity making it cleaner and easier to look for SMSs and avoiding clutter. The digital trace and availability of the consent makes it easier for auditors to identify and penalize violations based on complaints registered by the user.

5 IMPLEMENTATION

5.1 Implementation of the Blockchain Network

To test the feasibility of our proposal, a pilot implementation of the consortium blockchain network is built using Hyperledger Fabric, an open source consortium blockchain framework under the Hyperledger umbrella of the Linux Foundation [1]. Individual nodes of the telecom operators, a large telemarketer node, scrubbing service node and an observer node for the regulator (TRAI) form the permissioned blockchain network. *Endorsement policies* of the network are policies through which designated system administrators specify conditions for various types of transactions to be endorsed. It is also possible to specify custom endorsement policies, for example, a transaction to register a principal entity and their corresponding headers need to be endorsed by each of the telemarketer nodes on the network, the observer node and *at least* one of the telecom operators. Figure 3 shows the modules and implementation architecture at each physical node in the network.

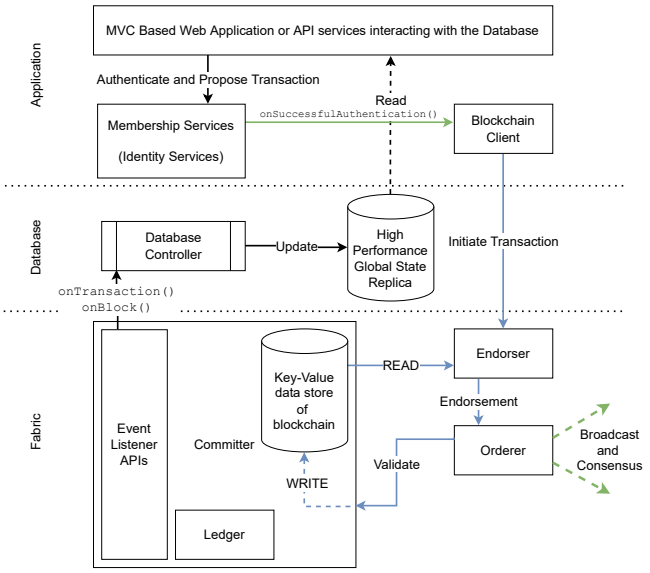


Figure 3: Blockchain participant node architecture indicating the web based application layer which includes an authenticated service proxying the requests made by the application users as a blockchain client. The database layer includes event driven approaches to replicate the global state of the blockchain, especially used by scrubbers for high performance tasks, layered over Hyperledger Fabric infrastructure. The blue arrows indicate the sequence of events in the blockchain.

In our implementation a majority of the participants on the network must endorse a transaction initiated by a client. During the endorsement, the designated peers according to the endorsement policy execute the transactions and share the output as the endorsement. The result of the endorsement is a cryptographically signed *read-write set* which includes the sequence of operations to perform on an underlying key-value database (CouchDB/LevelDB) to commit the transaction. This is indicated as the *Endorser* in Figure 3.

The read-write sets are then ordered by an ordering service which is a part of the Fabric framework. The consensus protocol which runs between the orderers of the network order the endorsed transactions and group them together into a *block* which is broadcast to all the participants of the network who then deterministically validate the endorsements & the read-write sets. On

successful validation a block is appended to the local ledger of each of the participants in the network and chained to the hash of the previous block. The corresponding key-value pairs indicated in the read-write sets are modified accordingly to achieve a new global state. This is indicated as the *Committer* in Figure 3.

5.2 Integrating Existing Identity Systems

The organizations participating in the network have their own centralized identity systems such as Azure Active Directory, OpenLDAP, Apache directory, IBM Tivoli, or similar. The credentials for each stakeholder in the system is maintained by the respective identity systems. A successful registration of a principal entity or telemarketer via a participant node on the network creates a cryptographic identity using standard public key infrastructure (PKI) methods and grants authentication to the network using digital signatures. Each node participating in the network stores their credentials and publishes the necessary public key information to other identity server nodes establishing a relationship between the identities of different organizations and the corresponding cryptographic keys needed for validation of transactions initiated over the network. This is indicated as the *membership service* in Figure 3.

5.3 Implementation of the Scrubbing Services

Scrubbing is a mandatory operation that needs to be performed on an input list of promotional phone numbers and other mandatory information as described in §4.2.4. These services are democratic and can be offered by anyone who willingly participates in the blockchain network after regulatory approval. The regulatory approval for the participants in the network is obtained after successfully scrubbing a standardized suite of test cases put together by the consortium and audit of the software system being used. The scrubbing operation reads the value associated with each key i.e. (hash of the phone number) from the consent and preference registries which are locally maintained in each participating nodes' key value data store as indicated in Figure 3. The scrubbing implementation can connect to the same database and filter the numbers from the input list provided and create the output files and encrypt them using the corresponding public keys of each of the telemarketers which can be obtained from the membership service.

To improve the speed of filtering through this data, we use the *event listeners* provided by the committer to listen to the completion events of block & transaction confirmation and mirror the updates to fabric's key value stores in a flexible format and re-indexing the data to optimize any queries over an open source in-memory database like *redis* with efficient and fast set difference implementations (`SDIFF`) compared to performing the same within document stores [53]. This enables extremely quick scrubbing results and the service is metered. Prior to this system, scrubbing was a time consuming operation as it involved the download of the entire data from NDND registry and reconciling the updates with their local databases before continuing to perform the telemarketing activities. Each scrub performed by the telemarketers was considered valid for a week thereby making it difficult for subscriber preferences to take immediate effect. The new system prevents this and enables immediate effect on subscriber preferences.

5.4 Integrating Existing End User Applications

End user applications like complaint registration systems, header, consent and content registration systems which need to interact with the blockchain system can continue to be built for users as traditional web applications by developers by reading the default key value data store provided by fabric or using a more performant mirror database for the global state of the blockchain. These end user applications can additionally also provide REST APIs or SDKs for their clients to interact with the blockchain using their node as a proxy. Self help portals provided by telecom operators can expose necessary APIs for their phone based and SMS based customer service systems to record complaints & register customer preferences.

The democratization of the scrubbing service operation on the network prevents any vendor lock-in for smaller telemarketers and allows potential organizations to experiment with various pricing models based on the quality of service provided therefore creating a healthy, fair and auditable ecosystem. A key goal for the introduction of scrubbing service providers is to decouple trust placed in the service. The ecosystem of scrubbing providers, and auditors on the network can verify the operations thereby incentivizing, and creating an ecosystem for provable operational compliance.

5.5 Automated complaint redressal & tracking

The availability of customer preferences and consents at any given snapshot, the content of the message sent, the customer phone number and the name of their telecom operator can be used to identify a transaction proposed by the telemarketer on behalf of a principal entity along with the proof of a scrubbing with the scrubbing token. This information can be replayed by observer/auditor nodes who register the complaint for validity. Using this approach, it becomes easy to find the participants who behaved maliciously and trace their actions which will be followed by a legal scrutiny. However, in a majority honest blockchain system such a situation would never arise because the encoded smart contract takes into effect these situations. If the situation still arises, it is due to a bug in the smart contract code and an updated policy with the contract can be issued to the blockchain for further usage by all the participants in the network with such a change being formally recorded.

However, Complaints against unregistered telemarketers making promotional calls without consent using previously leaked phone number data sets results in a complaint being registered with the maintenance of the watch list i.e. number of complaints registered against a specific number. On reaching a threshold number of violations, the observer nodes tracking the complaints can issue a special transaction requesting the telecom operators to provide the specific user degraded service. The telecom operators can then limit the total number of incoming or outgoing phone calls, SMS and access to mobile data of the violating subscriber behaving as an unregistered telemarketer and decide to terminate the phone number.

6 DEPLOYMENT CHALLENGES

With the regulation draft finalized after the demonstrated feasibility of the systems and released on 18 July 2018, the regulators set out with the ambitious goal to enforce the new requirements

starting Late December 2018 - Early January 2019. However, this received a lot of push back from the Cellular Operators Association of India (COAI) seeking the regulators pay attention to cost of implementation in the already financially-stressed telecom ecosystem indicating the technological overhaul to the current systems in place which become necessary due to the new mandate [8, 26]. Additionally the COAI rebut the proposed regulation indicating potential migration of users to over the top (OTT) services like WhatsApp, making the solution redundant after significant investments [26]. However, COAI eventually realized that (1) they could not block the regulation through legal challenges, (2) the telecom operators could work together to reduce costs, and (3) the inclusion of a small scrubbing charge could defray the expenses.

The adoption of new technological architecture posed significant risk of service disruption to the telecommunications operators in India who eventually decided for a phased roll out of the infrastructure and developed a "code of practice" (CoP). The CoP describes how existing business operations would be transformed due to the new blockchain architecture, and helped establish a common procedure to be encoded into a smart contract for programmatic enforcement, essentially mandating all telecommunications operators to coordinate. In addition, the adoption of these systems faced 6 legal challenges since 2020 with cases filed in the Delhi and Karnataka High Courts, as well as the Supreme Court of India, by various telemarketers, and principal entities. A Public Interest Litigation (PIL) filed by advocate Reepak Kansal in the Supreme Court of India (*Kansal v. The Union of India*) incorrectly argued to scrap the TCCCPR regulations on account of violating citizens' fundamental right to privacy due to the system creating a "priceless, mega database of commercial relationships" of over a billion individuals [36]. A 3 judge bench of the supreme court after reviewing the request refused to entertain the PIL request on 28th September 2020. Additional cases filed by a large mobile wallet and banking provider (One97 Communications, parent company of PayTM) used the updated TCCCPR'18 regulation to sue Telecom operators for failing to curb fraud of their registered header due to the similar deceptive headers, supporting the need for enforcement of the updated regulation. Smaller telemarketers filed legal cases claiming the new regulation hurt small businesses citing scrubbing enforcement resulting in over 80% drop in their message volume (*Shivtel Communications v. The Union of India* [Writ Petition (Civil) 3519/2021] at the Delhi High Court).

Eventually, the TCCCPR'18 regulation went into regulatory effect on 28th February 2019. This was followed by the enforcement of header registrations over the established blockchain network and scrubbing in September 2020, and soon followed by the need for registered templates and its inclusion in the scrubbing process on 8th March 2021.

The regulatory mandate was eventually adopted and put to practice adhering to the telecom operators' code of practice and included header, and content template registrations for the principal entities consuming SMS services. In §7 we present, various results from a longitudinal study of spam and SMS messaging in India, and argue the effectiveness of the implemented solution to operate at the scale of a growing telecom market like India, improved compliance of registered telemarketers reducing spam, while improving the security and privacy of subscribers across the country who benefit from the large scale deployment of the system.

Despite the efforts and quantifiable evidence presented in this paper from a longitudinal study of spam and complaints in the Indian telecom ecosystem, the problem of spam has not yet fully been addressed with increasing spam being reported from phone numbers outside the regulated advertising ecosystem. We detail the challenges faced and outline research challenges in future work presented in §8, and §9.

7 SYSTEM EVALUATION

The deployment of the infrastructure complying to the TCCCPR'18 regulation opened up new opportunities for businesses to enter the telecom ecosystem and provide services to existing telecom operators and telemarketers. While the ecosystem through their code of practice and deliberations agreed to scrub both transactional (header + template scrubbing), and promotional (transactional + preferences + consent) messages, continue using Hyperledger Fabric in their production deployment, various services like header, template, consent, scrubbing services were implemented directly by telecom operators, or other companies providing services to the telecom operators. As of today, the blockchain network consists of 7 Fabric orderer nodes run by the individual telecom operators (Vodafone-Idea Limited [VIL], Bharat Sanchar Nigam Limited [BSNL], Mahanagar Telephone Nigam Limited [MTNL], Airtel, Reliance Jio, Quadrant Televentures Limited [QTL], and Tata telecommunications). The network uses the Hyperledger Fabric v2 running RAFT consensus protocol in its deployment [1, 52] with each operator running their own certificate authority (Fabric CA) in the blockchain network [1]. We present our results below from one large scrubbing service provider in the ecosystem, and present evidence of reducing complaints, and increased adherence to the regulation in India.

7.1 Boostrapping: Header & Template Registrations from Principal Entities

By January 2020, the TCCCPR'18 regulation was very well known and the intent understood within the telecom operators. However, the fragmented ecosystem of principal entities relied on API partners providing them SMS services or telemarketers. Many of these stakeholders were unaware of the nuances of the new approach and how it could possibly disrupt their businesses. Many of them also did not pay attention to the notices from the telecom operators to register themselves again. Despite the readiness of the blockchain network in September 2019, the lack of engagement from businesses resulted in the slow on-boarding of principal entities and their registered headers into the new architecture.

This can be seen in Figure 4 with the solid red line denoting the registration of businesses. The spike in registrations seen between April 2020 to August 2020 was due to the issuance of multiple *sunset date* warnings and notifications to non-compliant businesses about the strict scrubbing operations to be in-effect in the future resulting in a possible drop in their SMS messaging traffic. This resulted in increased awareness among some businesses about the new regulations and anticipating future requirements for content template scrubbing also registered their content templates used

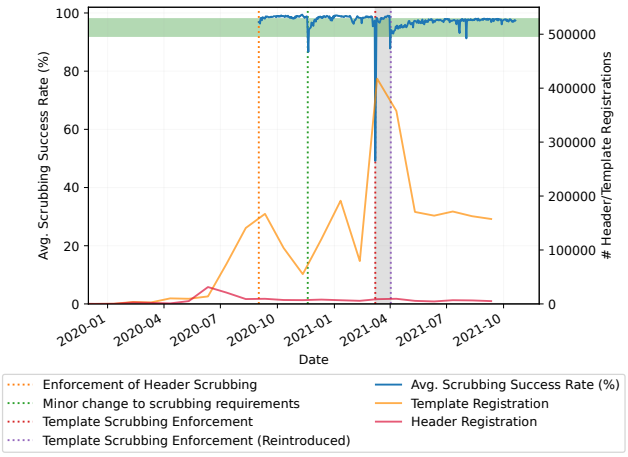
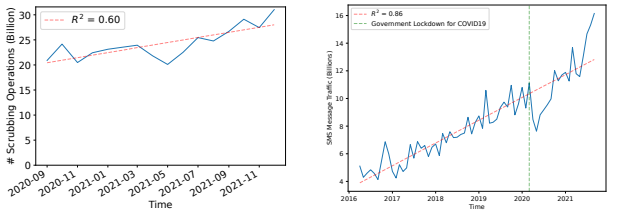


Figure 4: The figure shows the timeline of header (red) and template (yellow) registrations before the enforcement of the various phases of the regulations. The solid blue line indicates the scrubbing success rate and highlight various events resulting in a drop in the success rate. The green band shows the percentage success scrubbing events between 93 and 98% respectively. The grey vertical band indicates the temporary relaxation of scrubbing constraints after a country wide drop in SMS traffic.



(a) The plot shows the increasing number of scrubbing operations being performed by one large scrubbing service provider managing the scrubbing operations for over 60% of the registered businesses in the ecosystem

(b) The plot indicates the total number of SMS messages being sent by one single provider and indicates an increasing trend and usage of SMS messages across the country.

Figure 5: Volume of Scrubbing requests and SMS Messages Across India

for messaging obtaining a registered template ID. This is shown in Figure 4 with the solid gold line indicating an increase in the number of template registrations between April 2020 and October 2020. The proactive measures taken to prevent lookalike headers during the registration phase resulted in over 23890 headers being rejected during registration. Post enforcement of header scrubbing, over a year in operation, not even a single complaint citing fraud was registered against any registered headers.

7.2 Effectiveness of Scrubbing Services

As the number of registrations of principal entities reached their previously registered quantities effectively signifying the transition of businesses towards the new architecture, the registered header scrubbing rules were enforced. The enforcement of these rules on 1st September 2020 (indicated by the dotted vertical orange line), meant that only the registered telemarketers could send promotional messages through the official established advertising channel.

We define successful scrubbing as the percentage of phone numbers from the submitted list of numbers, to which a successful message has been delivered. For example, a marketing campaign with 10000 phone numbers has a 99% scrubbing success rate, if 9900 phone numbers provided by the telemarketers are in compliance and receive messages. The high scrubbing success rates could be for two reasons, (1) the default *opt-in* model of promotional messages in the country could indicate majority numbers who have not exercised their DND preferences, and (2) the telemarketers have slowly become compliant and only send messages to phone numbers who have expressed an explicit preference, or are default *opt-in* subscribers.

The new architecture and scrubbing requirements proved effective with an average over 95% success rate in scrubbing on the first day gradually improving to over 98% with compliant telemarketers removing the phone numbers from campaigns pro-actively. This is presented in Figure 4 as the solid blue line indicating the high number of successful scrubbing operations between September 2020 and November 2020. On 19th November 2020 (indicated by the dotted vertical green line), the operators updated their scrubbing requirements and operational workflows causing some message failures and degraded performance of the scrubbing system reducing the success rate to 85%. However, this error was transient and was quickly addressed within a day resulting in over 95% success rate. These results indicate the effectiveness of the scrubbing system in successfully identifying the 200M users in an ecosystem of a Billion exercising their preferences, and correctly preventing message delivery.

The number of scrubbing operations to perform also increased over time with the scrubbing system currently handling 50% more operations than it originally did when the system came into effect in September 2020, now handling over 30 Billion SMS scrubbing operations. The Figure 5(a) shows the increasing trend of scrubbing operations issued to the scrubber due to the increasing number of active SMSs being sent in the country (shown in Figure 5(b)). However, it is important to note that the measurement in Figure 5(b) only represents a partial view from one large operator and not the entire ecosystem. The overall ecosystem sends about a Billion SMS messages a day [37].

On 8th March 2021, the template scrubbing enforcement came into effect updating the scrubbing services to not only scrub verified headers and subscriber numbers but also validate the template of the message being sent. This resulted in an outage and a large drop in SMS delivery across the country with many critical banking, authentication, COVID-19 Vaccine registration information, and payment transaction messages being dropped resulting in only 49.2% of messages being delivered after scrubbing [38]. In addition to incorrect usage of template IDs in 41% of the cases, and 5% text mismatches between the registered templates, the major reason

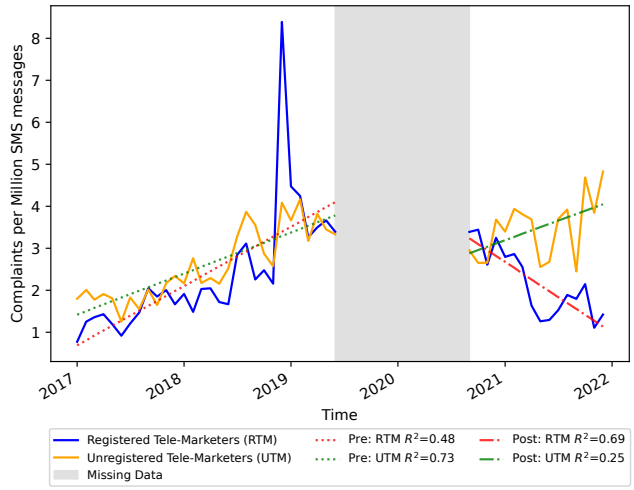


Figure 6: The plot shows a timeline of number of complaints against registered and unregistered telemarketers over time. The introduction of the blockchain system shows a decrease in the number of complaints against registered telemarketers while the number of complaints against unregistered telemarketers, and total complaints registered continue to rise.

for the failure (54%) was the lack of registration of templates by businesses due to possible miscommunication, or negligence. The disruptive nudge due to the drop of message traffic resulted in a spike in registrations as indicated by the orange line on March 2021 in Figure 4. With the intervention of the regulator, the scrubbing process was relaxed for a week and eventually put into effect on 2nd April 2021 causing a minor disruption with drop in scrubbing success to 90% before being returning to over 95% success rate within a week.

The green bands show consistent successful scrubbing operations between 92%-98%. The overall mean success rate for scrubbing during the lifetime of the operations presented is μ=97.5%, standard deviation σ=3.01%, and Median M=97.8% indicating proactive efforts to curb spam, and improved operational practices by the telemarketers.

7.3 Effect on Complaints Registered by Subscribers

We use public records of the complaints registered by subscribers to TRAI through the app [48, 49], or through their telecom operators and classify them into complaints against registered telemarketers (RTM) and unregistered telemarketers (UTM) based on the complaint against a specific registered header or against a valid 10 digit personal phone number through which unregistered telemarketing messaging has been carried out.

We present our results in Figure 6 and present the pre-blockchain and post-blockchain trends. The missing information between mid 2019 (development of the blockchain system), to mid 2020 (enforcement of mandates) is due to missing logs, and telemetry failures, resulting in data inaccuracies during the transition of systems. Historical data from 2017 to mid 2019 show an increasing number of complaints per million SMSs sent being registered. After the implementation of the blockchain based architecture and mandatory scrubbing, we notice a strong reducing trend (R^2=0.69, indicated by the solid blue line) in the number of complaints against RTM with complaints down to 1.13 registered complaints per million SMS messages sent indicating the effectiveness of the system in reducing the mean complaints against RTM from 2.39 during mid 2019 indicating over 50% improvement in the ecosystem, and increasing the marketers regulatory compliance. During the same phase, the number of complaints against UTM increased to 4.82 registered complaints per million messages sent (indicated by the solid orange line) making it easier for law enforcement authorities to identify spammers, fraudsters, and businesses violating subscriber consent.

However, the blockchain deployment phase, saw an increasing awareness among the subscribers who continued to report more complaints than in previous years. A majority (>75%) of these complaints registered were against unregistered telemarketers resulting in such accounts used being banned, throttled, or blocked by the telecom operators. The reduction in the number of complaints against RTM despite the increasing number of overall registered complaints demonstrates the efficacy of the deployed system, and its role in delivering the intended impact.

8 LIMITATIONS

While the development, deployment, of the proposed solution, a year into its operation has shown promising results as shown in §7, the practical deployment of the blockchain system deviated slightly from its original proposal, and did not yet address its promise of curbing spam now increasing through unregistered telemarketing channels or due to voice calls. We outline some of the current limitations in our work below.

8.1 Addressing Spam Calls and Unregistered Telemarketing Actions

Despite its ambitious inclusion in the TCCCPR'18 regulation to use the same technology proposal to address voice calls and completely curb UTM spam, the risk posed due to nation wide service outages and possible privacy violations resulted in the currently deployed solution completely detached from addressing robocalls (with automated voice, or human agent). While it is theoretically possible to perform content registration as spoken script templates in the current system, performing real-time checks of live calls is extremely difficult. It is also extremely hard to validate a complaint registered against a spam call without having access to the recordings of the conversations. Most telecom operators do not maintain this information but have provisions to explicitly target and do so for future calls to aid law enforcement actions when presented with a legal warrant. Performing these operations on every call is similar to wiretapping and severely compromises the privacy of subscriber communications since every phone call might potentially need to be monitored for identifying unregistered telemarketing calls initiated from malicious subscriber devices. The risks involved due to the voice data being biometric, and the severe impacts on privacy (intercepted SMS/voice information), implications on democracy,

make this an extremely hard problem to tackle and open up opportunities for research on privacy preserving approaches to achieve these goals.

8.2 Challenges with Delegations and Trust Relationships

The current deployment of the blockchain system in practice aims to have minimal disruption to principal entities carrying out their operations. Ideally, the principal entities would need to manage their cryptographic key identities and issue transactions (sending SMS / scrubbing) through the telemarketers. However, this would prevent various small businesses relying on SMS based marketing to gain experience and manage their keys. To simplify usage, the telemarketers act as delegated entities to the businesses and manage their keys, issue operations on their behalf. While the approach is a practical way to achieve the goals, it puts telemarketers at possible risk due to attacks from malicious adversaries wanting to compromise their systems and issue malicious transactions masquerading as the telemarketer affecting both the brand reputation of the principal entities and the telemarketers. The principal entities also in the process, continue to trust the telemarketers with plaintext phone numbers to send messages to which could be leaked to competing businesses by the telemarketer despite the telemarketer operating on hashed information when operating on the blockchain network. Scrubbing nodes are trusted not to misuse the phone numbers they receive from telemarketers in today's operations with active roadmap by the ecosystem to move towards reducing the trust placed in the service.

8.3 Complexity, and Usability of Consent

The current blockchain system and scrubbing systems continue to enforce the seven high level categories and do not extend to the fine grained preferences and consent management allowing subscribers to exercise their explicit choices. Additionally, the workflows for recording digital consent, using them is incomplete and not standardized. Enabling fine grained preferences and clearly enabling subscribers to exercise their consent has user experience challenges and needs changes to various portals implemented by TRAI, Telecom operators, and mobile applications to be updated. However, the current system in place is highly extensible and can support these needs in the future. Additionally, the extension of the header registrations to full business names instead of 6 character alphanumeric codes has not yet been implemented.

8.4 Translation of Code of Practices to Smart Contracts

The code of practices established by the telecom operators identify various ways in which the telecom operators can inter-operate with other participants on the blockchain. However, the combined effort at translating the operational business logic into programmatic enforcements on the blockchain as smart contracts comes with the challenge of long deliberations among the participants before any changes are made which could impact business flow. Additionally, these smart contracts are agreed upon by the participants and have not yet received an audit for correctness of operations.

9 DISCUSSION

The proposed solution in this paper stems from the idea of allowing mobile subscribers complete control and transparency of their preferences. The solution introduces a procedure to manage and acquire consent digitally which can be used in more cases in the future such as granting consent to insurance companies to view health records, employers to access educational records etc.., The role of blockchain in Telechain is the first formal experiment with blockchain in the Indian government (also the first in the telecom industry worldwide), and is highly motivated with the idea of avoiding spam altogether by being compliant ex-ante instead of validating a complaint ex-post and holding an organization or entity to blame. The usage of blockchain in telecommunications in India which is rapidly growing is a chance for regulators to establish the potential of the technology to perform at scale and explore new areas where such technology could create a significant impact and avoid single points of corruptibility.

9.1 Strengthening Credibility, Collaboration & Standardization

The usage of a blockchain while ensuring that the information can be accessed and read by anyone is a move to establish transparency which results in trust. By using blockchain and adopting the newly proposed systems the telecom operators in the telecom ecosystem can establish credibility by instantly taking into effect the subscriber preferences. The collaboration of the telecom operators of the country enabled via the network proves the ability of the technology to bring together mutually untrusted competitors, share necessary information and co-exist while still maintaining their business advantages. The usage of blockchains brings in the need for standardization and establishment of a common code of practice and cooperation between the entities.

9.2 Cost and Benefits of the New Model

While the creation of the blockchain network and securing it takes an investment of time and money, it also opens up new business opportunities. For example, We witnessed the growth of third party services monetizing services such as registration of headers, content and consent management, and providing scrubbing services. The ability to perform targeted reach to customers improves economic efficacy of telemarketers. The decentralized infrastructure improves adherence to regulations, makes participants responsible for each others' correct operations, and therefore prevents heavy penalties on the telecom operators and telemarketers while reducing the need for active regulatory oversight. The telecom operators and participants on the blockchain need to delegate dedicated infrastructure towards the network. We believe the costs of the infrastructure will be offset by the new business opportunities provided by improved quality of service and targeted reach.

9.3 Ever growing data sizes & Data storage

The tamper proof and immutable nature of the blockchain means that the data continuously grows with time. The usage of data storage containers outside the blockchain to store paths to the previously scrubbed results results in increasing data storage costs due to space requirements. This information serves as valuable

archival evidence for any future issues but can never be deleted without destroying the integrity of the blockchain.

9.4 Practical Security of Blockchain Systems

Blockchains enable mutually untrusted parties to collaborate and work together in a similar fashion. Blockchains if implemented correctly result in secure systems but there are various points where data leaks on the system can turn into security challenges. Any leak of keys stored in the membership services will result in malicious entities proposing faulty transactions. Similarly, colluding participants who can establish a majority in the network can tamper data and force the honest participants out of the network. While this can be counteracted with a policy stating that every single participant should validate the same content, it has an adverse impact on the performance and throughput of the system. The greatest risk to the consortium blockchain is posed by malicious system administrators who have privileges to the network and modify the network settings or tamper the keys maintained on the machine. However, these can be avoided by establishing an automated, verifiable and auditable release process. Consortium blockchains prove to be efficient in cases where mutually untrusted participants come together with a neutral regulatory oversight or auditor.

9.5 Extensibility to Spam Calls, and Mobile Number Portability

While the current proposed system focuses on curbing the issues due to unsolicited text messages, the same components on the blockchain can be used for tackling unsolicited phone calls. The TCCCPR'18 regulation takes into account the usage of the same architecture to curb spam phone calls. To avoid providing the scrubbed phone numbers to telemarketers, the scrubbing services provide aliased phone numbers which can be accessed via API interfaces on the blockchain enabling call based marketers to initiate calls to scrubbed numbers. This is done by initiating a Voice over IP (VoIP) based session with the telecom operator and providing the necessary scrubbing tokens received during scrubbing with authentication. The telecom operator validates and initiates the phone call to the actual number of the subscriber from the aliased value in the scrubbed list. Enabling such a solution would involve the 400-500 registered telemarketers in the country making phone calls to establish VoIP based SIP trunks with their partner telecom operators, update software to look up and initiate a connection than using an aliased phone number. By integrating such an approach, the drawback however is that the telemarketing agent initiating the call would not be able to look up the necessary information of the person being called without reconfirming their phone number and authenticating its match to the aliased number using APIs provided by the blockchain services. Implementing this process might extend the duration of the telemarketing call but help curb the problem of automated dialing calls or robocalls in the country.

9.6 Learning from Deployment

While the implementation of the proposed system, with the support of the ecosystem and driven by regulatory mandate resulted in partially achieving the goals we ambitiously set out with, it becomes evident that the adoption of the technology improves various high latency business operations involving synchronization and bring them towards real-time or near real-time latencies. Updates to subscriber consent now happens within minutes, and are used for scrubbing operations essentially reducing the time for consumer preferences to be in effect from 7-14 days in the past to within an hour and more ambitiously within minutes indicating an order of magnitude improvement in national scale operations. Additionally various fears from telecom operators about the loss of potential business posed by strict scrubbing requirements to over the top app channels such as WhatsApp, Telegram, etc.., remain unfounded due to the increasing volume of SMS as shown in Figure 5(b).

The usage of the blockchain as a shared ledger allowed for more efficient tracking of complaints, with better information sharing established between telecom operators to identify the reasons for fraud and take immediate corrective action. This has resulted in uncovering fraudulent registrations by a few businesses with different telecom operators. With data sharing practices enabled through the blockchain, the different telecom operators could identify businesses registered under different names and carry out fraudulent activities. While the results presented indicate that the problem of spam is reducing through official advertising channels (Application to Person messaging), it is slowly moving towards a peer to peer model and being carried out by telemarketers masquerading as regular phone subscribers. The movement of spam to peer to peer channels makes it extremely difficult to identify the originator with current techniques without breaching the privacy and reading all the messages being sent by the subscribers. A recent survey by *LocalCircles* indicated that 74% of the respondents continue to receive unwanted SMSs despite being registered on the NDND registry with 26% of them claiming these messages originate from service providers, or offers to earn more money [77]. Future efforts at privacy preserving techniques to identify spam need to be extensively tested, deployed, and improved through iteration.

The changes to the NDND registry and hashing the necessary information resulted in malicious actors either performing rainbow table attacks or performing a brute force sweep of phone numbers given known telecom operator and regional prefixes but can easily be avoided by using keyed hashes [80]. It becomes necessary to deploy *honeypot* solutions which detect such attackers, and filter them pro-actively amongst billions of legitimate subscribers without infringing on the privacy of the subscriber.

10 CONCLUSIONS & FUTURE WORK

In this paper we look into the history of regulatory and technological initiatives taken to combat the problem of unsolicited commercial communication in the telecommunication industry. We detail the challenges in the current business processes adopted by stakeholders in the ecosystem and propose a new consortium blockchain based architecture intended to address the problem of unsolicited commercial communication. We propose a solution using blockchain architecture that improves subscriber experiences, regulatory compliance and also creates a vibrant ecosystem with economic opportunities for potential enterprises to operate in the telecom industry. The proposed solution has been incorporated into the latest regulation for UCC (TCCCPR'18) in India announced on *19 July 2018*.

The solution has proven to be effective and operational at the scale of India, the second largest telecom market in the world with over a Billion active subscribers and with a message flow of over a Billion daily SMSs. The solution adequately met the design goals improving the speed, and efficiency of telecom operations, in addition to security, and privacy by preventing the sharing of plaintext subscriber information over the network. The implementation and enforcement of various suggestions in the proposal have significantly resulted in reduction of spam from organized advertising channels but see the flip effect of spam moving towards unorganized and peer to peer unregistered telemarketing practices needing further innovations. The establishment of the blockchain network enables new use cases such as mobile number portability and could also be applied to several other telecom services.

While present in the regulatory mandate, the current work does not yet establish a national consent registry allowing subscribers to exercise their ability to provide, and retract consent for advertising. However, the realtime nature of the new infrastructure will ensure that the consent options when introduced will take immediate effect. Alternate efforts such as the focus on STIR/SHAKEN protocols improve identity and authenticity of users in telecom networks and could complement the efforts taken in this work towards identifying unregistered telemarketers masquerading as individual subscribers [14, 43, 88]. We leave this as future work for subsequent versions of *Telechain*. The use of consortium blockchains with regulatory oversight is a promising way for governments to approach operational challenges involving mutually untrusted participants and enable cooperation to simplify and streamline their business operations while ensuring regulatory compliance. The effectivness of the solution described in this work inspired other countries such as the United Arab Emirates (UAE) to adopt the same blockchain based approach to curb spam in the UAE.

ACKNOWLEDGMENTS

We are incredibly grateful to the deep commitment and efforts put in by various individuals who made this work possible, including telecom operators, individuals, organizations, and various stakeholders who engaged actively with the consultation papers. We thank all the stakeholders for their active feedback during the design, development, deployment of the infrastructure and Telecom Regulatory Authority of India for enabling these discussions. We'd like to thank various teams from Microsoft Research India, Microsoft Global Delivery, TechMahindra, and Baohua Yang from the Linux Foundation Hyperledger for their support during the development of prototypes. We'd like to acknowledge the valuable feedback provided on the paper by the anonymous reviewers, Waylon Brunette, Matthew Johnson, Miranda Wei, Ananditha Raghunath, and members of the ICTD Lab at the University of Washington.

REFERENCES

[1] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18)*. ACM, New York, NY, USA, Article 30, 15 pages. https://doi.org/10.1145/3190508.3190538

[2] Yahel Ben-David, Shaddi Hasan, Joyojeet Pal, Matthias Vallentin, Saurabh Panjwani, Philipp Gutheim, Jay Chen, and Eric A. Brewer. 2011. Computing Security in the Developing World: A Case for Multidisciplinary Research. In *Proceedings of the 5th ACM Workshop on Networked Systems for Developing Regions (NSDR '11)*. Association for Computing Machinery, New York, NY, USA, 39–44. https://doi.org/10.1145/1999927.1999939

[3] Ben Patterson, PC World. 2014. How to stop SMS spam on your Android or iOS phone. https://www.pcworld.com/article/2848988/. Online.

[4] Broadband India Forum. 2018. Final BIFResponse to TRAI draft Regulations the Telecom Commercial Communications Customer Preference Regulations, 2018. https://trai.gov.in/sites/default/files/BroadbandIndiaForum28062018.pdf. 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] Miguel Castro and Barbara Liskov. 1999. Practical Byzantine Fault Tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99)*. USENIX Association, USA, 173–186.

[7] Idea Cellular. 2018. Idea Cellular Response to Draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/Idea28062018.pdf. Online.

[8] Cellular Operators Association of India (COAI). 2018. COAI Response to Draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/COAI28062018.pdf. Online.

[9] COAI. 2019. Cellular Operators Association of India. https://www.coai.com/. Online.

[10] Consumer Education and Research Centre. 2018. CERC Comments on the Draft Telecom Commercial Communication Consumer Preference Regulations, 2018. https://trai.gov.in/sites/default/files/ConsumerEducationandResearchCentre28062018.pdf. Online.

[11] Consumer Protection Association. 2018. Comments on Telecom Commercial Communication Consumer Preference Regulations, 2018. https://trai.gov.in/sites/default/files/ConsumerProtectionAssociation28062018.pdf. Online.

[12] Council of European Union. 2002. Council regulation (EU) no 58/2002. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32002L0058.

[13] 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

[14] Gregory W. Edwards, Michael J. Gonzales, and Marc A. Sullivan. 2020. *Robocalling: STIRRED AND SHAKEN! - An Investigation of Calling Displays on Trust and Answer Rates*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376679

[15] Enterprise Ethereum Alliance. 2018. Enterprise Ethereum Client Specification V2. https://entethalliance.org/wp-content/uploads/2018/11/EEA_Enterprise_Ethereum_Client_Specification_V2.pdf. Online.

[16] Federation of Consumer and Service Organizations. 2018. Forwarding our view on Telecom Commercial Communication Consumer Preference Regulations, 2018. https://trai.gov.in/sites/default/files/FedrationConsumernServiceOrganisation28062018.pdf. Online.

[17] Bulk SMS Gateway. 2022. Bulk SMS Services Pricing India, Bulk SMS Price List, Bulk SMS Rates in Hyderabad, India. https://www.bulksmsgateway.in/sms-pricing. (Accessed on 02/25/2022).

[18] Gopal Sathe, Huffington Post India. 2018. India's Latest Data Leak: People's Aadhaar Number And Bank Account Are Just One Google Search Away. https://www.huffingtonpost.in/2018/07/11/indias-latest-data-leak-is-so-basic-that-peoples-aadhaar-number-bank-account-and-fathers-name-are-just-one-google-search-away_a_23479694/. Online.

[19] Hindustan Times. 2017. McDonald's India app 'leaks' 2.2mn addresses, phone numbers; card details safe. https://www.hindustantimes.com/tech/mcdonald-s-india-app-leaks-customer-data-for-more-than-2-2-million-users/story-1EBCFinC4NItlfpyfj43VM.html. Online.

[20] Indian Cellular Association. 2018. Response to the Draft Telecom Commercial Communication Consumer Preference Regulations, 2018. https://trai.gov.in/sites/default/files/IndianCellularAssociation28062018.pdf. Online.

[21] ITU-APT Foundation of India. 2018. ITU-APT Comments in relation to Draft Telecom Commercial Communication Consumer Preference Regulations, 2018 released by TRAI. https://trai.gov.in/sites/default/files/ITUAPTFoundationofIndia28062018.pdf. Online.

[22] Javed Anwer, India Today. 2016. Dear Indians, have mercy on others and STOP using Truecaller. https://www.indiatoday.in/technology/talking-points/story/dear-indians-have-mercy-on-others-and-stop-using-truecaller-360275-2016-12-30. Online.

[23] Jehangir B Gai. 2015. Telecom service providers liable for violation of 'DND' facility. https://timesofindia.indiatimes.com/city/patna/Telecom-service-providers-liable-for-violation-of-DND-facility/articleshow/48841277.cms. Online.

[24] Nan Jiang, Yu Jin, Ann Skudlark, and Zhi-Li Zhang. 2013. Greystar: Fast and Accurate Detection of SMS Spam Numbers in Large Cellular Networks Using Gray Phone Space. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Washington, D.C., 1–16. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/jiang

[25] Nan Jiang, Yu Jin, Ann Skudlark, and Zhi-Li Zhang. 2013. Understanding SMS spam in a large cellular network. *ACM SIGMETRICS Performance Evaluation Review* 41, 1 (2013), 381–382.

[26] 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-on-spam-calls-on-hold-for-now/1248705/. (Accessed on 03/02/2022).

[27] Shirsendu Troy Karmakar. 2018. My response to the draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/ShirsenduTroyKarmakar28062018.pdf. Online.

[28] Katie Bernard. 2019. FCC: Nearly half the calls you receive this year will be spam. https://www.cnn.com/2019/02/14/politics/fcc-robocalls-report/index.html. Online.

[29] Dennis WK Khong. 2004. The problem of spam law: A comment on the Malaysian Communications and Multimedia Commission's discussion paper on regulating unsolicited commercial messages. *Computer Law & Security Review* 20, 3 (2004), 206–212.

[30] Alex C. Kigerl. 2016. Deterring Spammers: Impact Assessment of the CAN SPAM Act on Email Spam Rates. *Criminal Justice Policy Review* 27, 8 (2016), 791–811. https://doi.org/10.1177/0887403414562604 arXiv:https://doi.org/10.1177/0887403414562604

[31] KOAN Advisory Group. 2018. Response to Draft Telecom Commercial Communication Consumer Preference Regulations, 2018. https://trai.gov.in/sites/default/files/KoanAdvisoryGroup28062018.pdf. Online.

[32] Nir Kshetri. 2017. Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly* 38, 8 (2017), 1710–1732. https://doi.org/10.1080/01436597.2017.1298438 arXiv:https://doi.org/10.1080/01436597.2017.1298438

[33] Younghwa Lee. 2005. The CAN-SPAM Act: a silver bullet solution? *Commun. ACM* 48, 6 (2005), 131–132.

[34] Quadrant Televentures Limited. 2018. Comments on Draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/QuadrantTeleventuresLtd28062018.pdf. Online.

[35] Reliance JIO Infocomm Limited. 2018. Comments on Draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/RelianceJioInfocommLtd28062018.pdf. Online.

[36] Himanshi Lohchab. 2020. PIL in SC seeks scrapping of Trai's new regulation on checking pesky calls/SMSes. https://economictimes.indiatimes.com/industry/telecom/telecom-news/pil-in-sc-seeks-scrapping-of-trais-new-regulation-on-checking-pesky-calls/smses/articleshow/78037732.cms. (Accessed on 03/02/2022).

[37] Himanshi Lohchab. 2021. SMS traffic back to nearly 1 billion per day under new system to check pesky messages. https://economictimes.indiatimes.com/industry/telecom/telecom-news/sms-traffic-back-to-nearly-1-billion-per-day-under-new-system-to-check-pesky-messages/articleshow/82211826.cms?from=mdr. (Accessed on 02/27/2022).

[38] Himanshi Lohchab and Devina Sengupta. 2021. trai: After OTP and SMS services disruption, Trai asks telcos to switch off new filter for 7 days - The Economic Times. https://economictimes.indiatimes.com/industry/telecom/telecom-news/telcos-told-to-switch-off-sms-filter-for-7-days/articleshow/81421300.cms. (Accessed on 02/27/2022).

[39] Bharti Airtel Ltd. 2018. Response to Draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/BhartiAirtelLtd28062018.pdf. Online.

[40] Ujwal Makhija and Phonon Communications Private Limited. 2018. Comments on the Consultation Paper. https://trai.gov.in/sites/default/files/PhononCommunicationsPvtLtd28062018.pdf. Online.

[41] Data Privacy Manager. 2020. Italian DPA issued a €12.25 million GDPR fine to Vodafone for aggressive telemarketing. https://dataprivacymanager.net/italian-dpa-issued-e12-25-million-gdpr-fine-to-vodafone-for-aggresive-telemarketing/. (Accessed on 02/28/2022).

[42] Data Privacy Manager. 2020. €27,8 million GDPR fine for Italian Telecom -TIM. https://dataprivacymanager.net/e278-million-gdpr-fine-for-italian-telecom-tim/. (Accessed on 02/28/2022).

[43] Jim McEachern and Eric Burger. 2019. How to shut down robocallers: The STIR/SHAKEN protocol will stop scammers from exploiting a caller ID loophole. *IEEE Spectrum* 56, 12 (2019), 46–52.

[44] Microsoft. 2017. SMS Organizer - an Android app. https://www.microsoft.com/en-us/garage/profiles/sms-organizer/. Online.

[45] P. Mockapetris and K. J. Dunlap. 1988. Development of the Domain Name System. In *Symposium Proceedings on Communications Architectures and Protocols (SIGCOMM '88)*. Association for Computing Machinery, New York, NY, USA, 123–133. https://doi.org/10.1145/52324.52338

[46] Evangelos Moustakas, Chandrasekaran Ranganathan, and Penny Duquenoy. 2005. Combating Spam through Legislation: A Comparative Analysis of US and European Approaches.. In *Proceedings of the Fifth Conference on Email and Anti-Spam (CEAS)*. CEAS, Mountain View, CA, USA, 1–8.

[47] Akshay Narayan and Prateek Saxena. 2013. The Curse of 140 Characters: Evaluating the Efficacy of SMS Spam Detection on Android. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM '13)*. ACM, New York, NY, USA, 33–42. https://doi.org/10.1145/2516760.2516772

[48] Telecom Regulatory Authority of India. 2022. TRAI DND 3.0(Do Not Disturb). https://play.google.com/store/apps/details?id=trai.gov.in.dnd&hl=en-gb. (Accessed on 03/01/2022).

[49] Telecom Regulatory Authority of India. 2022. TRAI DND iOS Application. https://apps.apple.com/in/app/trai-dnd-do-not-disturb/id1443781196?ls=1. (Accessed on 03/01/2022).

[50] Telecom Regulatory Authority of India (TRAI). 2011. Press Release on Telmarketer Registration. https://www.trai.gov.in/sites/default/files/pr14jan11cndiv.pdf. (Accessed on 02/28/2022).

[51] Svein Ølnes, Jolien Ubacht, and Marijn Janssen. 2017. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly* 34, 3 (2017), 355 – 364. https://doi.org/10.1016/j.giq.2017.09.007

[52] Diego Ongaro and John Ousterhout. 2014. In Search of an Understandable Consensus Algorithm. In *2014 USENIX Annual Technical Conference (USENIX ATC 14)*. USENIX Association, Philadelphia, PA, 305–319. https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro

[53] Panoply. 2017. Redis Vs MongoDB. https://blog.panoply.io/redis-vs-mongodb. Online.

[54] Parliament of the United Kingdom. 1998. Data Protection Act 1998. https://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf.

[55] Bhavesh H. Patel. 2018. Views on draft UCC regulations released by TRAI on 29th May 2018. https://trai.gov.in/sites/default/files/BhaveshPatel28062018.pdf. Online.

[56] Morgen E Peck. 2017. Blockchains: How they work and why they'll change the world. *IEEE spectrum* 54, 10 (2017), 26–35.

[57] GPDP Garante per la protezione dei dati personali. 2020. Corrective and sanctioning measure against TIM SpA. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486. (Accessed on 02/28/2022).

[58] Fahad Pervaiz, Rai Shah Nawaz, Muhammad Umer Ramzan, Maryem Zafar Usmani, Shrirang Mare, Kurtis Heimerl, Faisal Kamiran, Richard Anderson, and Lubna Razaq. 2019. An Assessment of SMS Fraud in Pakistan. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS '19)*. Association for Computing Machinery, New York, NY, USA, 195–205. https://doi.org/10.1145/3314344.3332500

[59] Petlee Peter. 2018. SMS fraud: Conmen use malware to steal info from smartphones. https://timesofindia.indiatimes.com/city/bengaluru/sms-fraud-conmen-use-malware-to-steal-info-from-smartphones-siphon-off-money/articleshow/63753485.cms. Online.

[60] Vivekdeep Gupta | R3. 2018. Feedback on draft UCC regulations released by TRAI on 29th May 2018. https://trai.gov.in/sites/default/files/VivekdeepGupta28062018.pdf. Online.

[61] Bradley Reaves, Logan Blue, Dave Tian, Patrick Traynor, and Kevin R.B. Butler. 2016. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '16)*. Association for Computing Machinery, New York, NY, USA, 165–170. https://doi.org/10.1145/2939918.2939937

[62] Sandeep Kumar, Torsha Sarkar, Swaraj Barooah, Gurshabad Grover. 2018. Comments on the Telecom Commercial Communicaons Customer Preference Regulations 2018 | Center for Internet and Society. https://trai.gov.in/sites/default/files/TheCentreforInternetandSociety28062018.pdf. Online.

[63] Sudhakar Sharma and Syniverse. 2018. Comments on the Telecom Commercial Communicaons Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/SudhakarSharma28062018.pdf. Online.

[64] Prashant Shukla and Microsoft. 2018. Response to the Draft Telecom Commercial Communication Consumer Preference Regulations, 2018. https://trai.gov.in/sites/default/files/MicrosoftIndia28062018.pdf. Online.

[65] David E Sorkin. 1997. Unsolicited commercial e-mail and the telephone consumer protection act of 1991. *Buff. L. Rev.* 45 (1997), 1001.

[66] Stephanie Mlot. 2019. John Oliver Robocalls FCC to Prove Point About Robocalls. https://www.geek.com/tech/john-oliver-robocalls-fcc-to-prove-point-about-robocalls-1778084/. Online.

[67] Harish Sukhwani, José M. Martínez, Xiaolin Chang, Kishor S. Trivedi, and Andy Rindos. 2017. Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric). In *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*. IEEE, Hong Kong, 253–255. https://doi.org/10.1109/SRDS.2017.36

[68] Jeffrey D Sullivan and Michael B De Leeuw. 2003. Spam after Can-Spam: How Inconsistent Thinking Has Made a Hash out of Unsolicted Commercial E-Mail Policy. *Santa Clara Computer & High Tech. LJ* 20 (2003), 887.

[69] Telecom Regulatory Authority of India. 2018. Do Not Disturb 2.0. https://main.trai.gov.in/portals-apps/trai-apps. Online.
[70] Telecom Regulatory Authority of India - Government of India. 2007. The Telecom Unsolicited Commericial Communications Regulations, 2007. https://main.trai.gov.in/sites/default/files/201204190608149960110Regulation5june07.pdf. Online.
[71] Telecom Regulatory Authority of India - Government of India. 2010. The Telecom Commercial Communications Customer Preference Regulations, 2010. http://www.nccptrai.gov.in/nccpregistry/regulation1diccndiv.pdf. Online.
[72] Telecom Regulatory Authority of India - Government of India. 2017. Direction under Section 13 regarding unsolicited bulk SMSs related to investment in securities market. https://trai.gov.in/sites/default/files/Direction_10082017.pdf. Online.
[73] Telecom Regulatory Authority of India - Government of India. 2019. Direction under Section 13 regarding submission of Performance Monitoring Report to the Authority. https://trai.gov.in/sites/default/files/Direction_19062020.pdf. Online.
[74] Telecom Regulatory Authority of India - Government of India. 2019. Press Release on Telecom Subscription Data as on 31st December, 2018. https://main.trai.gov.in/sites/default/files/PR_No.13of2019.pdf. Online.
[75] Telecom Regulatory Authority of India - Government of India. 2020. Direction under Section 13 regarding implementation of Telecom Commercial Communications Customer Preference Regulations (TCCCPR) 2018. https://trai.gov.in/sites/default/files/Direction_19062020.pdf. Online.
[76] The Economist. 2017. Governments may be big backers of the blockchain. https://www.economist.com/business/2017/06/01/governments-may-be-big-backers-of-the-blockchain. Online.
[77] The Economic Times. 2021. 74% respondents getting pesky messages despite being in Trai's DND list: Survey. https://economictimes.indiatimes.com/industry/telecom/telecom-news/74-respondents-getting-pesky-messages-despite-being-in-trais-dnd-list-survey/articleshow/84334262.cms. Online.
[78] True Caller. 2017. SMS Categorizer. https://support.truecaller.com/hc/en-us/articles/360000767197-What-is-SMS-Categorizer-. Online.
[79] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. 2016. SoK: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 320–338. https://doi.org/10.1109/SP.2016.27
[80] James M Turner. 2008. The keyed-hash message authentication code (hmac). *Federal Information Processing Standards Publication* 198, 1 (2008), 1–13.
[81] United States Congress. 2003. Public Law 108-187-Dec16, 2003 - Controlling the Assault of Non Solicited Pornography and Marketing Act. https://www.govinfo.gov/content/pkg/STATUTE-117/pdf/STATUTE-117-Pg2699.pdf. Online.
[82] Value First Digital Media Pvt Ltd. 2018. Comments on the Telecom Commercial Communicaons Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/ValueFirstDigitalMediaPvtLtd28062018.pdf. Online.
[83] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, Article 25, 14 pages. https://doi.org/10.1145/3209811.3209818
[84] Gaurav Verma and Times Internet. 2018. Times Internet Limited's comments and observations on the Telecom Commercial Communicaons Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/TimesInternetLtd28062018.pdf. Online.
[85] Vodafone. 2018. Vodafone Comments to the TRAI's Draft Telecom Commercial Communications Customer Preference Regulations 2018. https://trai.gov.in/sites/default/files/VodafoneIndia28062018.pdf. Online.
[86] Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151 (2014), 1–32.
[87] Kuldeep Yadav, Ponnurangam Kumaraguru, Atul Goyal, Ashish Gupta, and Vinayak Naik. 2011. SMSAssassin: Crowdsourcing Driven Mobile-based System for SMS Spam Filtering. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications (HotMobile '11)*. ACM, New York, NY, USA, 1–6. https://doi.org/10.1145/2184489.2184491
[88] James Yu. 2021. An Analysis of Applying STIR/SHAKEN to Prevent Robocalls. In *Advances in Security, Networks, and Internet of Things*, Kevin Daimi, Hamid R. Arabnia, Leonidas Deligiannidis, Min-Shiang Hwang, and Fernando G. Tinetti (Eds.). Springer International Publishing, Cham, 277–290.