Shirsendu "Troy" Karmakar
Engineer | Previously QREOH, Solidry, LinkedIn, SlideShare | @troysk704
Draft

My response to The Draft Telecom Commercial Communications Customer Preference Regulations, 2018

The new TRAI draft regulation for commercial communications with the customer has made Blockchain based DLT (Distributed Ledger Technology) as its core. Most of the regulation is based on the belief that DLT technology is technically superior and suitable for storing customer commercial communication preferences. This is technically incorrect.

> Blockchain has proven useful where the objective is to cryptographically secure information and make it available only on need to know basis. Yet none may deny their actions or tamper with records, once recorded on the distributed ledger, which uniformly enforces compliance.
>
> Information to Press

The above statement is false. Blockchain hasn't been tested at scale anywhere in the world. Nor can Blockchain guarantee any security without the decentralised model.

Following are some of the definitions and regulations which have been used in the draft. I am reproducing them as I will be referencing them going forward.

(w) "Distributed Ledger Technologies (DLT)" means a set of technological solutions that enables a single, sequenced, standardized and cryptographically-secured record of activities to be safely distributed to, and acted upon, by a network of varied participants and their

(i) database can be spread across multiple sites or institutions;

(ii) records are stored one after the other in a continuous ledger and can only be added when the participants reach a consensus;

Distributed Ledger Technology(DLT)

(am) "Permissioned DLT networks" means those DLT networks where participants in the process are preselected and addition of new record on the ledger is checked by a limited consensus process using a digital signature;

Permissioned DLT networks

(bi) "Smart contract" means a functionality of intelligent and programmable code which can execute pre-determined commands or business rules set to pre-check regulatory compliance without further human intervention and suitable for DLT system to create a digital agreement, with cryptographic certainty that the agreement has been honored in the ledgers, databases or accounts of all parties

to the agreement;

Smart contract

13. Access Providers shall adopt Distributed Ledger Technology (DLT) with permissioned and private DLT networks for implementation of system, functions and processes as prescribed in Code(s) of Practice: -

(1) to ensure that all necessary regulatory pre-checks are carried out for sending Commercial Communication;

(2) to operate smart contracts among entities for effectively controlling the flow of Commercial Communication;

Obligation of Access Providers

36. Authority may set up or permit to set up a Regulatory Sandbox for testing implementation of regulatory checks using DLT networks and other technological solutions complementing DLT network(s) and to operationalize such regulatory sandbox, the Authority may, by order or direction, specify the requisite processes.

Chapter VII — Miscellaneous

The assumption seems to be that DLT is a safe datastore for storing user permissions. The draft doesn't define clearly who would be in-charge of running the permission and private DLT networks i.e. the definition of participants was missing.

Private and permissioned blockchain network is not secure.

Blockchain is a new technology which saw its first use in the cryptocurrency Bitcoin. Consensus among the Bitcoin miners define which transactions should be included in the next block. By making the Bitcoin network decentralised and free for anyone to join; it makes very tough for people to work together and add fraud transactions. To add fraud transactions; they will have to convince all the miners of the Bitcoin network of the fraud transaction which would add cost and hence become infeasible.

There are many charlatans in the tech industry who would give the name Blockchain to anything and everything but without the decentralised implementation using the word Blockchain is just misguiding. They are all trying to milk the hype cycle of Blockchain.

By making a network private; you are censoring the network from security audits as well as other independent verifications by anyone. And by making it permissioned; you are basically concentrating power with the Authority who gives permission and therefore bringing centralised solution. We have decades of experience in building centralised solutions using RDBMS and using Blockchain which is slow and expensive reflects poorly on the engineering decisions.

This is why a private blockchain is a bad idea.

Assumption 1

All data in a Blockchain is cryptographically signed and cannot be changed.

The truth is very far in the private and permissioned blockchain. All transactions can be changed if all/most members of the network decide so. The cryptocurrency Ethereum is a prime example of this. The currency was stolen by a hacker after he found flaw in the software. The founder of Ethereum rolled out a change which circumvented the transaction, thereby changing the Blockchain. This is often known as forking.

This is how it worked in a decentralised network, it is even a more serious problem in case of private networks where most members know each other.

Given a chance, Airtel, Jio, Vodafone etc. will collude to change the records of the transactions as they are businesses driven by advertising revenues. And if they wanted they could have fixed the problem of spam. They are not incentivied to do the same.

Recently, a “centralised” cryptocurrency (Bitcoin Gold) used this tactic to make double spend attacks on cyptocurrency exchanges by spending the same currency twice. The site; https://www.crypto51.app/; gives a dollar amount to do such attacks.

If the network is going to not have mining and just have stake; I would like to inform you that nowhere in the world has such technology been used at a scale which is even 0.01% of India scale.

Assumption 2

All requests on Blockchain are saved.

This is also not correct. On the blockchain network, whenever anyone wants to do a transaction/add entries; they broadcast the request on the network. Someone on the network has to accept it and add it to the blockchain. They are free to neglect it. On the Bitcoin network; this happens when a transaction has very less transaction charge linked to it. The miners; seeing that the poor financial reward is poor neglect the transaction. This is why there is a 10 minute wait time on the Bitcoin network for a transaction to complete.

Assumption 3

Storing user preferences in a sequential form is useful.

The access providers will want to query the data before sending the messages to a user. Therefore system which provides a random access is more suitable. In blockchain it is not trivial to pick a record whereas SQL powered databases like MySQL and Oracle have proven themselves are apt solutions.

Assumption 4

The records should not be modifiable.

Why would you want a solution where you cannot change the settings? User preferences will change and will need to get updated. Blockchain is not good at it. You may argue that you won't mutable the state of the old record and rather add a new record; but that will lead to questions around time. Any distributed systems engineer will tell you that it will be a slippery slope.

Assumption 5

Smart contracts are required.

Telecom is a regulated market and there are disputes. And these disputes often take place in the court of law. With no law around such digital tools; it is unwise to use it to implement data/resource sharing among business entities as it wouldn't hold up in the court of law. Also, in reality, negotiations happen and contracts change.

Smart contracts may work in Utopia but not in India. We have you, please regulate them by law.

. . .

I request you to look into history of spam filtering and use the learnings we had over there. I am happy to give inputs if it will help.

The following articles are good to have a better idea about the technology. These are by people in the industry who have actually built or educated about the tech for over 5 years.

"Private blockchain" is just a confusing name for a shared database

Banks and financial institutions seem to be the blockchain. It seems they agree with the Bitcoin community that the...

freedom-to-tinker.com

Why Blockchain is Hard

The hype around blockchain is massive. To hear the blockchain hype train tell it, blockchain will now:

medium.com

Alternatives to Blockchain

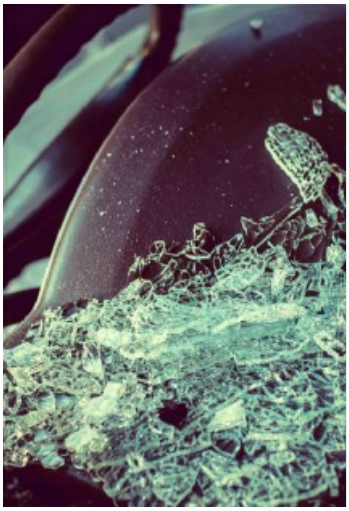
In my last article, I argued for why blockchain is not really a good fit for anything other than money. Blockchain as...

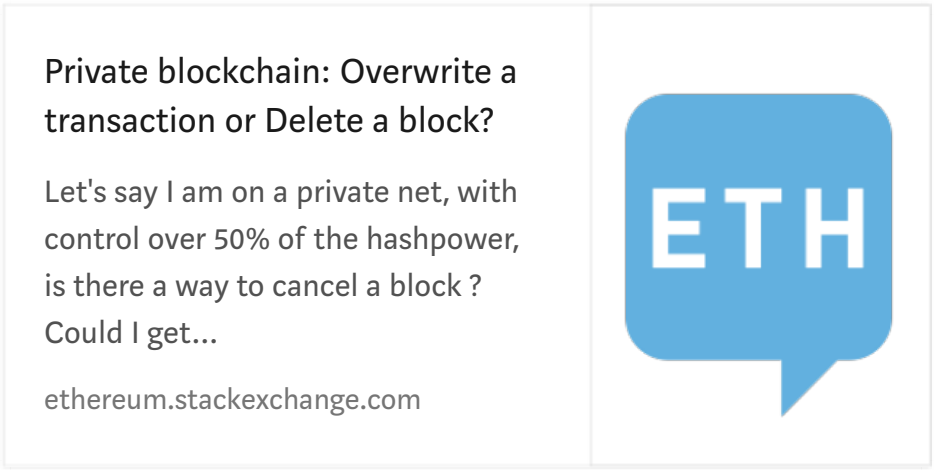
medium.com

Blockchain's Once-Feared 51% Attack Is Now Becoming Regular - CoinDesk

Monacoin, bitcoin gold, zencash, verge and now, litecoin cash. At least five cryptocurrencies have recently been hit...

www.coindesk.com





I hope you reconsider your decision to use an unproven bleeding edge technology for one of India's critical digital infrastructure.

. . .

Disclaimer: My observations are from a technical point of view. I have been working in technology for the past 16 years with corporate companies like TCS and LinkedIn as well as startups. I have no commercial interests in the Indian telecom sector. I am concerned about spam and India's digital infrastructure.