CIS Comments on the National Strategy on Blockchain

15th February, 2021

By **Vipul Kharbanda and Aman Nair**

The Centre for Internet and Society, India

Shared under

Creative Commons Attribution 4.0 International license

About CIS

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa. CIS is grateful for the opportunity to submit its inputs on the draft report on the National Strategy on Blockchain.

Executive Summary

This submission is a response by the researchers at CIS to the report "National Strategy on Blockchain" prepared by Ministry of Electronics and Information Technology (MEITY) under the Government of India.

We have put forward the following comments based on our analysis of the report.

I. **General Comments on the National Strategy**

1. There are currently a number of reports and policies on blockchain use across departments, ministries and even states. The absence of a harmonised blockchain policy across all departments and institutions of government must be fixed.
2. There are inherent dangers with viewing blockchain as a silver bullet solution.
3. Informational concerns with blockchain are existent and policies must be designed to reflect these concerns and minimise their occurrences.

II. **Section Specific Comments**

1. **Section 6.1** - There is a need for greater decentralisation and a shift away from a solely government operated blockchain
2. **Section 6.2**:
    a. The legality of blockchain also faces the hurdle of smart contracts
    b. The RBI decision to halt the use of cryptocurrencies was struck down by the Supreme Court
    c. The right to be forgotten exists as an extension of the right to privacy as well

3. **Section 7** - There is a need for greater detail and granularity in the report's analysis and in the suggestions and recommendations that it makes.

A. General Comments on the National Strategy

The report provides a comprehensive review and assessment of the potential benefits and challenges that are facing blockchain adoption in governance in India currently. However, the following section outlines some high level considerations that we believe should have been given additional thought when drafting the national strategy on blockchain.

1. Absence of a harmonised blockchain policy across all departments and institutions of government

The government of India, through its various departments and ministries, has issued a number of papers/policy documents on blockchain technology, some of the major ones being the Report of the Interministerial Committee on Virtual Currencies; Blockchain: The India Strategy by the Niti Aayog; Blockchain for Government Whitepaper by the National Informatics Center, etc.
This multiplicity of documents leads to confusion regarding the hierarchy of the various papers and the actual policy of the government. If different departments come out with different policy positions, then the stated purpose of policy clarity gets defeated which has the potential to slow the growth and adoption of this new technology. Thus there should be a single National Strategy Paper which should not only acknowledge the existence of the other papers, but also clarify that as a matter of government policy, the positions stated in this paper would take precedence over the others.

2. Danger of viewing blockchain as a silver bullet solution

Research into the potential application of blockchain into governance structures has consistently warned of an attitude of 'blind trust' that is oftentimes adopted by governments in this field.[1] A shift towards a blockchain led system of maintaining citizen's records, for example, would fundamentally shift the burden of trust from the institution managing the technology (in this case the government) onto the technology (blockchain) instead.[2] This presents problems of both accountability and response management when the technology

[1] H. Hou, "The Application of Blockchain Technology in E-Government in China," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 2017, 1–4, https://doi.org/10.1109/ICCCN.2017.8038519.

[2] Victoria Lemieux, "Blockchain for Recordkeeping; Help or Hype?," October 25, 2016, https://doi.org/10.13140/RG.2.2.28447.56488.

invariably faces a point of failure. This is again exasperated in cases wherein there are a multitude of actors and institutions involved without any clear delineation of roles and responsibilities, as is the case currently. This concern has also been expressed by the Niti Aayog.[3]

3. Informational concerns with Blockchain

Another key consideration is the policy questions surrounding data storage under a blockchain system.[4] Under the current proposed policy there is no clarity as to how certain data that will be stored within the blockchain is to be archived and maintained outside of the chain. If proposed that such data remain in the chain, there is no guarantee that such a strategy would be reliable and conducive to long term records maintenance.[5] Furthermore, there must be clear access mechanisms in place to allow for citizens accessing certain data such as data relating to functioning of public services (like court data) - with such data being essential in safeguarding civil liberties and rights.

At the same time, there are concerns regarding the misutilisation of data and records that are part of the chain. This is especially of concern in instances wherein data that is part of the chain is not binding for some reason (whether that reason be the data is outdated, or not legally binding). As noted here, "*...there is the risk that identity information authenticated on the Blockchain but which is otherwise invalid may find its way into traditional channels to enable creation of new, false identities, which could then be used to hide one's real identity.*"[6]

B. Section Specific Comments

The following comments are with regards to specific sections of the report where we believe either a clarification is required or additional context must be added.

1. Section 6.1 - Need for greater decentralisation

One of the reasons why Distributed Ledger Technology is considered to be safe is its

---

[3] Niti Aayog, "Blockchain: The India Strategy, Part 1", January 2020, available at https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf

[4] Victoria Louise Lemieux, "Trusting Records: Is Blockchain Technology the Answer?," *Records Management Journal* 26, no. 2 (January 1, 2016): 110–39, https://doi.org/10.1108/RMJ-12-2015-0042.

[5] Jason R. Baron and Drinker Biddle, "Blockchains: The Future of Recordkeeping?," *Legaltech News* (blog), accessed February 15, 2021, https://www.law.com/legaltechnews/almID/1202753737799/Blockchains-The-Future-of-Recordkeeping/?/.

[6] Clare Sullivan and Eric Burger, "E-Residency and Blockchain," *Computer Law & Security Review* 33, no. 4 (August 1, 2017): 470–81, https://doi.org/10.1016/j.clsr.2017.03.016. *In Charalampos Alexopoulos et al., "Benefits and Obstacles of Blockchain Applications in E-Government," 2019, https://doi.org/10.24251/HICSS.2019.408.*

decentralised nature which reduces a single point of vulnerability. However most of the use cases being discussed by the government in its various papers, seem to suggest the adoption of a permissioned blockchain rather than a public blockchain. In practice this might reduce the total number of nodes significantly since the particular blockchain would reside only on the computers of the closed system of the concerned department or limited stakeholders. If the departmental computers are linked through some other applications as well (such as a departmental portal, attendance system, etc.) then that could be a single point of vulnerability which may have the potential to affect a majority of the nodes. Such technical challenges should be acknowledged in the National Strategy.

2. Section 6.2 - Legal challenges faced by blockchain should also include the issue of smart contracts

Smart contracts are a growing area of blockchain application and the legal treatment of smart contracts, especially in relation to issues such as jurisdiction, enforceability, applicability of legal principles of contract law, etc. in a DLT framework is a challenge that needs to be addressed.

3. Section 6.2, Paragraph 1 - Inaccurate representation on the legality of cryptocurrencies (at the time of submission)

This paragraph is factually incorrect. The RBI had issued a circular to halt usage of cryptocurrency transactions in India, but that circular was struck down by the Supreme Court on March 4, 2020 in *Internet and Mobile Association of India* v. *Reserve Bank of India*, being Writ Petition (Civil) No.528 of 2018 with Writ Petition (Civil) No.373 of 2018

4. Section 6.2, Paragraph 4 - Right to be forgotten going beyond the Draft Personal Data Protection Bill

The “right to be forgotten”is not only a feature in the Draft Personal Data Protection Bill, 2019 but is also a recognised feature of the right to privacy which is a fundamental right.

5. Section 7 - Need for greater detail and granularity in analysis

While the National Strategy document recognises that there is a need to identify and apply Blockchain to the right processes and applications, a simple SWOT analysis given in the paper is not enough. A policy document as important as a National Strategy Paper by the Ministry of Electronics and IT should be much more granular and should at the very least contain the basic principles that need to be kept in mind while making such an analysis. The blockchain Use case selection framework contained in the Niti Aayog's paper Blockchain: The India Strategy is a good starting point for this exercise.