aapti institute   OMIDYAR NETWORK INDIA

The Governance of Digital Public Infrastructure

India Paper

This is a work of independent research, commissioned by **Omidyar Network India** in 2023-2024.

It was produced by **Aapti Institute**, a public research institute that works on the intersection of technology and society. Aapti examines the ways in which people interact and negotiate with technology both offline and online.

ACKNOWLEDGEMENTS

In addition to contributions from the wider Aapti team, this report also draws from the expertise of numerous academic and industry experts and practitioners. We are grateful for their input during interviews and rigorous feedback sessions.

Editor: Barnali Ghosh | **Report design:** Meher Rajpal | **Cover illustration:** Shaunauk Sokey

The Governance of Digital Public Infrastructure

India Paper

AVANI AIRAN, SURABHI HODIGERE,
SOUJANYA SRIDHARAN AND SARAYU NATARAJAN

aapti institute

OMIDYAR NETWORK INDIA

Table of Contents

Abbreviations

ABDM	Ayushman Bharat Digital Mission
ABHA	Ayushman Bharat Health Application
API	Application Programming Interface
AUA	Aadhaar Authentication System
CEO	Chief Executive Officer
CIDR	Central Identities Data Repository
CPGRAMS	Centralised Public Grievance Redress and Monitoring System
DAAS	Digital Agricultural Advisory Services
DBT	Deputy Directors General
DEPA	Data Empowerment and Protection Architecture
DPG	Digital Public Goods
DPGA	Digital Public Goods Alliance
DPI	Digital Public Infrastructure
DSC	Digital Solution Companies
GRO	Grievance Redressal Officer
HFR	Healthcare Facility Registry
HIP	Health Information Providers
HIU	Health Information Users

HPR	Healthcare Professional Registry
IGM	Issue and Grievance Management
IMPS	Immediate Payment Service
ISN	Inventory Seller Nodes
MEITY	Ministry of Electronics and Information Technology
MoHFW	Ministry of Health & Family Welfare
MSN	Marketplace Seller Nodes
NDEAR	National Digital Education Architecture
NDHE	National Digital Health Ecosystem
NDHM	National Digital Health Mission
NHA	National Health Authority
NPA	Network Participant Agreement
NPCI	National Payments Corporation of India
ODR	Online Dispute Resolution
ONDC	Open Network for Digital Commerce
OTP	One-Time Password
PKI	Public Key Infrastructure
PSP	Payment Service Provider
RBI	Reserve Bank of India
RTI	Right to Information

SHA	State Health Agencies
SME	Small and Medium Enterprises
TPAP	Third-Party Application Provider
UID	Unique Identification Numbers
UIDAI	Unique Identification Authority of India
UPI	Unified Payments Interface
VPA	Virtual Payment Address

Executive Summary

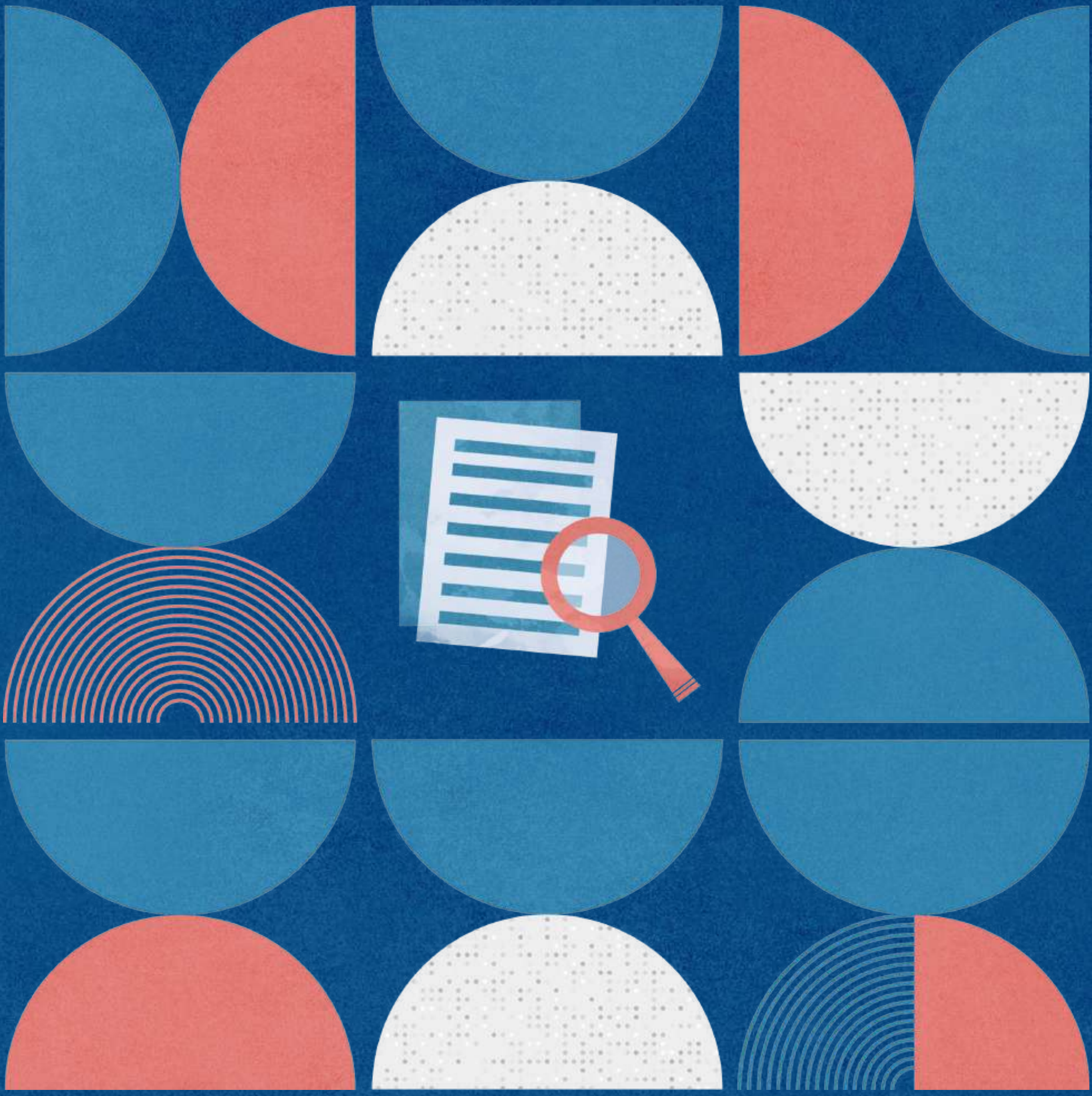


TABLE OF CONTENTS ABBREVIATIONS

Executive Summary

This consultation paper examines the governance of Digital Public Infrastructure (DPI), focusing on initiatives across the globe. While DPI plays a crucial role in the digital era of Government and public service delivery, there is a lack of comprehensive assessment and documentation of its governance best practice. The paper fills this gap by documenting the evolution of India's DPIs initiatives including Aadhaar, Unified Payments Interface (UPI), Open Network for Digital Commerce (ONDC), Account Aggregator (AA), ABDM (Ayushman Bharat Digital Mission), and National Digital Education Architecture (NDEAR), drawing insights from their evolution to form a DPI governance framework.

This paper comes immediately after a renewed approach to public service delivery that is underpinned by innovative DPI powering large-scale digitisation. Scholars offer that the 'DPI approach' is characterised by **common design, robust governance, and private sector participation.** This approach underscores the need for common principles and prioritises frameworks for collaboration, capacity building, and the development of common standards.

In the context of India's G20 leadership, where digital transformation is a prominent lever, the importance of effective governance for inclusive, secure, and sustainable digital infrastructure becomes imperative. Governance plays a crucial role in addressing digital challenges and unlocking the potential of digital technologies to deliver public and private services at scale. This consultation paper explores innovative forms of DPI governance, such as protocols and network-based models.

Building the methodology for the governance framework comprises four stages:

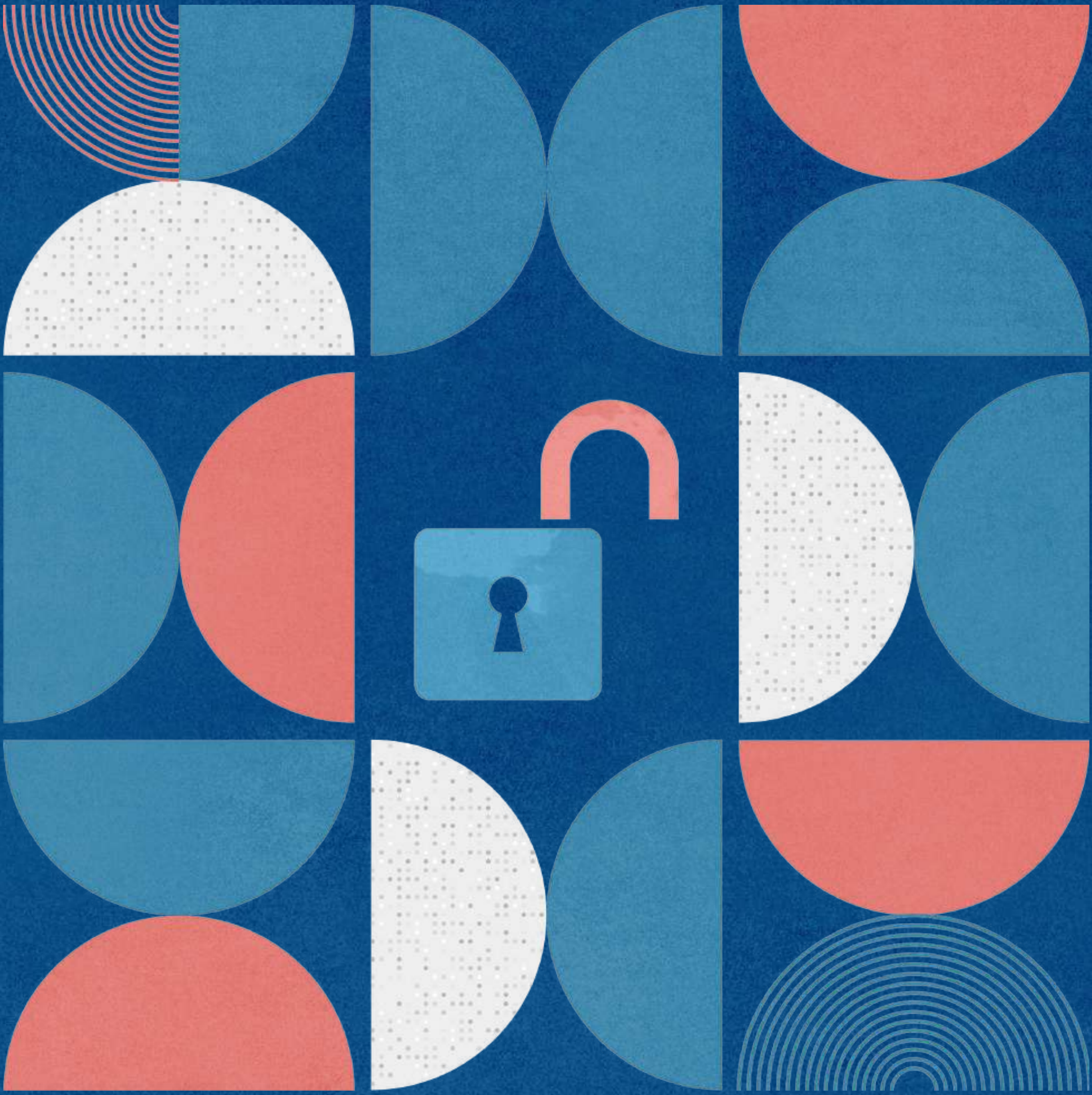
- Desk research on guiding definitions and goals for DPI governance
- Interviews with leading experts in the DPI ecosystem
- Case studies on the governance journeys of Aadhar, ABDM, ONDC, and UPI
- Consultations with key stakeholders

By providing insights and recommendations, the establishes an effective DPI governance framework, encompassing principles such as accountability, privacy, security, and inclusiveness. This paper's findings will contribute to wider discussions on the governance of DPI, both within the G20 and globally. This will foster collaborative efforts and knowledge sharing to encourage the widespread adoption of best practices.

At the core of our governance framework are the guiding principles specifically identified for DPI. They serve as the foundation for the governance systems. In turn, the principles are operationalised via the use of tools that either exist or are embedded in laws, policies, regulations, and technical architecture. These tools constitute the paper's recommendations to operationalise DPI principles across its lifecycle – from conception to development, deployment, and beyond. As DPI governance involves a multi-stakeholder landscape, the responsibility for the governance is distributed among Government entities, regulatory bodies, industry organisations, civil society groups, and technology experts.

SECTION 1

Introduction



SECTION 1

Introduction

1.1. Framing the Issue

Across the world, DPI continues to grow in scale, scope, and significance. In India, DPI is an integral component of everyday public service delivery and administration. The DPI journey began with the roll out of Aadhaar as a medium for public service delivery. It, in turn, served as a stepping stone for the phenomenal success of the digital payment infrastructure, the UPI. Other noteworthy initiatives include the ABDM, Data Empowerment and Protection Architecture (DEPA), and ONDC – DPI that operate across sectors such as health, education, finance, and commerce – at varying stages of maturity and implementation.

Over the past decade, multiple reports have documented the population-scale implementation and impact of DPI in India. However, a comparable, dedicated effort to assess the evolution of DPI and codify the best practices for their governance is still to be undertaken. This whitepaper is an attempt to document and delineate the evolution of extant DPI, specifically Aadhar, ABDM, UPI, and ONDC, to draw insights that inform the framework for the governance of DPI in India.

Why we need a Framework for the Governance of DPI

DPI has evolved into a distinct approach, revolutionising the digitisation of large-scale systems for public service delivery. Recent research argues that DPI is an approach to delivering public services through digitisation. It emphasises three key concepts: common design, robust governance, and private sector participation. DPI's common design principles prioritise openness, scalability, and interoperability. Its modular architecture allows independent development and seamless integration of components, enabling quick adaptation to evolving market needs.

Robust governance is integral to DPI, embedding legal obligations and privacy features into the infrastructure. Adherence to common standards ensures trust, transparency, and accountability. DPI promotes inclusion by connecting low-literacy and low-connectivity areas while fostering trust and accountability. Private sector participation is critical for the success of DPI, driving market innovation, competition, and sustainability. It creates fair competition, generates job opportunities, and enhances user experience.

This research underscores the need for a governance framework to implement the DPI approach successfully. DPI has the potential to either promote inclusion and safeguard rights or exclude and monitor individuals. Therefore, a robust governance framework is essential to ensure fair competition, protect privacy, and empower users while fostering market innovation and consumer protection. Privacy by design, a key component of DPI governance, ensures the implementation of privacy-enhancing technologies and secure data practices, instilling trust in the digital ecosystem. Empowering users with autonomy over their data allows for transparency, accountability, and informed decision-making, addressing concerns surrounding data protection and consumer rights. Protocol-based supervision offers regulators direct control over the underlying protocols, enabling effective policy influence and regulatory oversight. Moreover, obligations established through code reduce compliance burdens on market participants, streamlining governance frameworks. A governance framework for DPI is essential to ensure its responsible and beneficial deployment at scale.

In India, the 2023-2024 Economic Survey highlights the importance of creating strong safeguards through appropriate governance and policy to bolster the potential of DPI. The survey notes that “[...] as digital spaces widen to bring in newer services, the need for appropriate regulations also becomes paramount. Therefore, techno-smart regulations are the future of digital societies. In this regard, Governments worldwide have adopted or are introducing legislation to provide a foundation for robust data governance. Their policy goals can be complemented and advanced with the help of standard, open, and interoperable protocols that increase the choice of digital services available to a user and enhance user privacy, such as the proposed Data Empowerment & Protection Architecture [...].”

With this in mind, a robust governance framework is essential for the successful implementation and sustainable operation of DPI. This paper focuses on building a set of guiding principles underpinning DPI to serve as the foundation for this framework. However, principles alone are not enough; they must be translated into actionable norms through a range of tools and mechanisms. These tools encompass institutional guidelines, policies, legislative measures, regulations, and technical specifications that govern the behaviour and actions of stakeholders involved in the DPI ecosystem. Therefore, this governance framework aims to bridge the gap between principles and actionable norms, promoting responsible innovation and safeguarding the rights and interests of individuals and society at large.

1.2. Document Objectives

The primary objective of this paper is to establish a comprehensive governance framework for DPI in India, while also considering its relevance on a global scale. This framework is designed to align with the Constitutional rights and values of the country, ensuring the responsible and effective implementation of DPI initiatives. By drawing insights from successful DPI projects in India, such as Aadhaar, UPI, ABDM, and ONDC, the paper identifies key governance practices and lessons learned. These insights are then synthesised and presented as a set of principles and tools in the governance framework.

To gather diverse perspectives and foster collaboration, the whitepaper seeks public consultation, inviting stakeholders to provide input and contribute to the ongoing development of DPI governance. By addressing the specific needs and priorities of India, while considering global implications, this whitepaper aims to establish a robust and inclusive governance framework that serves as a model for DPI initiatives both within India and worldwide.

1.3. Methodology

The methodology employed for this paper encompasses four distinct stages to ensure a comprehensive and informed approach.

- **The First Stage**
  Involves conducting desk research to gather guiding definitions and goals around the governance of DPI. This step aims to establish a solid foundation of knowledge and understanding of the subject matter.
- **The Second Stage**
  Includes interviews with experts within the DPI ecosystem. These bring valuable insights and perspectives from individuals with deep expertise and practical experience in the field.
- **The Third Stage**
  Focuses on conducting case studies on specific DPI initiatives, such as Aadhaar, UPI, ABDM, and ONDC. The selection criterion ensures a comprehensive examination of DPI projects that considers factors such as the age of the initiative, institutional structure, maturity level, and the key individuals involved in their development and implementation. This criterion facilitates a comprehensive and representative analysis of DPI initiatives across different dimensions.
- **The Fourth Stage**
  Centers around consultations with key stakeholders to collaboratively build the governance framework. This stage engages with various stakeholders, including Government entities, regulatory bodies, industry organisations, civil society groups, and technology experts. Their input and perspectives validate the proposed governance framework.

Following this approach, the paper benefits from a robust foundation of research, expert insights, in-depth case studies, and extensive stakeholder consultations. This comprehensive methodology enables the development of a governance framework that is informed, inclusive, and aligned with the specific characteristics and requirements of DPI initiatives.

1.4. Guiding Definition

Digital Public Infrastructure

Although existing literature does not arrive at a conclusive definition of DPI, there are common themes that stand out among different stakeholders' understanding of the term. Some major themes that emerged throughout our review are as follows:

1. DPI implementation is undertaken at scale, often population-wide in ways that enable the infrastructure to create society-wide connections
2. DPI comprises foundational public administration levers upon which other solutions are built
3. DPI systems and solutions are anchored in the creation of public value

Within India, the commonly used definitions of DPI are consistent with the three themes identified above. One such definition looks at DPI as a "... transparent, citizen-centric, societal platforms that distribute the value created for all stakeholders and are governed by impact goals, rather than the profit motive of a few shareholders."

This paper codifies the DPI governance best practices. We use a simple framework of guiding questions to taxonomise what constitutes a DPI in India. This guiding framework has been derived from the extensive literature review detailed in the subsequent headings under this section. Through each of these questions, we qualify a DPI based on an unbundling of three elements:

1. **Digital:** To test whether a solution uses the features of 'digital technology', we asked: Is this a technology solution that stores and processes data and is evolving at a fast pace?
2. **Public:** To test if the solution is 'public', we asked: Is this an enabler of society-wide impact?
3. **Infrastructure:** To test whether the solution qualifies as an 'infrastructure', we asked: Is this a system or solution a building block to build other solutions on? And does it enable the effective provision of functions and services in the public and private segments?

The gating criteria form our working definition of DPI. This guides the analysis and recommendations presented.

"Digital public infrastructure refers to digital technologies that enable society-wide impact, act as a building block for other technological solutions, and enable the effective provision of services in the private and public sectors."

Evolving Definition of DPI

Over the years, deliberations led by multilaterals with Government bodies industry practitioners, and academics have arrived at a reasonable consensus on the definition of DPI. Today, the most widely used definition is one that is codified by the Digital Public Goods Alliance (DPGA). The DPGA defines DPI as solutions and systems that enable the effective provision of essential society-wide functions and services in the public and private sectors. Co-develop, which was formed to promote safe, inclusive, and equitable DPI, uses the following similar criteria to distinguish between digital goods and infrastructure. It defines DPI as implemented, operational systems whereas Digital Public Goods (DPGs) could be open software, data, and content that are used to build a system, whether DPI or otherwise. Going further, Co-develop identifies DPI vis-a-via DPG through three characteristics:

1. Enables widespread use across country or sectors, creating a common platform for societal scale connection
2. Possesses basic functionality but is powerful and broadly applicable. It allows for other things to be built on top or be integrated
3. Comprises systems that allow performance of core societal functions and create public value

Like Co-develop, Ethan Zuckerman presents that DPI is distinguished from DPG based on the following characteristics. They:

1. They are necessary for society to function
2. They are built so other things can be built
3. They generate externalities

Physical vs Digital Infrastructure

The above-mentioned characteristics are equally applicable to physical infrastructure, particularly public infrastructure such as roads, highways, and waterways. To distinguish DPI from physical public infrastructure, we refer to a framework provided by Paul Edwards, a scholar of information and history, in <what publication>. Edwards notes that "[...] Infrastructure based on software is fundamentally different from its physical counterpart. Unlike railway construction, which is slow and costly, software can be rapidly written and widely distributed. Speed and flexibility can be advantageous but also affect reliability and durability. Although software infrastructure can be relatively cheap and quick to build, it can be costly and laborious to maintain. Digital infrastructure can have a wildfire-like speed as well as an unpredictability and an ephemerality [...]."

Similarly, Co-develop notes that in the context of DPI, digital technologies allow for a variety of uses, users, and problem statements. This diversity of impact, when intentionally applied to public value creation, creates a DPI capable of both never-before-existent scale and scope. Similarly, digital technologies allow for more value to be created as more people and places are connected. The inherent network-building capacity of digital technology lends itself as a means for DPI to create societal scale impact. The fact that digital technologies are built to allow integration, leads itself to creating more value as new functions are built and the value of DPI is grown. While country-specific and sectoral laws regulate sharing, the function of digital technology does not change across contexts and borders. This ensures that DPI built anywhere is utilised to solve public problems everywhere.

As noted in the definition, the evolving nature of digital technologies ensures that the technology is adapted to changing societal requirements and structural advancements. Digital technologies often become foundational aspects of our modern life. Through DPI, this spills over into activities and touchpoints that generate public value. Possibly the most important feature of digital technology is that it generates vast amounts of data with varying uses. In DPI, data generated lends itself to improving the quality of services provided and quantifies impact.

These insights from research demonstrate that digital technologies are ever-evolving and impact an interconnected range of private and public functions. As our world increasingly becomes digitally driven, it is imperative to acknowledge that existing methods of governing physical infrastructure need to differ from the requirements of governing digital infrastructures.

Meaning of 'Public'

The digital technologies that create significant public value in the modern day are those that originated for private gains. How then can we differentiate digital private infrastructure from DPI?

In academia, the word 'public' is defined as the body politic, or the people of a state, nation, or municipality. The word derives from the Latin 'publicus' meaning "pertaining to the people, state, or community." While there have been a lot of references to the economic concept of public goods (non-rivalrous, non-excludable), DPGA clarifies the dual meaning of public about DPG and DPI. For DPG, which needs to be open-source, the conditions of pure 'public goods' apply better than for a DPI; which is built on proprietary or open-source technologies. Instead of DPI, DPGA observes that 'public' implies that the technologies in question are implemented as backbones/enablers of public service delivery and/or provide public services. This definition of the word evokes pertinent questions on the role of the state in designing and implementing DPI.

The World Bank argues that 'public' refers to Governments having a primary role and responsibility in deciding whether and how DPI is provided in the interests of the broader society and economy, such as through regulating, operating, and/or partnering with the private sector.

Stakeholders Involved in Governance

Governance of DPI involves the active engagement of diverse stakeholders, each playing a critical role in shaping and driving its adoption. These stakeholders offer their expertise and resources to ensure effective governance and the successful implementation of DPI initiatives.

The most important of these stakeholders is the public sector which holds a significant responsibility in governing DPI. Government entities regulate the ecosystem, provide funding support, and actively participate in the co-design of DPI solutions. Their involvement is vital for establishing regulatory frameworks, ensuring compliance, and overseeing the wide-scale implementation of DPI. However, the private sector also plays a crucial role in governance by driving software innovation and setting technology standards for DPI usage.

Similarly, open-source communities and organisations also contribute to DPI governance by supporting the development of standards, protocols, and community-driven open-source technologies. They provide intellectual resources, such as volunteering efforts and advocacy for open-source adoption, which promotes collaboration, transparency, and innovation within the DPI ecosystem. Development actors, including non-profit organisations and philanthropic foundations, actively promote best practices for DPI governance. They facilitate collaboration among stakeholders, bring in funding support, and provide offline intermediation to ensure the effective adoption of DPI, particularly in underprivileged and marginalised communities.

End-users are important stakeholders in governing DPI as they actively participate in the co-design process and innovation built on top of DPI. Their engagement helps ensure that DPI solutions are user-centric, inclusive, and meet the needs of the people. Additionally, end-users play a vital role in raising awareness about the benefits and potential of DPI, fostering public understanding and support.

By involving these diverse stakeholders in the governance of DPI, it becomes a collaborative effort that combines regulatory oversight, private sector innovation, open-source contributions, development actor support, and end-user participation.

The Role of Public Institutions in DPI

In this section, we delve into the significance of governance innovation in creating sustainable DPI, emphasising the pivotal role of public institutions while exploring emerging trends in institution building across the globe.

Governance innovation is pivotal in ensuring the seamless operation and evolution of DPI. It entails the design and implementation of novel institutional frameworks that can adapt to the dynamic digital environment, harnessing the potential of technology while working to mitigate its risks. Public institutions play a central role in shaping and safeguarding DPI. Such institutions act as custodians, setting standards, regulations, and policies that guide the development, deployment, and usage of digital tools. They ensure data security, privacy protection, and equitable access, fostering public trust and confidence.

Within the DPI journey of a country, public institutions take on multifaceted roles. They formulate regulations that govern the collection, storage, and use of data. This safeguards the privacy of citizens and ensures that the benefits of DPI are not at the expense of personal freedoms. These institutions also establish guardrails for DPI access, promoting transparency and accountability in Government operations. By fostering interoperability standards, they enable the integration of various digital platforms and services, creating a cohesive digital ecosystem that enhances service delivery.

The intricacies of India's context necessitate an approach that resonates with its multifaceted challenges, opportunities, and aspirations. The Indian DPI governance model not only illustrates these trends but also underscores the significance of tailoring governance strategies to align with the nation's specific requirements and objectives. The Indian examples elucidate how the nation's distinct backdrop has facilitated the development of diverse governance models, each tuned to address particular needs and priorities.

Public Sector-led Governance: Aadhaar

A standout illustration of public sector-led governance innovation is Aadhaar, overseen by the Unique Identification Authority of India (UIDAI). The UIDAI, a statutory entity, plays a central role in governing Aadhaar, India's biometric identification system. The UIDAI governance framework vests the responsibility of oversight and accountability in a dedicated public body, ensuring a robust and controlled governance structure.

Private Sector-led Governance: ONDC

Contrasting the public sector-led approach is the case of ONDC. Governed as a Section 8 company under the Companies Act, 2013, it includes public sector banks among its shareholders. ONDC represents a distinctive amalgamation of private-sector ingenuity and public-sector investments. This model empowers private entities to spearhead rule-setting, foster innovation, and safeguard public interest.

Community-centric Approach: Sahamati

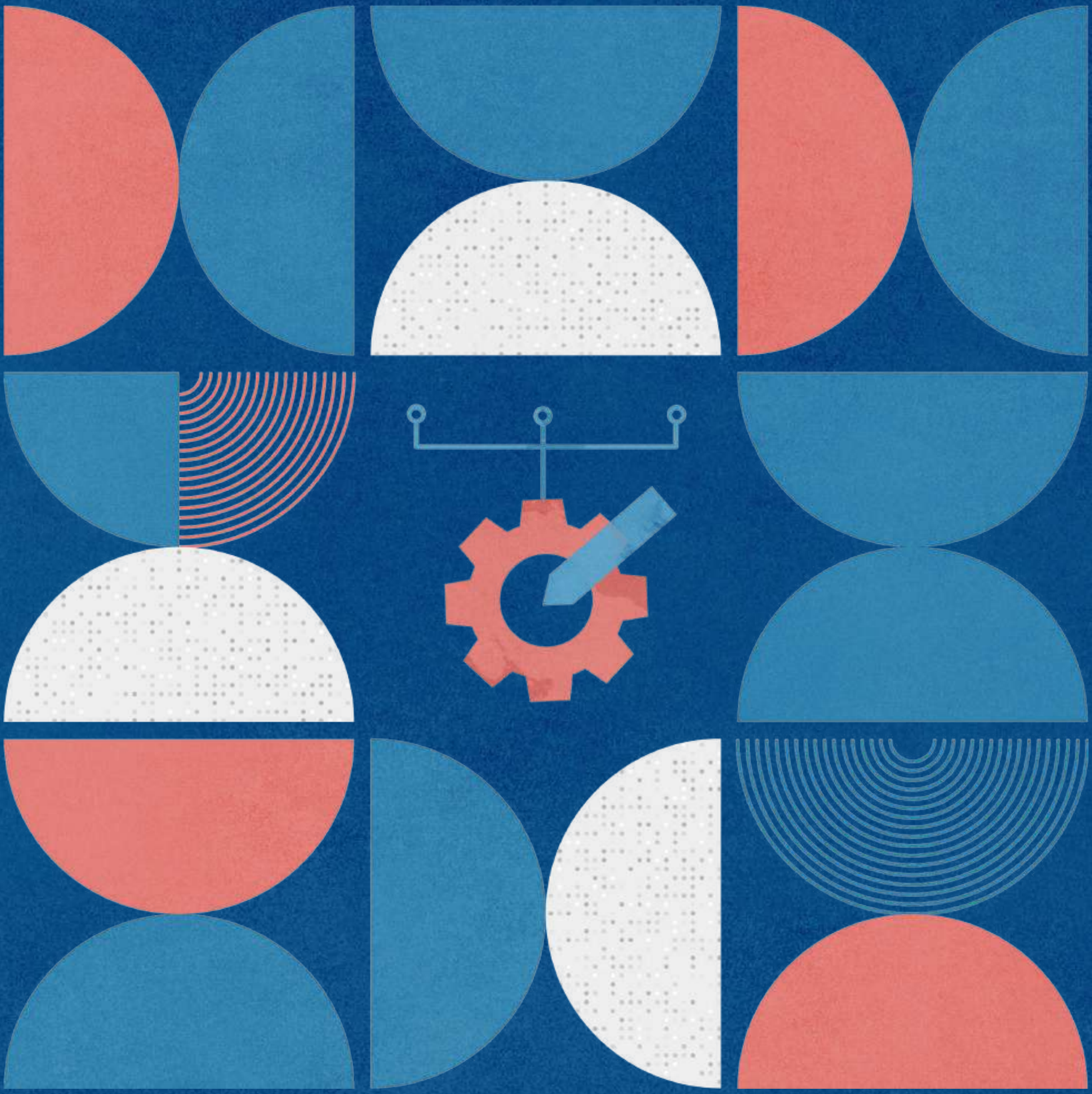
While the Reserve Bank of India (RBI) holds primary regulatory authority, Sahamati, a consortium of account aggregators, significantly contributes to community-driven governance within the Aadhaar ecosystem. This collaborative model exemplifies the potential of participatory endeavours between regulatory bodies and community-based entities, effectively managing governance dynamics in an evolving digital landscape.

The diversity of levers to enable governance innovation around DPI has yielded interesting insights for regulatory design. From a public policy standpoint, it entails formulating standards for data security, personal data protection, and ethical considerations, balancing technological innovation with societal well-being. From a public administration perspective, it emphasises the seamless integration of digital platforms into existing governance structures, ensuring that the benefits of DPI are accessible to all citizens, regardless of their technological literacy or socio-economic status. This emerging paradigm for governance innovation, one that is firmly anchored in advancing DPI while upholding necessary regulatory safeguards for privacy, is poised as India's unique ‘techno-legal’ approach to digitisation.

The importance of governance innovation in building sustainable DPI cannot be overstated. The trajectory of DPI development rests on the shoulders of public institutions that navigate the complex interplay between technology, policy, and societal needs. As countries endeavour to establish and nurture their DPI, they must carefully consider the roles that these institutions play. The emerging trends of public sector-led, private sector-led, and combined approaches underscore the diversity of strategies available, each with its own set of benefits and challenges. By embracing governance innovation, nations can unlock the true potential of DPI, shaping a future where technology empowers societies while preserving fundamental values.

SECTION 2

Creating a Framework for DPI Governance



SECTION 2

Creating a Framework for DPI Governance

The DPI landscape is a dynamic space with a multitude of factors affecting their adoption and meaningful operation. Effective governance is essential to ensure its success and seamless integration into public service delivery. To achieve the same, we draw a principle-led approach to DPI governance – one that is grounded in a comprehensive set of guiding principles that are rooted in the larger national and international legal frameworks and relevance to diverse DPI systems. These guiding principles are the bedrock of a common and robust governance framework that applies across the stages of the DPI lifecycle.

By unifying the governance under a common framework, we aim to promote consistency, interoperability, and synergies across DPI initiatives. This enables DPI from diverse sectors and contexts to complement and build upon each other and adhere to fundamental values across the digital infrastructure landscape. The clarity and predictability resulting from this governance framework also provides stakeholders involved in the development and operation of DPI with a reliable roadmap to secure an effective, safe, and responsible framework for its implementation.

2.1. Identifying the Principles of Governance

The creation, adoption, and operation of DPI systems should adhere to a set of identifiable principles that are upheld by all processes, institutions, and actors. Taking a functional approach to a comprehensive set of guiding principles that are operationalised through instruments of governance allows the ecosystem to meet the baseline obligations of arriving at a ‘good’ DPI, which is:

1. Inclusive, accessible, and equitable
2. Private and secure
3. Co-created for public benefit
4. Within the framework of transparency, accountability, and appropriate grievance redressal

These principles are informed by an identification of the guiding values within the governance systems for extant DPI . Additionally, they are traced as an extension of the system of rights and obligations entitled to all individuals and actors within the domestic constitutions and common international covenants. A system that abides by these principles, can achieve the identified goals of governance for the DPI ecosystem that is based on trust, access, and collaboration.

2.2. Pathways and Tools

The guiding principles identified for DPIs are incorporated into the ecosystem through policy-level pathways and are operationalised with the codification of specific governance tools. The Organisation for Economic Co-operation and Development framework presents a combination of these values, enablers, and tools to realise successful reforms enabled by systems of governance. Built on similar lines, we arrive at the enablers or pathways as institutional arrangements and policies that are operationalised via governance tools. These tools represent the specific techniques and mechanisms which help translate the principles in the ecosystem from vague indicators to actionable processes.

The final list of tools in this paper has implications across laws, policies, standards, and rules. They may be embedded within different levels of the Government framework – from legislative acts to specific rules of engagement for individual DPI projects. For example, while notice and consent mechanisms are integrated into data protection laws and policies, encryption and security safeguards are embedded in technological standards or cybersecurity protocols. The cross-sectional approach of implementing the right tool creates an effective governance structure that operates at multiple levels within the Government.

The flexibility of these tools allows them to be tailored to the unique context and requirement of each DPI initiative while aligning with the overarching governance framework. This adaptability ensures that the principles remain robust and relevant, regardless of the DPI's sector, scope, or scale.

The table below indicates how the materialisation of core principles in the DPI ecosystem is imagined through identifiable pathways and tools of governance.

CORE PRINCIPLES	PATHWAYS/ ENABLERS	TOOLS/INSTRUMENTS
Inclusivity, accessibility, and equity	• Offline access • State budgeting and investments • Participatory mechanisms for consultation and feedback	• Active internal feedback portals • Government subsidies and exemptions for expansion • Investment in capacity building • Codifying for welfare and access • Codifying integration with analogue and offline architecture
Privacy and security	• Strong consent framework • Privacy-by-design • Data protection • Cybersecurity responsibilities	• Notice and consent mechanisms • Data disclosure obligations, • Access controls and authentication mechanisms • Encryption, regular security audits and risk assessments • Independent oversight bodies, decentralised data storage
Collaborative and co-created for public benefit	• Open innovation, codified and tangible public benefit • Ensures equity, affordability, and accessibility • Community participation.	• Codified consultation processes for new developments, portals for feedback • External regulatory oversight to ensure compliance • Interoperability and modularity • Technical advisory boards with a diverse representation of interests • Institutionalised framing of welfare for the marginalised
Transparency, accountability, and redress	• Transparency and disclosure obligations • Dedicated oversight bodies • Accessible grievance portals with clear sources of authority	• Access to data • Clear procurement and success metrics • Impact assessments • Layered grievance redressal mechanisms from internal to independent/external

2.3. Lifecycle of a DPI

The guiding principles identified for DPIs are enshrined in the ecosystem through policy-level pathways and are operationalised with the codification of specific governance tools. These tools apply to the processes, institutions, and actors involved in DPI systems and find resonance during all stages in the lifecycle of a DPI including:

1. **Conception**
   This is the first step in ideating on the need for and structure of DPI. The purpose is to deliberate on setting up institutional designs and designating the roles and responsibilities of the actors within the framework. This involves expert deliberation and public consultation to ensure transparency, co-creation, and inclusion. These processes encourage diverse perspectives that shape the initial ideation and conceptualisation, aligning them with the principles of openness, collaboration, and equal participation.

2. **Development**
   This stage sets up appropriate structures for the technological, institutional, and governance functions. For governance, this involves identifying a governing institution and financing models, as well as codifying the rules of engagement based on collaboration. For key technology processes, procurement is based on transparency and equity, as well as the development of platforms, protocols, and processes that adhere to identified standards. Principles such as system security, transparency, accountability, co-creation, inclusion, and equity guide the establishment and enhance the DPI, ensuring its effectiveness and responsiveness to evolving needs.

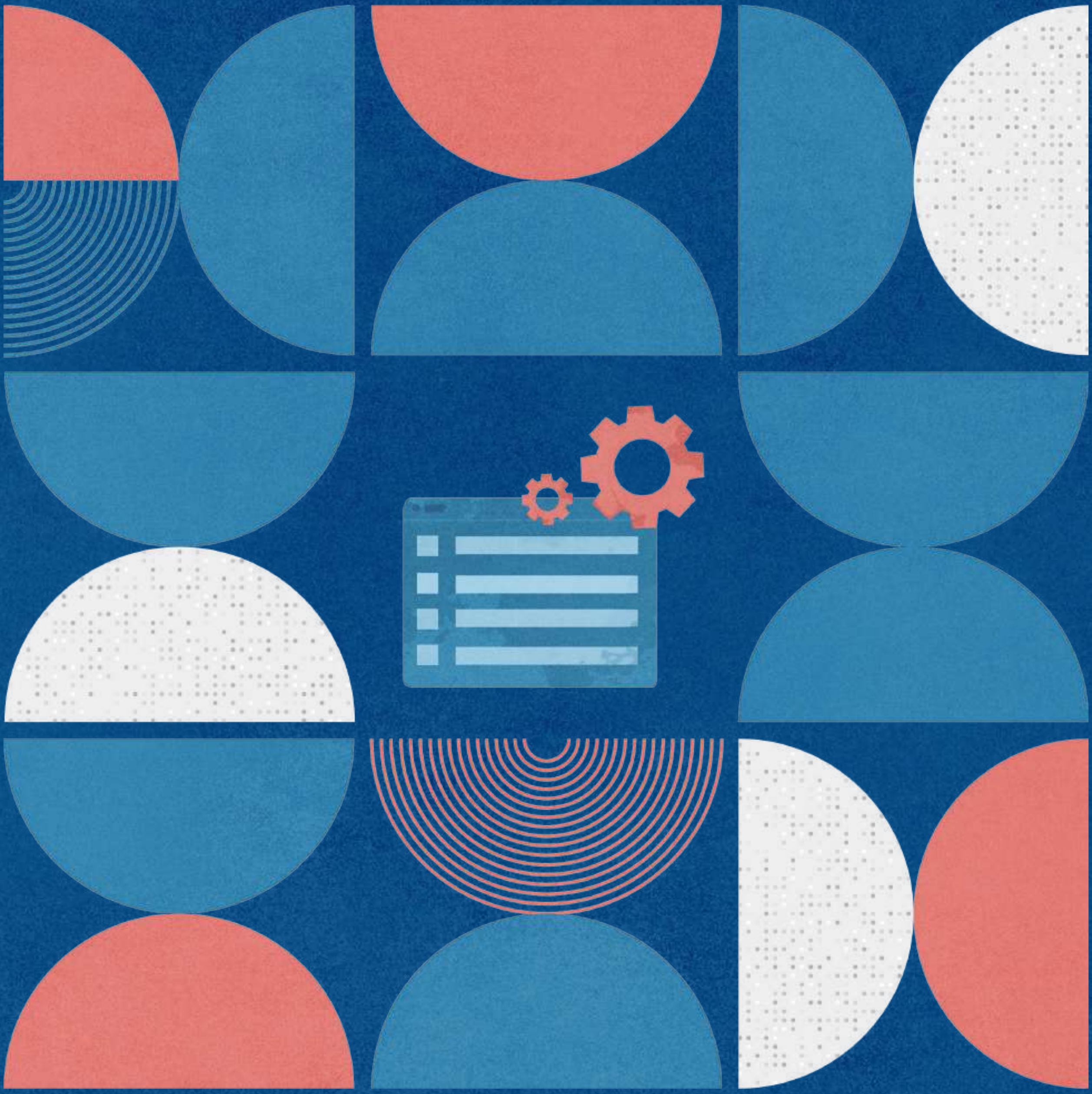
3. **Operation**
   This involves processes such as onboarding participants, implementing feedback and grievance redressal mechanisms, and conducting regular audits. These processes align with the need for inclusion, collaboration, public benefit, transparency, and accountability. By actively engaging with users and stakeholders, addressing their concerns, and ensuring transparency in operations, the DPI fosters trust, equal access, and responsive service delivery.

4. **Feedback and Revision**
   This stage actively focuses on seeking inputs, conducting monitoring and evaluation, assessing impact, and implementing necessary amendments. Inclusion, collaboration, public benefit, transparency, and accountability guide this stage. By evaluating the DPI's effectiveness and incorporating feedback from users and stakeholders, the infrastructure is continuously improved and refined to better serve the public.

To build an understanding of how principles are relevant to each stage of a DPI’s lifecycle, this document provides examples of how different tools are adopted to operationalise each principle. Thus, regulators can visualise actionable steps to enshrine the right principles for a stage that is most relevant to their position in the lifecycle.

SECTION 3

Framework for DPI Governance



Framework for DPI Governance

Our Framework for governance of DPI follows a cross-sectional approach in identification of a diverse set of tools that can be contextualised for the relevant DPI ecosystem, to instil a common set of principles at an appropriately comprehensive level. To that end, our tools range from instruments of governance that operate at the broad scale of law and policy or at the more specific instantiation of technical standards or operational rules and guidelines. The following key provides a clear classification of the tool sets -

LAWS, IN GREEN

Laws are broad and overarching in nature, and they establish the fundamental principles, rights, and obligations that govern a system. These are formal rules that are enacted by a legislative body (such as a parliament or congress), and are at the highest level in terms of legal authority. They provide a legal framework on the foundations for data protection, grievance redressal, and other regulatory aspects of a DPI. For instance, data protection laws establish the fundamental rights and responsibilities related to individuals' personal data.

POLICIES, IN BLUE

Policies are the high-level statements or guidelines that guide decision-making and actions within a DPI. These policies set out the overall objectives, principles, and directions that need to be followed. They provide a strategic framework for various activities and help in aligning actions with organisational goals. Accordingly, general policies could pertain to the overarching approaches for managing DPI, and outline the broad intentions and strategies for imbibing the right principles within the DPI ecosystem.

TECHNICAL STANDARDS, IN PURPLE

Technical standards refer to established specifications and guidelines for products, processes, or services to ensure consistency, interoperability, and quality. These standards are often developed by industry organisations, international bodies, or regulatory agencies. Technical standards provide specific requirements that products or systems must meet to ensure compatibility, safety, and reliability. These could be in the form of the stipulated data sharing protocols and cyber-security standards that must be implemented in DPI projects.

OPERATIONAL RULES AND GUIDANCE, IN PINK

Operational rules or guidelines provide detailed instructions and procedures for carrying out specific tasks or activities. These rules offer actionable information on how to implement policies, standards, or laws in day-to-day operations. Operational rules are more specific than policies and standards, and could give specific instructions on how to implement principle based measures, such as interoperability or offline integration, within individual DPI projects through practical guidance.

4.1. Build for Inclusion, Accessibility, and Equity (What)

Commitment to inclusivity – to promote access and equity in essential public infrastructure – has been a longstanding priority in the Indian Constitution. Prioritising it alongside meaningful access mitigates the risk of excluding marginalised communities and those on the other side of the digital divide. It also maintains appropriate channels to engage with the DPI to promote welfare delivery, public administration, or critical services offered to citizens. These values originate in articles 14 to 19 of the Constitution regarding an individual's fundamental rights – through the right to occupation, expression, and equality. The Directive Principles of State Policy also outline the state's duty of protecting access to infrastructures associated with health, education, and livelihood.

Successful operation of these DPIs relies on an enabling ecosystem of high digital connectivity, technical literacy, and public trust. When considering a healthy DPI system, it is important to focus on accessibility and meaningful participation. This requires addressing the accessibility of the infrastructure, as well as the ability of users and developers to engage with To enable this, the ecosystem strives to leverage governance tools and policy instruments that promote offline access, employ participatory mechanisms for consultation and feedback, and actualise state budgeting and investments for scale and capacity.

Tools (How)

1. **Codify integration of technology with offline architectures and processes to bridge the digital divide. This ensures inclusive and equitable access to DPI.**

   > ***Practice:*** UPI 123 for internet-free transactions, off-line eKYC for Aadhar registries, and assisted mode and offline mode for the creation of Health ID and Digital Personal Health Records

2. **Invest in capacity-building and awareness initiatives that promote welfare. This enables individuals and organisations to acquire the necessary skills and knowledge to effectively engage with and benefit from the DPI.**

   > ***Practice:*** National Payments Corporation of India (NPCI) Circular with recommendations on simplification of user-side flows in apps for easy onboarding; and publication of simple, verified information collaterals to build literacy and awareness. Similarly, the Aadhar charter mandates registrars to take special measures to enrol marginalised residents, such as senior citizens, people with disabilities, women, children, unskilled and unorganised workers, and nomadic tribes.

3. **Allocate budgets for early stages to support the expansion of DPI, particularly targeting underserved communities and marginalised groups. This enhances accessibility and ensures that cost does not act as a barrier to access.**

> ***Practice:*** Periodic union budget for UPI and National Health Authority's (NHA's) Digital Health Incentive Scheme (DHIS) with an estimated initial financial outlay of Rs. 50 Crore.

4. **Establish active feedback portals to facilitate open communication and engagement between users, stakeholders, and the DPI system. This enables continuous improvement, addresses concerns, and promotes inclusivity in decision-making.**

> ***Practice:*** The three-layered grievance redressal mechanism in UPI, allows users and other stakeholders to raise complaints via dedicated portals instituted by third-party platforms, banks, as well as the NPCI website. Aadhaar incorporates feedback and communication with an administrative focus, where the Aadhar Knowledge Management Portal (as a central repository) is aimed to enhance internal communication, facilitate information exchange, and encourage collaboration among UIDAI staff.

EXAMPLE 1:
Bridging the Digital Divide with Aadhaar Offline e-KYC and UPI Lite

In the pursuit of inclusive and equitable access within India's Digital Public Infrastructure (DPI), exemplars like Aadhaar Offline e-KYC and UPI Lite stand as beacons of innovative practices that resonate with the principle of inclusion and the tool of codifying integration with offline architectures.

Aadhaar Offline e-KYC, introduced by UIDAI, empowers individuals to establish their identity without relying on consistent connectivity or revealing sensitive Aadhaar numbers. By offering digitally signed KYC data, including only necessary demographic information and a reference ID, this mechanism addresses privacy concerns while enhancing accessibility. The integration of offline systems enables wider usage, ensuring that individuals with limited connectivity or technical resources can access essential public services securely. This practice embodies the commitment to inclusivity, safeguarding privacy, and fostering equitable access.

In a similar stride, UPI Lite, launched by NPCI, caters to low-denomination transactions, primarily targeting feature phone users. By enabling real-time transactions without a UPI PIN for amounts up to ₹200, UPI Lite acknowledges that a significant portion of transactions fall within this range. This innovative feature bridges the digital divide by making digital financial services accessible to users with basic phones. With a focus on convenience and reduced clutter in bank statements, UPI Lite ensures that small-value transactions are as seamless and secure as larger ones. This showcases a commitment to inclusive access and simplified transactions for all, affirming the core values of DPI governance.

EXAMPLE 2:
Promoting Inclusive Access through ABDM's Digital Health Incentive Scheme

Addressing the core principle of inclusion within India's Digital Public Infrastructure (DPI), the establishment of proactive measures such as the National Health Authority's (NHA) Digital Health Incentive Scheme resonates with the tool of allocating budgets for early stages to support the expansion of DPI.

The Digital Health Incentive Scheme, a part of the Ayushman Bharat Digital Mission (ABDM), endeavours to create a robust digital health ecosystem accessible to all segments of society. By allocating an estimated initial financial outlay of Rs. 50 Crore, the scheme incentivizes various stakeholders to adopt and embrace digital health transactions. This progressive initiative aims to minimise the existing digital divide by targeting untapped segments, particularly underserved communities and marginalised groups.

The scheme extends its benefits to diverse players, including healthcare facilities with 10 or more beds, laboratory/radiology diagnostics centres, and entities providing ABDM-enabled digital solutions. For instance, hospitals and labs exceeding base-level transactions receive monetary incentives per additional transaction, promoting the usage of digital health records. Digital Solution Companies (DSCs) are encouraged to support smaller healthcare setups, contributing to their digitization process while bridging cost barriers.

4.2. Adhere to Privacy and Security Standards (What)

DPI collects large amounts of personal and sensitive information related to finance, health, and location. Robust privacy and security measures safeguard individual's personal data and build trust in the digital infrastructure, which is vital for its widespread adoption and use. The collected data becomes an important asset to improve service delivery and innovation. With the reading of the Right to Privacy as a Fundamental Right within the Right to Life (Article 21) and its recognition in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, privacy, security, and protection of personal data are essential principles that protect against risks that DPIs could otherwise present.

In the absence of dedicated regulation and safeguards, identity systems linked to welfare delivery risk the breach of sensitive personal and financial information. This results in financial losses, profiling, identity theft, and denial of services to vulnerable individuals who depend on welfare programs. Similar consequences arise from the lack of technical skill and awareness of the importance of privacy. Thus, beyond appropriate regulatory mechanisms and to ensure user privacy and system security, DPI must incorporate additional safeguards such as privacy by design. This ensures that data protection and cybersecurity are built into the infrastructure from the outset, alongside initiatives fostering user education and awareness. Complementing this system design with a strong data protection and cybersecurity framework provides appropriate rights and mandates that apply to all stakeholders in the ecosystem.

Tools (How)

1. **Implement notice and consent mechanisms when collecting, using, and sharing personal data. This allows individuals to provide informed consent for the purpose and recipients of their data.**

   > ***Practice:*** NPCI circulars on mandatory consent for location data with an option to opt-out and subsequently revoke.

> Clause 11.1 of ABDM's Health Data Management Policy emphasises a consent-based approach that aligns with existing legal requirements.

2. **Adhere to purpose specification and limitation principles of collected and stored personal data. This ensures that data is collected and retained only for specific, lawful purposes and restricts the amount of data collected to necessary information.**

> ***Practice:*** Section 3.4 of ONDC's strategy document on ONDC's data policy, aligns with the Information Technology Act, 2000 to maintain very limited visibility and storage of transaction data. Similarly, clause 26.6 of AMDB's Health Data Management Policy restricts data collection to identified information pointers and explicitly prohibits the storage of sensitive financial or health data.

3. **Enforce disclosure obligations when data is compromised, requiring organisations to promptly inform individuals affected by the breach and take appropriate measures to mitigate harm.**

> ***Practice:*** Section 8.2 of ONDC's Network Policy, mandates network participants to provide ONDC with all relevant information necessary to fully comprehend the nature and extent of the data breach, which is then reported through a circular published on the ONDC website.

4. **Adopt decentralised data storage approaches that distribute data across multiple nodes or systems. This improves privacy and security while simultaneously reducing the risks associated with breach, loss, or concentration of control.**

> ***Practice:*** NPCI procedural guidelines on customer data storage mandate specific categories of information need to be stored with specific actors only (like banks, TPAPs, PSPs, etc.). Section 26.6 of the Health Data Management Policy states that all digital health data and applications be held in a decentralised manner, following the principle of minimality.

5. **Empower individuals with the right to control and participate in decisions about their personal data. This enables them to access, rectify, delete, or restrict the processing of their data and make informed decisions regarding its use.**

> ***Practice:*** Clause 27 of AMDB's Health Data Management Policy, provides citizens full control over processing their health data with access through links, subject to the applicable permissions and consent. Additionally, in Section 28 of the Aadhaar (Authentication) Regulation, 2016, Aadhaar number holders have the right to access their authentication records, subject to specified conditions and payment of prescribed fees to the authority.

6. **Implement encryption and security safeguards to process or store personal data. This ensures that appropriate technical measures are in place to protect data from unauthorised access, disclosure, alteration, or destruction.**

> ***Practice:*** NCPI's UPI Procedural guidelines mandate that "all UPI transaction data should be stored with the app providers, in an encrypted format." Additionally, while UIDAI has not specified any encryption algorithm for the Aadhaar data vault, eKYC API specifications state that RSA 2048 for Public key encryption and AES 256 for symmetric encryption will be followed for Aadhar. The ABDM Sandbox also provides specifications on encryption and decryption.

7. **Conduct regular security audits and risk assessments to identify and address vulnerabilities and threats to the privacy and security of personal data. This ensures continuous monitoring and improvement of security measures.**

> ***Practice:*** ONDC has the authority to conduct periodic audits of Information and Communication Technology systems, security practices, and compliance of network participants with the ONDC Network Policy. These audits may be conducted directly by ONDC or by an appointed auditor.

EXAMPLE 1:
ONDC's Data Privacy Measures and Shielding of Transaction Data

Aligned with the principle of purpose specification and limitation, ONDC's strategy prioritises the collection and storage of personal data for specific, lawful purposes, while minimising the volume of data collected. The data policy, as outlined in ONDC's strategy document and website echo the robust data security and credibility at the transaction level, enhancing user confidence in digital trade. Transaction data, pivotal to the interactions between buyers and sellers, remains solely within their applications, rendering it invisible to ONDC. The policy goes a step further, vowing against the storage or viewing of transaction data by ONDC. Moreover, personally identifiable information (PII) and essential seller data, crucial for trade, are shielded from unauthorised access, affirming the organisation's dedication to safeguarding sensitive information.

ONDC's privacy policy, complementing its data practices, reaffirms its commitment to user privacy. The organisation's transparency regarding data collection and usage, in combination with adherence to the emerging Personal Data Protection Bill, echoes its proactive approach to privacy governance. This example underscores the significance of purposeful data collection and the meticulous implementation of privacy measures to reinforce trust and ensure data security within the digital commerce landscape.

4.3. Promote Collaboration and Co-creation for Public Benefit (What)

Collaboration and open innovation are key drivers for the success of DPIs. By engaging various stakeholders, including Government entities, private sector organisations, civil society, and individuals, DPIs gain a range of expertise, perspectives, and resources. This collaboration promotes co-creation, knowledge sharing, and collective problem-solving, ultimately leading to the development of robust and inclusive digital infrastructures. By embracing open innovation, DPIs benefit from the collective intelligence of a wider ecosystem, fostering creativity, and promoting the continuous improvement of services and functionalities.

The collaborative approach and collective action fostered within the ecosystem ensure that the development and operation of DPIs are guided by a shared vision of public welfare and contribute to the overall wellbeing of individuals and communities. These values are deeply rooted in the Indian Constitution and democratic ethos. The Constitution emphasises the principles of democracy, equality, and social justice, and envisions a society that works collectively for the common good. The Directive Principles of State Policy further highlight the state's responsibility to promote citizen welfare, protect their interests, and foster social and economic justice.

To achieve collaborative and public benefit-oriented DPI governance, it is essential to establish public consultative forums to encourage open dialogues that promote the exchange of ideas, feedback, and co-creation of policies and initiatives. Moreover, the governance framework should encourage the use of technology and platforms that enable co-creation and collaboration. These include encouraging open data and Application Programming Interface (APIs) to foster innovation, adopting interoperability and modularity in the system, and facilitating participatory governance based on a common, codified understanding of public benefit.

Tools (How)

1. **Establish codified consultation processes for developments within the DPI. This ensures that stakeholders and the public have opportunities to provide input, feedback, and suggestions on the design and implementation of new initiatives.**

   > ***Practice:*** Authorities for ABDM have established a practice of publishing all consultation papers on the National Health Authority (NHA) website. Similarly, ONDC holds frequent meetings with network participants who are a part of the user council to discuss crucial policy developments and publish a summary of the proceedings for all meetings.

2. **Promote openness in technology architecture to foster innovation within the DPI ecosystem. This enables collaboration and the development of new applications and services for public benefit.**

> ***Practice:*** With an open API structure followed for UPI, NPCI has come out with dedicated circulars with guidance on using the UPI API to ease collaboration and co-creation. Similarly, Aadhaar embraces open APIs that allow authorised agencies and service providers to integrate Aadhaar services into their applications and systems seamlessly. Additionally, AMDB has published such APIs on its website, and NDEAR mandates all services built into the digital infrastructure be built as open source and be based on open standards.

3. **Mandate interoperability and modularity in the design and operation of DPI components. This adopts a building blocks approach where different systems and services can seamlessly work together, enabling integration and scalability.**

> ***Practice:*** NPCI mandates all participants of UPI to adhere to RBI interoperability guidelines. Meanwhile, the ONDC strategy document speaks at length on how interoperability is both a technology feature as well as a principle that ONDC hopes to achieve in the market.

4. **Establish diverse expert committees and advisory boards with stakeholder representation to provide guidance and expertise, and ensure that a broad range of perspectives are considered in the decision-making processes related to the DPI. This promotes transparency, inclusivity, and public trust.**

> ***Practice:*** Within the UPI ecosystem, guidance comes from various NPCI dedicated committees and individual advisors with diverse experience in management, audits, technology, and CSR. Additionally, the ABDM governing board mandates the inclusion of two domain experts from fields such as administration, insurance, public and private healthcare, economics, and management, etc.

5. **Provision for sandboxes – controlled environments where innovators and developers experiment and test new ideas, technologies, and applications within the DPI. This encourages innovation, risk-taking, and learning without disrupting the overall system.**

> ***Practice:*** Within the UPI ecosystem, guidance comes from various NPCI dedicated committees and individual advisors with diverse experience in management, audits, technology, and CSR. Additionally, the ABDM governing board mandates the inclusion of two domain experts from fields such as administration, insurance, public and private healthcare, economics, and management, etc.

EXAMPLE 1:
Fostering Innovation and Security with ABDM Sandbox

The ABDM (Ayushman Bharat Digital Mission) Sandbox stands as a pivotal instrument for licensing partners within the ABDM ecosystem. Its primary role is to facilitate the seamless integration of healthcare providers' information management systems or electronic medical record software with ABDM's digital building blocks. This sandbox serves as a controlled testing environment where developers can experiment, ensuring compliance with ABDM guidelines and digital health standards. These standards also foster security in the ecosystem, with detailed guidelines on the steps a participant shall take towards data encryption and decryption.

The ABDM Sandbox aligns with the collaboration and public benefit principle, providing innovators with a dedicated space to experiment, validate, and refine their solutions. By incorporating open APIs and a self-assessment kit via an empanelled agency, Suma Soft, it adheres to the principles of transparency and inclusivity. Furthermore, Suma Soft's DEPA Validator ensures compliance through automated testing.

This sandbox is instrumental in catalysing innovation within the healthcare sector. It encourages risk-taking and learning without disrupting the broader ABDM system. The certification process, supported by Suma Soft, assures compliance, offering a reliable pathway for applications to transition from the sandbox to production. The sandbox's focus on milestones like patient registration and health record sharing reflects its commitment to improving patient outcomes. By providing a structured testing environment, it safeguards against potential system disruptions, fostering a culture of continuous improvement and collaboration in digital healthcare.

4.4. Ensure Transparency and Accountability with Appropriate Grievance Redressal Mechanisms (What)

Ensuring accountability and trust mandates the scope for public scrutiny and feedback through transparent DPI governance mechanisms with well-defined roles and decision-making processes. Appropriate disclosure requirements, supported by legislative and other norms for regulatory bodies, help furnish a comprehensive understanding of the DPI ecosystem and enable citizens to better realise their entitlements. By establishing the rights of individuals in DPIs comes the inevitable need to remedy grievances. The realisation of these rights must also extend to adopting consultative processes for implementation and revision that make the infrastructure open and responsive to feedback.

However, while building these systems and visualising their governance, it is also important to consider the spillover of functions and responsibilities of its regulation, management, and operation across ministries, administrative entities, and processes. Towards this, it must be ensured that accountability is translated into well-defined obligations and the adoption of clear channels of escalation for disputes with external oversight. Finally, accountability frameworks in this space must be rounded by appropriate disclosure obligations and processes that promote the translation of feedback into practice.

Tools (How)

1. **Publish DPI vision and strategy documents arising from expert deliberation. This fosters transparency and allows stakeholders to align their expectations with the long-term objectives of DPI.**

> ***Practice:*** The ONDC strategy paper provides an overview of the context, principles, and components of the Network. It highlights the benefits of ONDC for different stakeholders in the digital commerce ecosystem and its potential impact. The paper aims to gather input and perspectives to shape the design and principles of ONDC, fostering a collaborative approach towards its development. The ABDM ecosystem

> also operates with a larger strategy document. This was published by NITI Aayog in 2018, as well as the ABDM strategy overview that provides details of the larger scope of the DPI.

2. **Establish an independent nodal agency with authority to operate and monitor the DPI ecosystem. This ensures dedicated resolution for sector-specific considerations.**

> ***Practice:*** NPCI, a Section 8 company, is responsible for operating and monitoring the UPI ecosystem. Similarly, the UIDAI finds statutory backing to be the nodal agency for the Aadhar ecosystem.

3. **Establish clear procurement processes and define success metrics. This ensures transparency and accountability in the acquisition of resources and services for DPI.**

> ***Practice:*** Within the UPI ecosystem, banks release elaborate open requests for proposals to develop and maintain the infrastructure for clear details of the rights, obligations, terms, and conditions of the engagement. Similarly, public tenders are released on the NHA website for requirements within the ABMD ecosystem.

4. **Require disclosures on appointments and clarity on delegation of authority to enhance transparency and enable stakeholders to understand the decision-making structure within DPI governance.**

> ***Practice:*** ONDC publishes an extensive repository of the various committees and councils, and detailed network policies on the roles, processes, and service devolution mechanics on their website.

5. **Implement responsive and independent grievance redressal mechanisms to address complaints and provide effective remedies for individuals and entities affected by DPI operations.**

> ***Practice:*** NPCI follows a three-tiered approach to grievance redressals and complaints with portals mandated for the

> user-facing technology platform, the banks involved, and an overarching portal for NPCI in general. Similarly, ONDC’s proposed Issue and Grievance Management (IGM) system and Online Dispute Resolution (ODR) services adopt a decentralised approach to complaint resolution, empowering network participants to take ownership of resolving grievances.

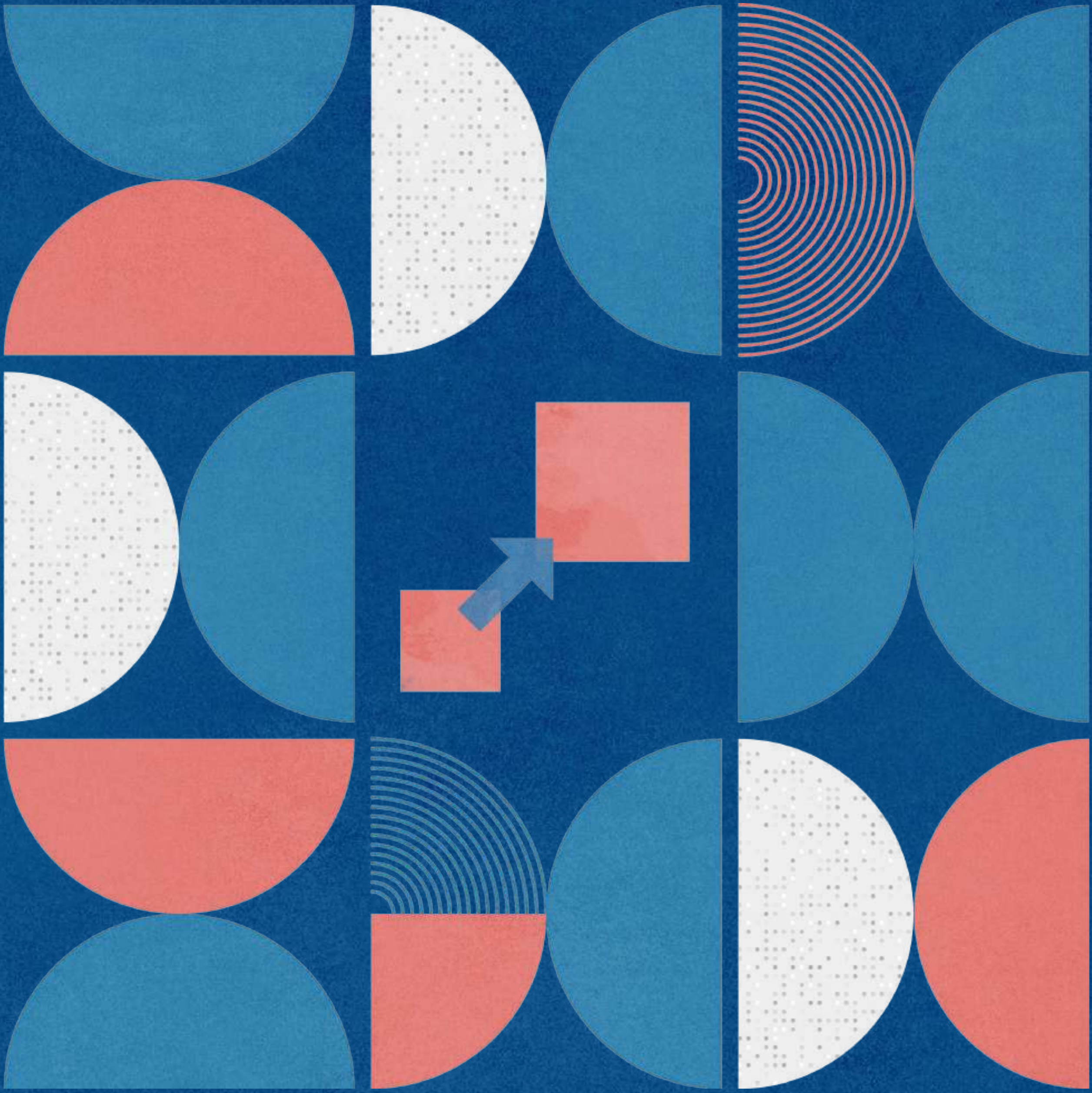
EXAMPLE 1:
Empowering Users: UPI's Decentralized Grievance Redressal

Unified Payments Interface (UPI) champions a decentralised grievance redressal system that involves three key stakeholders: Primary Service Providers (PSPs), Third Party Application Providers (TPAPs), and the National Payments Corporation of India (NPCI). UPI's innovative structure integrates a tiered model wherein users can escalate complaints through successive levels, starting from TPAPs to PSPs and culminating at the NPCI. This comprehensive design ensures that every user-facing entity in the UPI ecosystem plays an active role in resolving grievances, creating a dynamic and inclusive resolution pathway.

Aligned with the transparency and accountability principles, UPI's decentralised model distributes responsibilities clearly among entities. Each participant, be it a PSP or a TPAP, has defined roles in grievance resolution. This approach resonates with the principle of empowerment, and is envisioned to enable Network Participants with taking ownership and resolving grievances promptly. UPI's system adheres to a carefully delineated set of rules and regulations, emphasizing the need for secure and audited systems to maintain the integrity of UPI transactions.

SECTION 4

Way Forward



○ ○ ○ ● ○ ○

TABLE OF CONTENTS

ABBREVIATIONS

SECTION 4

Way Forward

The governance of DPI in India holds significant implications for the country's digital transformation journey and the delivery of public and private services. To this end, the evolving landscape of DPI in India presents both opportunities and challenges. While there has been remarkable growth and impact of various DPIs that aim to enable greater access and efficiency in service delivery, there is a growing need for responsible innovation to maintain public trust. This research unearths critical considerations to ensure adherence to principles such as inclusion, privacy, collaboration, and accountability.

Our paper examines practices around the operation of DPI in India, focusing on case studies on Aadhaar, UPI, ONDC, and ABDM, and the need for a comprehensive framework to guide their governance. Drawing insights from their governance journeys, the paper codifies a common framework based on an extensive analysis and a documentation of best practices for DPI governance. In our study, we recognise the interconnectedness of various DPIs and their collective contribution to the broader ecosystem of digital infrastructure; each with its specific objectives and implementation strategies. Subsequently, we present a unified governance framework that transcends individual DPIs and ensures synergy and alignment with a common set of core principles.

By adopting a principle-based approach, this study presents a set of values that underpin all DPI governance frameworks to combine inclusion, access, equity, privacy and security, collaboration, public benefit, transparency, and accountability. Our analysis presents tools to operationalise these principles within the DPI ecosystem. These tools offer a variety of pathways to select from when formulating the principles of a specific DPI.

Our study provides a framework for DPI governance with regards to:

1. The establishment of clear lines of authority
2. The adoption of transparent and accountable procurement processes
3. The implementation of robust security and privacy safeguards
4. The creation of accessible and responsive grievance redressal mechanisms

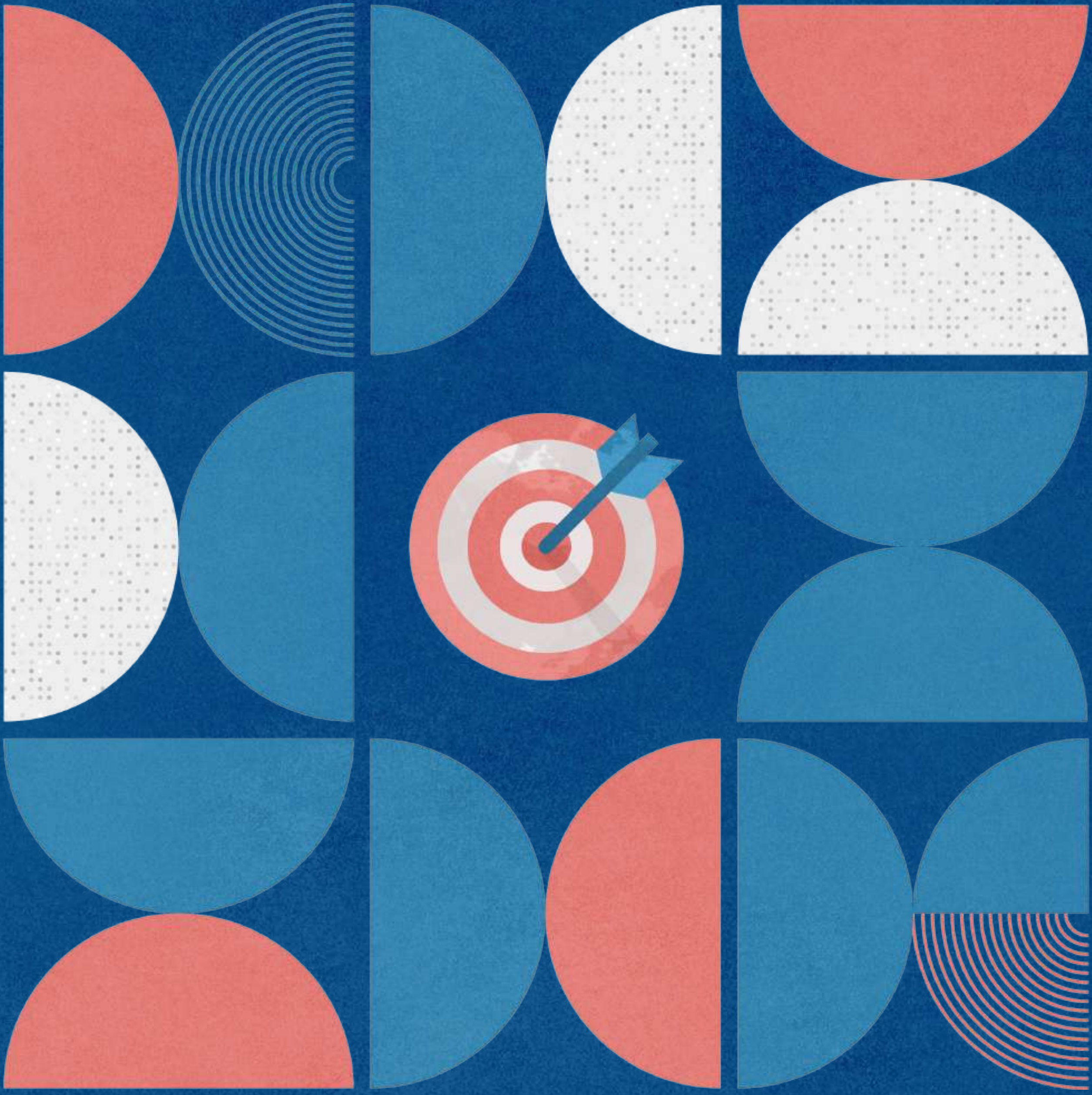
These form the foundation of a governance framework that upholds public trust, ensures equitable access, and promotes the welfare of marginalised communities.

In addition, ongoing capacity-building initiatives, awareness campaigns, and digital literacy programs are crucial to empower individuals and organisations to navigate the DPI ecosystem effectively. By enhancing technical skills, promoting data literacy, and fostering a culture of responsible use and protection of personal information, we create informed and engaged citizens who actively participate in shaping the governance of DPIs.

As India moves forward in its digital transformation journey, it is vital to ensure that DPI governance remains at the forefront, driven by the principles established in this study. These principles are not meant to be static. Rather, they serve as a foundation for continuous dialogue and adaptation. By embracing these principles within a comprehensive governance framework, India will position itself as a global leader in responsible, inclusive, and impactful DPI.

SECTION 5

Key Consultation Questions



SECTION 5

Key Consultation Questions

01 How can the governance of DPI be structured to align with the principles and values of public benefit, the welfare of marginalised communities, and societal impact, while ensuring inclusive and equitable access to DPI? Please provide specific recommendations and strategies to achieve these goals.

02 Mindful of emerging technologies and evolving societal needs, there might be additional considerations and concerns regarding the governance of DPI. What specific adaptations or improvements should be made to address these changing dynamics and maximise DPI's effectiveness and responsiveness?

03 How best can privacy protection be effectively translated into the design of DPI? What recommendations would you propose to embed the principle of 'privacy by design' within emerging DPI frameworks to ensure that individual privacy rights are upheld while enabling an effectively functioning infrastructure?

04 Collaboration and co-creation are essential drivers of innovation and address societal challenges in the DPI ecosystem. What are effective methods that foster interaction among stakeholders — Government agencies, private sector organisations, and civil society — and encourage partnership in design and implementation?

05 How can the governance of DPI be structured to align with the principles and values of public benefit, the welfare of marginalised communities, and societal impact, while ensuring inclusive and equitable access to DPI? Please provide specific recommendations and strategies to achieve these goals.

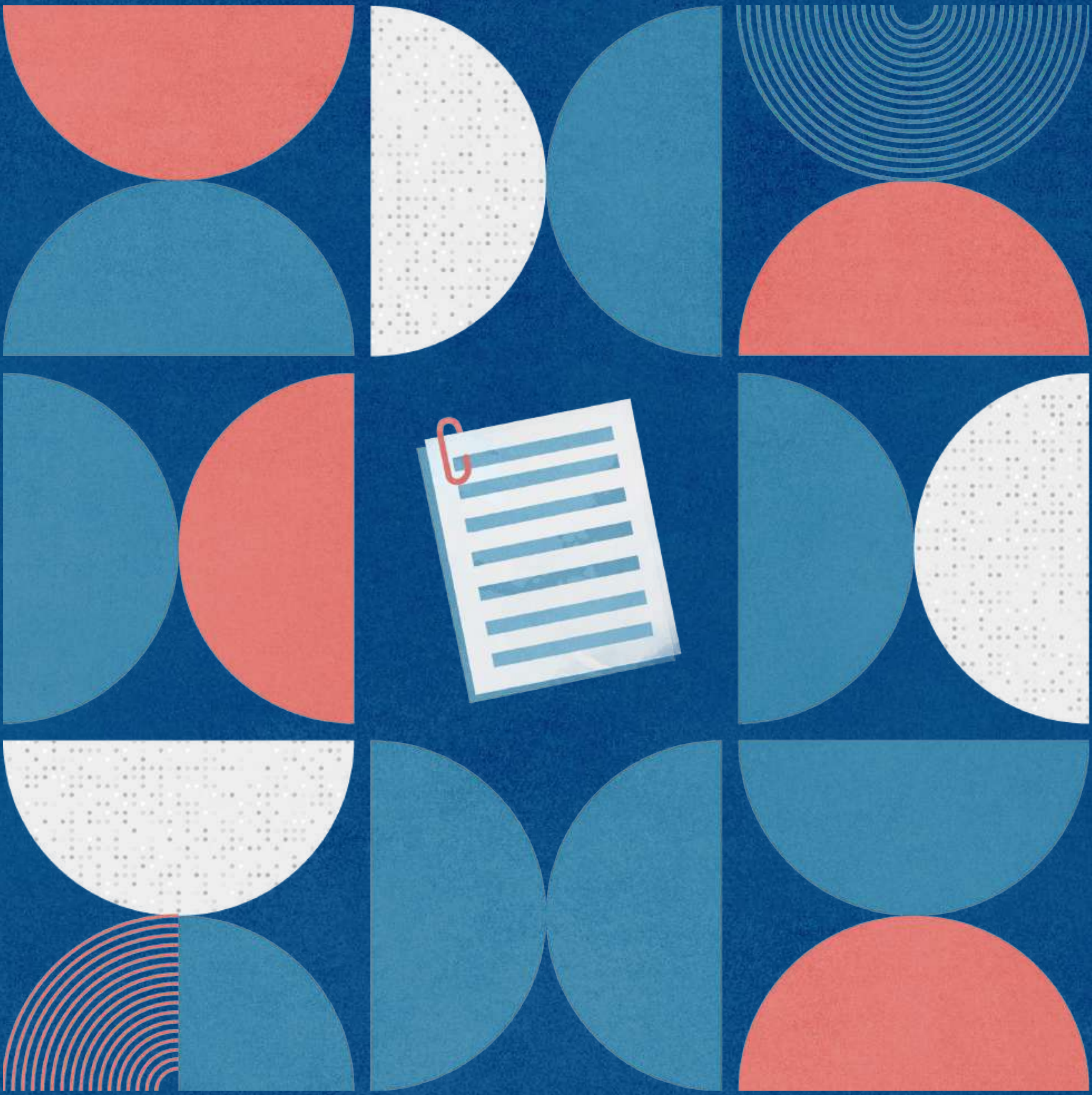
06 Mindful of emerging technologies and evolving societal needs, there might be additional considerations and concerns regarding the governance of DPI. What specific adaptations or improvements should be made to address these changing dynamics and maximise DPI's effectiveness and responsiveness?

07 How best can privacy protection be effectively translated into the design of DPI? What recommendations would you propose to embed the principle of 'privacy by design' within emerging DPI frameworks to ensure that individual privacy rights are upheld while enabling an effectively functioning infrastructure?

08 Collaboration and co-creation are essential drivers of innovation and address societal challenges in the DPI ecosystem. What are effective methods that foster interaction among stakeholders?

SECTION 6

Appendix



SECTION 6

Appendix

6.1. Aadhaar

Context and Introduction

Aadhaar is a biometric identification system implemented by the Government of India. Launched in 2009, Aadhaar provides a unique identification number to every resident of India, addressing challenges related to identity verification, efficient public service delivery, and inclusive governance.

The Aadhaar system utilises biometric and demographic data to create a unique digital identity for individuals. Biometric data such as fingerprints, iris scans, and facial photographs are collected, along with demographic information including name, address, date of birth, and gender. This comprehensive dataset forms the basis of the Aadhaar identification system. Aadhaar plays a significant role in facilitating financial inclusion and transforming various sectors. It has been integrated with Government schemes, particularly the Direct Benefit Transfer (DBT) program, to ensure that welfare benefits reach their intended beneficiaries directly. Aadhaar authentication is now essential to open bank accounts, obtain mobile connections, and conduct financial transactions, thereby enhancing security and streamlining processes.

With its widespread adoption, Aadhaar is the world's largest and most ambitious biometric identification program. As Aadhaar continues to evolve and expand its reach, it remains a cornerstone of Government efforts to enhance transparency, efficiency, and inclusivity in public service delivery.

Institutional Design and Functions

Aadhar is housed within the Unique Identification Authority of India, a statutory authority established in July 2016 as per the Aadhaar Act, 2016 by the Government of India. It operates under the Ministry of Electronics and Information Technology. The primary objective of UIDAI is to issue Unique Identification numbers (UID) –known as "Aadhaar" – to all Indian residents. Aadhaar numbers eliminate duplicate and fake identities and cost-effectively provide verification and authentication services. Under the Aadhaar Act, 2016, UIDAI is responsible for Aadhaar enrolment and authentication, including the operation and management of all stages of the Aadhaar life cycle. It develops policies, procedures, and systems to issue Aadhaar numbers, authenticate digital identities, and ensure the security and confidentiality of identity information and authentication records.

The UIDAI, as an intermediary authorised by the Parliament, exercises quasi-executive, quasi-legislative, and quasi-judicial powers within the Aadhaar ecosystem. Its executive powers encompass the entire lifecycle of Aadhaar, including enrolment, generation, and delivery/e-Aadhaar. The UIDAI also provides facilities for Aadhaar updates, e-KYC authentication, and other authentication services. These functions are executed through a network of registrars and enrolling agencies regulated and licensed by the UIDAI. Additionally, the UIDAI has quasi-judicial powers to suspend the licence of enrolling agencies and registrars when necessary. The specific details and processes of these functions are documented in the applicable Aadhaar regulations, rules, and procedures established by the UIDAI.

Further, as a statutory body, the UIDAI is governed by the rules outlined in its parent legislation, the Aadhaar Act, 2006. The UIDAI's structure includes key roles such as the Chairperson, Members, Chief Executive Officer (CEO), Deputy Directors General (DDGs), Joint Secretaries, and Regional Offices. The Chairperson provides overall guidance and leadership, while the other members leverage their expertise to support the organisation. The CEO is responsible for day-to-day operations, and the DDGs assist in various aspects of the UIDAI's functions. Joint Secretary-level officers contribute to policy-making and decision-making, while

Regional Offices play a crucial role in implementing Aadhaar-related programs at a local level. The UIDAI's statutory body status ensures that it operates within a defined legal framework and is accountable for its actions and responsibilities.

Technology Architecture

The technology behind Aadhaar combines biometric information, data management, encryption, authentication protocols, digital signatures, and open APIs to create a robust and secure identification system. This technological infrastructure enables the creation, storage, and verification of the Aadhaar identity numbers, ensuring accuracy, security, and efficiency in service delivery.

One of the key components of Aadhaar technology is biometric identification. Aadhaar captures an individual's biometric data, including fingerprints, iris scans, and facial photographs, during the enrolment process. These biometric templates are then stored securely in a centralised database managed by the UIDAI called Central Identities Data Repository (CIDR). The Aadhaar system also incorporates data management techniques. The massive volume of personal data collected during enrolment requires robust storage and retrieval mechanisms. UIDAI employs data centres with high-security measures and redundant storage systems to ensure data integrity and availability. Additionally, data encryption techniques are applied to protect sensitive information during transmission and storage, safeguarding privacy.

To ensure secure and efficient authentication, Aadhaar uses various authentication protocols. The Aadhaar Authentication System (AUA) allows authorised agencies and service providers to verify an individual's identity by accessing the centralised Aadhaar database. This verification process occurs in real-time, providing instant confirmation of an individual's identity. Authentication methods include fingerprint matching, iris scanning, One-Time Passwords (OTPs), and demographic matching.

The Aadhaar technology ecosystem also leverages digital signatures and Public Key Infrastructure (PKI) to ensure the integrity and authenticity of Aadhaar transactions. Digital signatures enable the verification of the origin and integrity of digital documents, ensuring that they have not been tampered with. PKI facilitates the creation and management of digital certificates, which are used to validate the authenticity of Aadhaar-related transactions, such as digital signatures on electronic documents.

Aadhaar embraces open APIs that allow authorised agencies and service providers to integrate Aadhaar services into their applications and systems seamlessly. This integration promotes interoperability and enables the efficient and widespread use of Aadhaar for various Government and private services, such as banking, telecommunications, and welfare programs.

Salient Governance Attributes

This section talks about the governance of Aadhaar, highlighting important aspects such as knowledge management, citizen charter, authentication methods, data security, grievance redressal, public consultation, and support channels for residents.

- **Knowledge Management Portal**
  The UIDAI established a Knowledge Management Portal to enhance internal communication, information exchange, and collaboration among its staff. This portal is a community-based platform that promotes teamwork and supports knowledge management practices within the UIDAI.

- **Citizen Charter**
  The Aadhaar Citizen Charter provides guidelines for the acceptance of various documents as proof of identity and address during enrolment. The UIDAI accepts a diverse range of documents to ensure that all residents can enrol, even those with limited access to official identity proof documents.

- **Paperless Offline e-KYC Verification**
  The UIDAI launched Aadhaar Paperless Offline e-KYC Verification. It eliminates the need for core biometrics and allows for paperless and electronic identity verification. This feature is particularly useful in cases where online e-KYC is not feasible due to connectivity issues or technical infrastructure requirements.

- **Right to Information (RTI) Compliance**
  While personal information unrelated to public activity or interest is exempted from disclosure under Section 8 (1) (j) of the RTI Act, the UIDAI ensures that residents can access their enrolment details, check Aadhaar status, and obtain E-Aadhaar through the UIDAI website or regional offices. However, privacy and confidentiality are maintained by not providing personal information to third parties or other residents.

- **Access to Aadhaar Information**
  Aadhaar number holders have the right to access their authentication records and e-KYC data stored in the UID database. UIDAI establishes mechanisms such as online portals, mobile applications, or designated contact centres to provide authenticated records to Aadhaar number holders, subject to specified conditions and payment of fees.

- **Encryption and Data Security**
  The UIDAI emphasises the privacy and security of Aadhaar data. While specific encryption algorithms and key strengths for the Aadhaar data vault are not specified, industry standards and best practices should be followed. UIDAI has introduced Aadhaar Data Vault to store Aadhaar numbers in encrypted form, reducing the risk of unauthorised access.

- **Public Consultation**
  The UIDAI publishes regulations for public consultation, ensuring transparency and stakeholder involvement in the governance of Aadhaar.

- **Integration through APIs**
  Aadhaar embraces open APIs, enabling authorised agencies and service providers to seamlessly integrate Aadhaar services into their applications and systems. This promotes interoperability and widespread use of Aadhaar for various Government and private services.

- **Support Channels**
  The UIDAI provides multiple support channels for residents, including a toll-free number, chatbot, resident portal, email, walk-ins at regional offices, and the Centralised Public Grievance Redress and Monitoring System (CPGRAMS) website. These channels facilitate complaints, queries, and access to information related to Aadhaar services.

6.2. Open Network for Digital Commerce (ONDC)

Context and Introduction

The ONDC is an initiative by the Government of India aimed at reshaping the digital commerce landscape in the country. ONDC envisions the creation of an open and inclusive digital commerce ecosystem that empowers businesses and consumers. It addresses the challenges faced by Small and Medium Enterprises (SMEs) in participating and thriving in the digital economy. By leveraging technology and promoting interoperability, ONDC aims to foster fair competition, enhance consumer choice, and drive innovation in the digital commerce sector. The platform is designed to provide a level playing field for all stakeholders, ensuring that SMEs can compete effectively with larger players.

Institutional Design and Functions

The ONDC platform is governed by a Section 8 company also called ONDC. It operates under the Ministry of Commerce and Industry and was established to promote fair competition, consumer protection, and interoperability in the digital commerce space.

The ONDC was officially incorporated as a Section 8 company in December 2021. The formation of the ONDC involved collaboration and investment from several institutions. The founding members of the ONDC include the Quality Council of India and Protean eGov Technologies Limited. In addition, several other prominent institutions have invested in the ONDC to support its objectives.

The ONDC has been entrusted with several functions to regulate and facilitate digital commerce in India. These functions include:

1. **Creating Regulations and Guidelines**
   The ONDC regulates entities in the digital commerce ecosystem, such as e-commerce platforms, logistics providers, and payment service providers. It establishes rules and guidelines for fair competition, consumer protection, and data privacy.

2. **Creating Standards for Data Sharing and Interoperability**
   The ONDC encourages data sharing among digital commerce entities and promotes interoperability to enhance competition and innovation in the sector. It sets guidelines and standards for data sharing, ensuring privacy and security.

3. **Facilitating Dispute Resolution**
   The ONDC facilitates the resolution of disputes arising in digital commerce transactions. It establishes mechanisms and processes for dispute resolution to ensure a fair and transparent resolution process.

Technology Architecture

The architecture of the ONDC is crafted to uphold several key principles that foster an inclusive and dynamic ecosystem. One of its primary objectives is to facilitate a decentralised and interoperable framework that encourages broad participation from both large and small retail players. By promoting autonomy and unrestricted movement of value across the supply chain, the ONDC empowers seamless transactions and interactions within the network. Moreover, the platform-agnostic discoverability feature ensures accessibility and compatibility across various platforms, enhancing user convenience. Embracing an ecosystem approach rather than a rigid 'system', the ONDC nurtures collaboration and synergy among diverse stakeholders. Emphasising open digital technology infrastructure, the platform acts as a catalyst to distribute problem-solving capabilities across the network. Through the adoption of open protocols, open registries, and reference apps, ONDC actively stimulates and activates large-scale participation, leading to a vibrant and inclusive digital commerce landscape.

The ONDC Network consists of three types of participants:

1. **Buyer Apps or Buyer Nodes**
   These participants handle buyer-side operations, including acquisition, search and discovery, and order placement on the network.

2. **Seller Apps**
   Seller Apps are responsible for seller-side operations and are categorised as Marketplace Seller Nodes (MSNs) or Inventory Seller Nodes (ISNs). MSNs function as marketplaces, while ISNs are sellers who also participate in the network.

3. **Gateways**
   Gateways play a crucial role in search and discovery by multicasting search queries and collecting results.

The legal relationships within the ONDC Network are defined by the Transaction-level Contract, which governs the terms of a specific transaction between a buyer and a seller. The buyer and seller have pre-existing legal relationships with their respective apps (Buyer App and Seller App) through terms and conditions or merchant agreements. However, there is no direct legal relationship between the buyer and seller apps. The ONDC Network Policy outlines the operational aspects for participants to transact on the network. It, along with the Network Participant Agreement (NPA), establishes the legal relationship between the apps and ONDC. These documents, in conjunction with the transaction-level contract, ensure fair, predictable, transparent, and consistent behaviour among participants. The hierarchy of rules of engagement on the ONDC network is depicted below. The transaction-level contract governs the specific terms of a transaction, while the ONDC Network Policy sets the general rules of engagement.

Salient Governance Attributes

- **Decentralised Governance and Three-Phase Grievance Resolution**
  The IGM system employs a three-phase approach to grievance resolution, incorporating specific tools for each stage. Internal issue resolution utilises collaborative platforms and communication tools to enable swift resolution within 24 hours. Grievance Redressal Officers (GROs) leverage dedicated ticketing systems and case management tools to address issues within seven days. For dispute resolution, the ONDC partners with ODR service providers that facilitate mediation, conciliation, and arbitration through specialised platforms.

- **Interoperability and Open Standards**
  The ONDC fosters interoperability and embraces open standards through dedicated tools and technologies. APIs are provided to enable seamless compatibility and integration with various technologies and systems. Existing DPI is leveraged with the help of open-source frameworks and development kits, promoting collaboration, innovation, and inclusivity within the ecosystem.

- **Access for Smaller Players**
  Specific tools like data sharing APIs and data analytics platforms enable smaller players to access and utilise critical data to create competitive solutions. The ONDC's draft regulations on personal data protection employ consent management tools, data access logs, and audit trails to address the misuse of personally identifiable information and ensure transparent protocols to obtain customer consent.

- **Clear Rights and Obligations**
  The ONDC's decentralised approach is facilitated by clear and transparent tools such as smart contracts, which create digital agreements between buyers and sellers during transactions. These smart contracts ensure that the rights and obligations of each party are explicitly defined, and automated protocols govern the execution of terms without the intervention of the ONDC as a third party.

- **Community-led Development**
  The ONDC's community-led development approach utilises collaboration tools, open forums, and version control systems like Git to gather feedback and insights from the public and stakeholders. Through active participation in the development process, community members contribute to refining the design and principles of the ONDC, aligning the platform to meet the diverse needs of players in the digital commerce ecosystem.

6.3. Ayushman Bharat Digital Mission (ABDM)

Context and Introduction

The Government of India launched the ABDM to promote digitisation in healthcare and establish an open interoperable digital health ecosystem. The mission establishes common health data standards and develops core modules such as health facility registries and healthcare professional databases for seamless data sharing among digital health systems. ABDM also focuses on digitising processes in healthcare institutions by leveraging available resources. The pilot project, initially known as the National Digital Health Mission (NDHM), was launched in six union territories on 15 August, 2020. On 27 September, 2021, a nationwide rollout was announced by the Prime Minister, renaming it to Ayushman Bharat Digital Mission (ABDM).

The ABDM fosters an efficient and inclusive healthcare system. It provides equitable access to healthcare and health records to all citizens, even in remote areas through alternative means like telemedicine kiosks. Registration to the ABDM system is free. Users have the freedom to opt out of the ABDM ecosystem, allowing them to deactivate or delete their accounts, though the latter results in the loss of linkage to digital health records. ABDM ensures a single source of truth by maintaining verified and authorised registries, eliminating the existence of parallel copies. Privacy by design is a core tenet of the ABDM, ensuring data security through a federated architecture and encrypted transmission. Participation in ABDM is voluntary for citizens and healthcare facilities, with respective managements making the decision, while healthcare professionals are encouraged to register with the Healthcare Professionals Registry for full integration with the National Digital Health Ecosystem (NDHE). These principles collectively drive the ABDM's mission to revolutionise healthcare accessibility, privacy, and efficiency.

Institutional Design and Functions

The NHA is an attached office to the Ministry of Health & Family Welfare (MoHFW) and is entrusted with the implementation of the ABDM. However, the role of the NHA is limited to the creation of an interoperable digital platform that enables communication and interaction between different digital health systems. This involves developing core modules or building blocks that other digital health systems should integrate with. The NHA can also recommend common standards and languages in a consultative manner.

The NHA is governed by a Governing Board chaired by the Union Minister for Health and Family Welfare. The CEO, an officer of the rank of Secretary to the Government of India heads the NHA. The Governing Board, led by the Union Minister for Health and Family Welfare, provides governance and a decision-making framework for the NHA. The CEO, as the Member Secretary of the Governing Board, manages day-to-day operations with support from the ABDM team, Deputy CEO, and Executive Directors, ensuring effective implementation of healthcare programs and partnerships. The responsibilities of the NHA include framing, amending, and repealing policies and administrative procedures, acquiring and maintaining a property, initiating contracts and agreements, receiving budgetary support, and exploring fund-generation opportunities. Additionally, the NHA drives strategic partnerships and collaborations with various entities to support its objectives.

At the state level, State Health Agencies (SHAs) are established as societies/trusts by respective states to implement the PM-JAY scheme. The SHAs have operational autonomy over the scheme's implementation in their states, including the extension of coverage to non-SECC beneficiaries.

The primary goal of the NHA is to address the existing gap in the digital space, ensuring that authorities within the healthcare ecosystem seamlessly integrate with the digital world. It facilitates integration and interoperability among digital health systems, without extending into the functions or jurisdiction of other authorities. NHA does not encroach upon the responsibilities of other authorities or entities. If certain permissions are granted by a specific authority, that authority continues to handle those permissions. Similarly, the regulation of healthcare professionals remains the responsibility of their respective councils.

Technology Architecture

The ADBM establishes interoperability among different digital health systems, eliminating the need for centralised storage of all digital health records. ABDM does not store any health data itself. It adopts a federated architecture where healthcare providers create and store the health data. It facilitates secure data exchange among authorised stakeholders on its network, ensuring patient consent is obtained. Through ABDM-compliant applications, patients have control over which health records they want to link with their Ayushman Bharat Health Application (ABHA) or digital health ID. Patients can securely store their digital health records on their devices, access them online, and securely share them with healthcare providers, consensually.

Only data collected for registries such as the ABHA registry, Healthcare Professional Registry (HPR), and Healthcare Facility Registry (HFR) is stored centrally. These datasets are crucial for interoperability, trust, identification, and maintaining a single source of truth across different digital health systems.

The ABDM operates through a well-structured information flow involving three essential components:

- **Health Information Providers (HIPs)**
  Includes doctors, diagnostic centres, and other healthcare providers. They are responsible for generating and maintaining health records.
- **Health Information Users (HIUs)**
  Include doctors seeking patient medical history for informed decision-making and citizens desiring access to their medical records. These HIUs request access to health information to meet their specific needs.
- **Health Information Exchange – Consent Manager**
  This is a gateway for information exchange. The Consent Manager ensures that health data linked to the ABHA is shared with HIUs only upon obtaining explicit consent from the ABHA owner. By upholding patient privacy and enabling secure and authorised information exchange between HIPs and HIUs, the Consent Manager ensures the confidentiality and integrity of health records within the ecosystem.

Salient Governance Attributes

- **Existence of a Governing Board**
  The NHA's Governing Board provides the necessary governance and decision-making framework for the organisation. It is chaired by the Union Minister for Health and Family Welfare and consists of domain experts from various fields, ensuring effective implementation of healthcare programs and partnerships.

- **The ABDM Grievance Redressal System**
  It is an online web-enabled platform designed to address grievances related to the ABDM building block. It allows the aggrieved party to submit complaints 24x7 using multiple channels, such as by post/letter, through the call centre, and through a grievance portal. Each grievance is assigned a unique tracking number for easy monitoring and resolution.

- **Capacity Building and Exposure Visits**
  The NHA emphasises capacity building and exposure visits for officers and officials from states and districts. Selected individuals are exposed to successful digital healthcare practices implemented in other countries or within India, contributing to the development of the digital healthcare ecosystem through knowledge sharing.

- **Incentives and Digital Solution Companies**
  The NHA incentivises stakeholders in the digital health ecosystem, including health facilities and Digital Solution Companies (DSCs). DSCs receive cost incentives for supporting smaller clinics, hospitals, teleconsultation platforms, and health lockers when they adopt digital health solutions and promote affordability and accessibility.

- **Health Data Management Policy and Consent Management**
  The Health Data Management Policy follows a consent-based approach, to ensure data privacy and align with existing legal requirements. Consent is obtained electronically or on paper, and consent managers maintain consent records and facilitate authorised data exchange.

- **Decentralised Storage and the ABDM Sandbox**
  The NDHM adopts a decentralised approach to health data storage, holding patient data at the point of care or the closest possible physical location. The ABDM Sandbox is a framework for technology and product testing, enabling seamless integration into the national digital health ecosystem.
- **Consultative Approach and Collaborations**
  The NHA collaborates with central and state Governments, public and private institutions, not-for-profit organisations, banks, insurance companies, academic institutions, and national and international bodies. This inclusive approach ensures diverse perspectives that shape healthcare policies and initiatives.
- **Inclusivity and Interoperabilitys**
  The ABDM promotes inclusivity through assisted and offline modes for the creation of Health IDs and Digital Personal Health Records, accommodating citizens with limited internet connectivity. Interoperability is facilitated through a federated architecture, allowing storage at multiple locations and providing a single source of truth across digital health systems.

6.4. Unified Payments Interface (UPI)

Context and Introduction

Introduced in 2016 by the NPCI and backed by the RBI, the UPI operates on the Immediate Payment Service (IMPS) infrastructure. It allows users to consolidate multiple bank accounts into a single mobile application using a unique Virtual Payment Address (VPA), facilitating effortless transactions. This system, leveraging standardised API specifications, offers a robust framework for secure, convenient, and efficient online payments. It aligns with regulatory standards to maintain financial stability. Initially starting with 21 banks, UPI has expanded to include 414 live members, significantly impacting digital commerce and financial accessibility for small and medium-sized enterprises.

The UPI streamlines payment processes by integrating various banking services onto one platform. It eliminates the need for multiple account credentials and simplifies transactions. The UPI fosters interoperability, allowing seamless fund exchanges between different financial institutions and payment service providers. It encourages financial inclusion, inviting participation from non-banked sectors by linking bank accounts with mobile numbers; thus broadening access to financial services. Moreover, it has propelled a shift towards digital payments by offering a secure platform for various transaction types, diminishing the prevalence of cash transactions and steering towards a cashless economy.

Institutional Structure and Functions

The UPI ecosystem in India operates under the primary governance of two central institutions: RBI and NPCI. The RBI, India's central banking authority, oversees the country's financial system, including its payment structures. It established the foundational strategy of UPI through its Vision 2018 document. This strategy emphasised the development of a secure, efficient retail payment system, eventually leading to the launch of UPI by the NPCI in 2016.

The NPCI, established in 2008, is the cornerstone of retail payment systems in India, working in conjunction with the RBI. It ensures system security, smooth operation, and stakeholder accountability, drawing authority from its status as a Payment System Operator designated by the RBI. While it operates as an independent non-profit entity, the NPCI maintains rigorous compliance with internal agreements across banks and payment service providers. These confidential agreements dictate the technical and operational prerequisites that integrate into the UPI ecosystem. Both the RBI and NPCI play crucial roles in the ongoing evolution of the UPI system, with the RBI providing regular regulatory guidelines and the NPCI handling technical and operational aspects. Through continuous dialogue with stakeholders, periodic reviews, and user feedback, these institutions collaboratively enforce compliance, address system challenges, and guide the technological progression of the UPI framework.

Beyond the NPCI and RBI, the larger UPI ecosystem comprises banks, Payment Service Providers (PSPs), developers, and end-users. Banks are integral, enabling customer access to UPI services and facilitating various aspects of the transaction process. They work closely with the NPCI to ensure system interoperability and regulatory adherence, forming the backbone of the UPI service infrastructure. Meanwhile, developers and PSPs innovate within this ecosystem by creating UPI-compatible applications, serving as a crucial bridge between users and the UPI mechanism. They continuously enhance these applications to ensure that they meet regulatory standards and user needs, thus expanding the UPI's reach and functionality.

The end-users, encompassing individuals, merchants, and businesses, utilise UPI services for diverse transactional purposes. By linking their bank accounts to UPI-enabled apps and forming unique identifiers and VPAs, users transact while also offering feedback. This collective input from users refines the UPI system's capabilities, security measures, and overall user experience.

Technology Architecture

The UPI technology connects all actors in a transaction flow, demonstrating the success of a ’5-party model’ over the traditional ’2-party model’, signalling significant disruption in innovation. The UPI is built on a secure, interoperable, and real-time payment infrastructure that enables users to make instant transactions from their bank accounts using their smartphones. The UPI platform operates on a unique VPA system, eliminating the need for traditional bank account details during transactions.
UPI leverages a combination of secure protocols, including two-factor authentication, encryption, and tokenisation, to ensure the confidentiality and integrity of transactions. The platform facilitates seamless fund transfers, bill payments, merchant transactions, and peer-to-peer payments, making it versatile and convenient for a wide range of use cases.

The UPI technology performs the dual function of enabling widespread user access and fostering collaboration and innovation in the ecosystem. The platform promotes financial inclusion by providing a simple and user-friendly interface, and the open architecture of UPI has encouraged innovation and competition, allowing various banks, fintech startups, and developers to build UPI-enabled applications and services, expanding the ecosystem's reach and functionality.

Salient Governance Attributes

- **Structured Feedback and Redressal Channels**
  A robust three-tier UPI grievance mechanism alongside dedicated portals for various participants, ensuring effective dispute resolution and continuous feedback.

- **Strategic Financial Planning for System Growth**
  Regular allocations in the union budget fostering adoption, complemented by periodic reviews of incentives or exemptions – catering to both users and transaction types – sustains and stimulates the ecosystem's expansion.

- **Capacity Enhancement and User Engagement Initiatives**
  A range of activities aimed at boosting system capacity, refining user experiences, and raising public awareness about UPI services, thereby promoting inclusivity and extensive reach.

- **Seamless Integration with Conventional Systems**
  Initiatives like the UPI-enabled cardless ATM withdrawals, emphasise a harmonious blend with offline transaction methods. This ensures accessibility and convenience across diverse user preferences.

- **Comprehensive Data Protection Protocols**
  Rigorous policies requiring informed consent for data handling, strict adherence to data minimisation principles, and user empowerment in data management decisions, safeguard individual privacy.

- **Robust Security Infrastructure and Regular Compliance Monitoring**
  Enforcing encryption standards, conducting regular audits, and maintaining continuous risk assessment procedures uphold integrity, confidentiality, and security in data storage and transactions.

- **Decentralisation and Transparency in Data Storage**
  Advocating distributed data storage methods to enhance security, coupled with obligatory disclosures, ensure transparency and accountability in data handling practices.

- **Inclusive Consultation for Technological Evolution**
  Codified consultative processes engaging diverse stakeholders, paired with the promotion of open technology-sharing protocols, fuel innovation, and systemic advancements.

- **Interoperable and Flexible Design**
  Directives ensuring all-encompassing interoperability and a modular approach to system architecture, guarantees a seamless, user-friendly, and future-ready transaction ecosystem.

- **Social Welfare and Financial Inclusion Policies**
  Dedicated strategies focusing on extending the UPI's financial services to the underprivileged and marginalised sectors, embodies the principle of inclusive growth and social welfare.

aapti institute

Aapti is a public research institute that works at the intersection of technology and society. Aapti examines the ways in which people interact and negotiate with technology both offline and online.

contact@aapti.in | www.aapti.in