5

Digital Sovereignty and Payments

A Case Study of the National Payments Corporation of India

Venkatesh Hariharan and Sarayu Natarajan

5.1 INTRODUCTION

In early 2014, the United States imposed economic sanctions prohibiting the export of American goods to Russia (Borger, Lewis, & Mason, 2014). MasterCard and Visa, credit card providers, rushed to comply, leaving millions of Russians without access to their credit accounts and several hundred billion dollars of assets frozen (BBC, 2014). At the time, these two American corporations controlled over 90% of the Russian credit card market. While services were restored within days, the situation prompted Russia to issue an alternative credit card – MIR. Since payments are the lifeblood of an economy, Russia also contemplated a law that will require payments providers to register in-country within a stipulated time or exit the country (Dettmer, 2019).

This incident in Russia and the US consideration in prohibiting Visa and MasterCard from operating in Venezuela as financial sanctions (Mason, 2019) raise questions about the value of sovereignty over fundamental digital infrastructures and the need to reclaim these in the public interest (Stanford PACS, 2020). In this chapter, we examine the intersection of India's indigenous payments system, the Unified Payment Interface (UPI) and the National Payments Corporation of India (NPCI), a special purpose vehicle set up to manage payments and strengthen India's digital sovereignty.

With this chapter, we wish to add to the growing literature on digital sovereignty. A non-Western view of sovereignty may add to the growing voices on policy and design around digital infrastructures in the Global South, applicable to digital infrastructures in other domains of state activity (e.g., technology used to access judicial services). We hope to inform policymakers, think tanks, and citizens of the trade-offs in building digital infrastructures for payments. Our chapter aims to highlight, through the study of the NPCI and

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

analysis, the key parameters and choices that policymakers, designers, and researchers might consider in evaluating investments in digital infrastructure. We do not aim to prescribe any course of action but merely demonstrate the choices available.

We find that, in India, the NPCI and the UPI are instruments that advance digital sovereignty. Following Pohle & Thiel (2020), we interpret digital sovereignty as combining the protection of infrastructure, enablement of market competition, and the enhancement of individual self-determination. We argue that technological, institutional, regulatory, and programmatic efforts are needed to enhance digital sovereignty, and these are the approaches policymakers globally may consider examining. The idea that digital infrastructures advance sovereignty finds articulation in the New Delhi Leaders' Declaration (2023, p. 22).

For this chapter, we select the UPI and the NPCI for analysis. The case study method allows us to surface structural characteristics that are worthy of study (Tillin, 2013). In this case, we explore those characteristics and approaches that have been important in the trajectory of the NPCI. We chose the NPCI because it speaks to emerging concerns around digital economies, payments, and sovereignty. This is additionally contextualized in the growing conversations around Digital Public Infrastructure (DPI) and Digital Public Goods (DPGs).[1] The NPCI's existence for nearly a decade now as well as India's experience with indigenous DPI development and governance have useful lessons to offer in terms of building flexibility and resilience into a country's digital ecosystems.

Methodologically, we combine a theoretical treatment of sovereignty with an empirical and practical understanding of the experiences and concerns of lawmakers and practitioners globally along with the performance of the NPCI itself. This effort looks at both the NPCI and the underlying technological architecture, the UPI. This empirical approach allows us to have a real sense of the efforts and trade-offs involved in building, deploying, and managing digital infrastructures while protecting citizens' interests. For this study, in addition to desk research, we conducted ten interviews with policymakers, practitioners, and experts in India and globally. Interviews were analyzed interpretatively by the researchers together.

We believe our work and approach and this analysis are significant for two reasons. First, we build on the emerging literature on digital sovereignty to emphasize the concerns and constraints of price-taker states, which have lesser bargaining power in negotiations. These states far outnumber powerful states but may lack similar bargaining power due to a host of economic and historical reasons. Understanding the parameters for consideration in building out digital infrastructures is significant for such states. Second, we examine the implications of sovereignty in the context of

[1] For more information on DPGs, see http://digitalpublicgoods.net.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

digital infrastructure guaranteed by the state (payments). Unlike sovereignty debates in the context of creative services (e.g., applications, software) that may concern issues such as monopoly, data protection, or abuse of power, payments are intimately linked to state function. Thus, interpretations of sovereignty need to additionally engage with the denial-of-service issues and their catastrophic implications for the economy.

This chapter is structured as follows: Section 5.2, following the introduction, builds a working definition of sovereignty. This definition relies on a broad interpretation of sovereignty and considers some of the critiques of such expansion. Section 5.3 describes the structure and operations of the NPCI in brief. Section 5.4 explores the workings of the NPCI through the framework and approach described in Section 5.2 and examines its successes and failures. Section 5.5 conducts a broad assessment of the working of the NPCI. A concluding section follows Section 5.6, providing possible avenues to address some of the concerns described in earlier sections, and explores some meta issues in the context of payments.

5.2 BRINGING THE STATE BACK INTO DIGITAL: BUILDING A WORKING UNDERSTANDING OF SOVEREIGNTY

In this section, we take a brief look at digital sovereignty and arrive at an operational frame for analysis. We follow Pohle and Thiel (2020) to unpack sovereignty as control over critical infrastructure, economic freedom, and individual agency. We then examine the threats to sovereignty and the mechanisms available to exercise sovereignty. Our analysis is underpinned by Floridi's approach of seeing *power as control* (Floridi, 2020). We argue that a sovereign state needs to control and protect digital infrastructures against state and nonstate and domestic and foreign threats through legitimate means available to it.

Sovereignty is the ability of a nation to make not only its own laws but also the ability to protect itself and its citizens from harm, achieve policy objectives, and enhance citizen well-being. The core meaning – sovereignty as the supreme authority over territory – emerges from the Westphalian notion of sovereignty, which bases state sovereignty on territoriality and the absence of a role for external agents in domestic structures. This definition of sovereignty places the state, whether liberal democratic or not, and its physical territory at the center of the imagination (Philpott, 2020).

In the digital realm, two main challenges to territorial notions of sovereignty have arisen: the ideas of cyber exceptionalism and multi-stakeholder governance (Pohle & Thiel, 2020). Cyber-exceptionalism sees cyberspace as exceptional and therefore contends that traditional frames of reference are not adequate (Pohle & Thiel, 2020). This has been articulated in multiple ways, starting with John Perry Barlow's 1996 declaration:

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." (Barlow, 1996)

Cyber exceptionalism is based on the premise that the rise of the internet implies the demise of state sovereignty and that national borders are rendered irrelevant. Multi-stakeholder governance is closely related to the ideas of cyber exceptionalism, which focuses on the roles played by various actors toward the development of shared norms and rules in the regulation and development of the internet. The ideas of multi-stakeholder governance emphasize open, consultative, and bottom-up decision making, involving those who are affected by decisions (Hoffman, 2016; Raymond & DeNardis, 2015).

Both cyber exceptionalism and multi-stakeholder governance are not a part of prominent narratives of digital governance. Instead, nations across the world are increasingly using the vocabulary of digital sovereignty to assert control over digital infrastructures within their borders. The term has become a way to bring back the state, as well as ideas of nationhood, economy, and citizenship, into debates around governance of digital infrastructures (Pohle & Thiel, 2020). There is a robust literature in the context of the European Union (EU) as the EU and its member states grapple with the emergence of technology giants who possess significant amounts of data as well as well as vast networks from which to mine data (Couture & Toupin, 2019; Gueham, 2017; Pohle & Thiel, 2020; Ruohonen, 2020).

In a context of increasing datafication of our lives, it is critical to examine conceptions of sovereignty and the role of the state. The state is relevant to examine for two reasons. First, individuals are increasingly engaging with the state through digital means across many arenas and domains. Several aspects of state functions such as welfare and government services are increasingly digitally mediated. Additionally, as Marianna Mazzucato (2018) has demonstrated, the state is central in framing and enabling the digital world. Her book, *The Entrepreneurial State*, demonstrates how the state does so through policies, subsidies, and infrastructure, playing a role in "making" the digital (Mazzucato, 2013). In that sense, the digital and the state cannot be parsed from each other. Importantly, digital goods and services are deeply connected with conceptions of liberty, rights, and norms, many of which are articulated through constitutional and legal frameworks at a national level. Accordingly, it is critical to center the state.

Second, the state is important in the imagination of digital infrastructures for the public. Many critical digital infrastructures are built using public funds and offer public services that emerge from statute or law, to which the principles of nondiscrimination and equal access apply. Nondiscrimination and access are enforceable in that citizens may bring claims in a court of law. Accordingly, the role of the state in ensuring this access for all necessitates an examination of state sovereignty and a deeper engagement with the state.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

To analyze relationships between the state and digital infrastructure and the functioning of the NPCI, we adopt the framing in Pohle and Thiel (2020). Their paper suggests that the reemergence of sovereignty in digital debates is founded in three strands of thinking: (1) state autonomy and the security of national infrastructures; (2) economic autonomy and competition for market actors within the territory, and (3) autonomy and individual self-determination for citizens. Of these three, only the first argument refers to a territorial sense of the state and the need to protect infrastructure. This is akin to the need for the state to protect digital infrastructures such as physical infrastructure. The other two aspects of sovereignty relate to state goals of protecting indigenous market actors to enable a fair and free market economy to flourish and supporting citizens' aspirations of self-determination (Pohle & Thiel, 2020). The second strand also speaks to emergent literature in the context of the EU that frames sovereignty as the need for the state to protect the interests of citizens and the ideals of a free and fair internet and to enable a free market and level playing field (Gueham, 2017).

Understanding sovereignty as autonomy and individual self-determination requires some thought to operationalize. We use the language of agency to unpack autonomy and individual self-determination. The work of Sharma and Natarajan (2020) suggests that agency is fundamental to individual self-determination. However, agency is a complex concept and needs to be seen near ideas of inclusion and equal access. Sharma and Natarajan argue that for technologies that arise from one's rights under constitutional or legal frameworks, the onus is placed on the state to ensure that all individuals have access, and therefore agency. Agency can be dimensionalized to include concepts such as choice (among alternatives) and ability (to make choices and bargain). Agency must additionally be framed within a language of rights, aspects of access that relate to individuals' rights under the constitution (specifically, Articles 19(1)(g) and 21[2]) (Sharma & Natarajan, 2020).

In our exploration in this chapter, we consider challenges to sovereignty from both state and nonstate actors. First, we consider state actors. States are sovereign entities themselves, subject to international law, agreements, and norms. Second, we consider nonstate actors. While nonstate actors may include legally established and recognized entities (e.g., corporations, both domestic and foreign) and unrecognized entities, we focus on the former category. We exclude bad actors such as hackers from the scope of this chapter. Indeed, all our interviewees concurred with the view that sovereignty must consider state and nonstate actors as oppositional forces that might undermine sovereignty.

We also need to address the question of how sovereignty is exercised, that is, what modes and mechanisms are available to the state and what the ultimate outcome of this exercise must be. Floridi (2019) articulates the latter through

[2] Article 19(1)(g) of the Constitution guarantees the freedom "to practise any profession, or to carry on any occupation, trade or business." Article 21 states that "No person shall be deprived of his life or personal liberty except according to procedure established by law."

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

the language of "control," that is, that power is control. Fioridi describes power as being both poietic (creative control, vesting with companies) and cybernetic (the ability to regulate or steer, vesting with the state). This framing and the delineation between creative control and cybernetic/regulatory control offer a way to think about the goals of the sovereign exercise of power, and the means available to the state. The goal of cybernetic control is attained through regulation and policies (Floridi, 2020). The cybernetic power is the control we attempt to assess through this chapter.

In this assessment, we must be careful not to depoliticize the idea of sovereignty and grant it only a functional and utilitarian character. A widened interpretation of digital sovereignty comes with simultaneous concerns about the expanded role of the state in business (Kelkar & Shah, 2019) and the enablement of a surveillance state (Srnicek, 2016). The availability of vast data to the state can enable large-scale violations of individual privacy. When combined with state power sans adequate data protection frameworks or procedural safeguards, individual liberties are at risk.

Sovereignty must not be seen as a frame to empower an already powerful state. Particularly, they must not enable ways to erode judicial and legislative checks and balances over executive power. The inadequacies of legal frameworks in the face of authoritarian governments' inclination to override them cannot be ignored. Equally, choices and practices of defending and defining sovereignty, particularly the ways in which questions relating to the individual are handled, are political in themselves as they are likely to privilege certain viewpoints and identities.

5.3 UNDERSTANDING THE NPCI AND UPI

NPCI, a nonprofit company regulated by the Reserve Bank of India (RBI), was set up as a DPI that manages the payment backbone of India. NPCI's majority shareholding is held by public sector banks and offers utility pricing for its services. For this chapter and analysis alone, we define DPIs as *technology infrastructures built/managed by the state for universal use and availability, and upon which innovation can occur*.

NPCI operates India's ATM networks, National Automated Clearing House to facilitate interbank transactions, the RuPay credit and debit card network and other payments infrastructures. In 2016, NPCI launched a new generation payment network called the Unified Payments Network (UPI), a mobile-first, open API-based, instantaneous payment network. While card networks have been around in India for decades, their penetration has been low. UPI enabled India to leapfrog to a mobile-first era of digital payments, similar to how countries leapfrogged the landline era and went straight to the mobile phone era. Countries that do not have card networks but have growing telecom and smartphone penetration have the potential to leapfrog the cards era straight into a mobile-first, UPI-like ecosystem.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

5.3.1 Understanding the UPI

India has built three key digital infrastructures: Aadhaar, UPI, and the Data Empowerment and Protection Architecture (DEPA). These three layers come together to form India Stack (n.d.) and provide identity, payments, and data as services. The payments layer of India Stack, which forms the subject of this chapter, has been housed within the NPCI, which is an umbrella organization for operating retail payments and settlement systems in India. It is an initiative of the RBI and Indian Banks' Association (IBA) under the provisions of the *Payment and Settlement Systems Act*, 2007, for creating a payment and settlement infrastructure in India (NPCI, n.d. -a). The NPCI has been set up as a non-for-profit company, with the goal of providing physical and electronic payment and settlement systems in India. Six public sectors, two private sectors, and two foreign banks were the ten core promoters. In 2016, the shareholding contained 56 members.

NPCI operates an array of infrastructures such as the RuPay debit, credit, and prepaid cards; the UPI, which is a mobile-first, interoperable payments network; and the Immediate Payment Service (IMPS). Launched in April 2016, the UPI has been the biggest success in NPCI's portfolio, achieving 2.5 billion transactions in January 2021 (NPCI, n.d. -b). UPI enables anyone with a mobile app from one of the 224 participating banks, or Third-Party Service Providers (TPSPs) such as Google Pay or PhonePe to make payments within the UPI network using QR codes or virtual Payment Addresses like abc@xyzbank.

Worldwide, payment networks have evolved as monopolies or duopolies, due to network effects. Consumers flock to the networks that have the widest acceptance, while merchants flock to the networks that have the most customers. In contrast, NPCI built UPI as a relatively open payment rails upon which banks can become payment service providers (PSPs), to their own customers, and to third-party apps such as Google Pay, PhonePe, and WhatsApp. The design of UPI and the institutional architecture of NPCI have many implications for digital sovereignty. This chapter will take a deeper look into them. Figures 5.1 and 5.2 explain the difference between card networks and the UPI network.

5.3.2 Cards, UPI, and NPCI

Traditional card networks are a three-party model with transactions routed from the payer's card to the switch, which sends the money to the payee's bank account. The switch is at the heart of the network, which is why when sanctions were imposed on Russia with which MasterCard and Visa complied, the lifeblood of payments came to a halt. Since 90% of card payments in Russia were routed through MasterCard and Visa, this had a very disruptive impact, leading Russia to create an indigenous payment system MIR.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

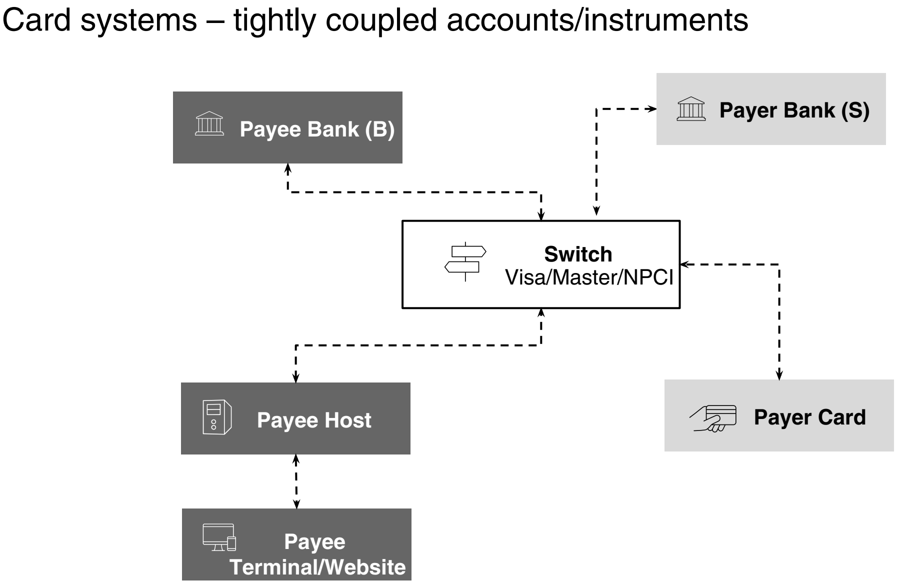

FIGURE 5.1 Schematic description of card systems[3]
Source: iSPIRT, Sanjay Swamy

In India, NPCI operates its own card network called RuPay, which has 60% share of the cards issued. In terms of value, MasterCard and Visa cards have a higher share because of incentives and cash backs. All three networks operate in parallel, and the existence of RuPay means that if MasterCard and Visa were to stop working, Indians have another network to switch over to.

RuPay also has a lower cost structure. Therefore, the Indian government has issued RuPay cards along with its financial inclusion initiative, the Jan-Dhan bank accounts. Over 424 million bank accounts were opened as part of an initiative to provide minimum balance bank accounts to the poor, so that money from welfare schemes can be transferred directly into the recipients' Jan-Dhan accounts. Of these 424 million accounts, 310 million users were issued RuPay cards (PMJDY, 2023).

5.3.3 UPI

In contrast to the card networks, UPI has been set up as a four-party model. The payer uses an app, which could belong to a bank or a TPSP. The key innovation in UPI was decoupling permissions from the payment instruments such as online banking. The UPI app acts as a permission collector and the user approves a payment through the app. This approval is sent to the payer's

[3] This figure is adapted, with permission from Sanjay Swamy, based on his presentation "Payments4G" at iSPIRT's Fintech Leapfrog Council on September 6, 2016 in Mumbai, India.

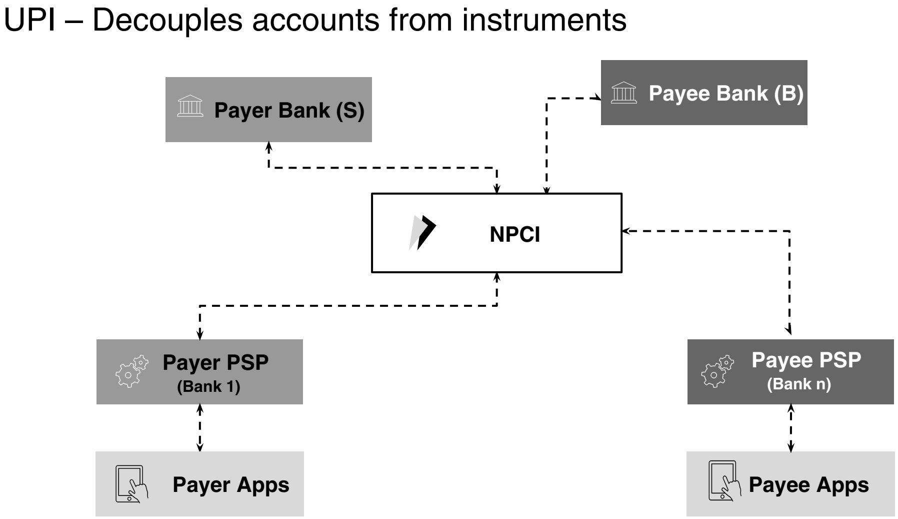

FIGURE 5.2 Schematic depiction of UPI[4]
Source: iSPIRT, Sanjay Swamy

bank account through the UPI switch controlled by NPCI and the payer's account is debited and the payee's account is credited.

Since the UPI switch is housed within NPCI, which is run as DPI and all UPI players have to connect to this switch, it is difficult for network monopolies to emerge. Interviewees suggested that TPSPs such as Google Pay and PhonePe have acquired a sizable market share of UPI transactions because of the incentives and cashbacks they offer, but not through network effects.

5.3.4 Understanding the Structure of the NPCI

The NPCI is the institution that houses the payments protocol, the UPI. Marianna Mazzucato (2013) has argued against the idea of the state as a collection of static bureaucratic organizations needed only to "fix" market failures, leaving dynamic entrepreneurship and innovation to the private sector. She has instead worked to reshape the narrative of the state's role in the economy to one of creating and shaping new markets.

In their working paper on the NPCI, William Cook and Anand Raman of the Consultative Group to Assist the Poor (CGAP) sketch out the history of NPCI where Indian regulators actively shaped its formation (Cook & Raman, 2019). In 1996, Y. V. Reddy (the then deputy governor of the RBI and later its governor) asked, "How far are we from global standards?" In the early 2000s when India's GDP grew at 7.3%, the country's payment systems were not keeping pace. The RBI's Vision Document for 2005–2008 scanned fourteen

[4] This figure is adapted, with permission from Sanjay Swamy, based on his presentation "Payments4G" at iSPIRT's Fintech Leapfrog Council on September 6, 2016 in Mumbai, India.

leading markets and found that very few central banks operate retail payment systems. In the Vision Document, RBI stated:

> The primary goal of any national payment system is to enable the circulation of money in its economy. It is recognised worldwide that an efficient and secure payment system is an enabler of economic activity. It provides the conduit essential for effecting payments and transmission of monetary policy. Payment systems have encountered many challenges and are constantly adapting to the rapidly changing payments landscape. More recently, the proliferation of electronic payment mechanisms, the increase in the number of players in the financial arena and the payment crises in quite a few countries and regions in the 1990s have focused attention on public policy issues related to the organization and operation of payment systems. Three main areas of public policy have guided payments system development and reform: protecting the rights of users of payment systems, enhancing efficiency and competition, and ensuring a safe, secure and sound payments system (Reserve Bank of India, 2005).

The Payment and Settlement Systems Act in 2007 allowed the RBI to authorize a company or a corporation to operate or regulate the clearing houses of banks, provided that at least 51% shares of such an organization are held by public sector banks.

All of this paved the way for the creation of NPCI. The body was set up as a nonprofit company that would answer to the RBI, but was operationally independent. The decision to structure as a nonprofit underscored the NPCI's utility nature from the outset. NPCI follows the principle of cost-plus pricing, and this enables financial inclusion and penetration across the country. Furthermore, NPCI is not driven by considerations of valuation and going public as are private corporations (Ramesh, Jangid, Sivamalai, & Rebelly, 2020). The nonprofit company status also allows the NPCI to be an agile organization that could hire the best talent available in the market.

Globally, payment systems have been privately owned duopolies because of the very nature of the business. Due to network effects, merchants and customers gravitate to the largest payment platforms, resulting in a few large players dominating the market. UPI was set up as a comparatively open, interoperable payment platform. Any bank can plug into the NPCI's backend system and offer UPI as a service to their own customers or to Third-Party App Providers (TPAPs) such as Google Pay and PhonePe. For customers, this means that they have a choice of more than a hundred UPI apps to choose from.

As of June 5, 2021, more than 224 banks were providing UPI transactions as a service by plugging into NPCI's UPI backend (NPCI, n.d. -c). Sixteen TPAPs such as Google Pay, the Walmart-owned PhonePe, and WhatsApp ride on top of banks who offer UPI services as registered PSPs of NPCI (NPCI, n.d. -d). These TPAPs collectively account for more than 90% of total UPI transactions by offering cashbacks and incentives with PhonePe accounting for 48.73% and Google Pay accounting for 37.31% of total UPI volumes in May 2021 (NCPI, n.d. -e). Since banking is a highly regulated sector, these TPAPs have to have an arrangement with one or multiple banks that provide UPI as a service.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

UPI is also a policy innovation because it was designed to be interoperable from the start. In many countries, payment networks have grown rapidly, and regulators have tried to enable interoperability in hindsight. For example, it is only after the rapid growth of Alipay and WeChat that China made them connect to Nets Union Clearing Corporation (NUCC), a public clearing and settlement institution for online payments.

The interoperability of the UPI platform means that, once a user has downloaded and signed up on UPI, they can instantaneously send money to anyone else on the UPI system. It must be noted that very few countries, including the US, have a mobile-first, interoperable national payment network that enables instant settlement. Enabling interoperability post-facto is often hard because the dominant players will always resist opening up their networks to other players.

5.4 NPCI AND SOVEREIGNTY

In this section, we explore the workings of the NPCI and the UPI (NPCI, n.d. -b) through the framework proposed in Section 5.2. We attempt to uncover the functioning and the performance of the UPI with respect to the three elements of sovereignty and then examine what states might do to respond to nonstate and other state actors. In doing so, we look at both technological approaches and institutional mechanisms.

5.4.1 State Autonomy and Security of Digital Infrastructure

The security of digital services from denial of technology remains the primary articulation of state sovereignty. As discussed earlier, situations such as the MasterCard, Visa, and SWIFT sanctions of Russia can be a threat to a given nation-state and the primary entry point for framing inquiries into state sovereignty. Policy shifts in other nations and insidious and criminal threats from malicious nonstate actors can heavily undermine the functioning of elements of the digital economy such as payments in this case.

This is articulated in two ways. First, the effects of geopolitical actions such as economic sanctions or war may result in private service providers having to comply with orders. This was demonstrated in the case of Visa and Mastercard in suspending their operations in Russia (Dettmer, 2019). Second, nations might want greater control over the payments infrastructure to achieve policy goals such as financial inclusion and regulatory oversight to accelerate a shift from cash to digital transactions, encourage competition and innovation, and prevent monopolies or duopolies.

Introduced in 2016, UPI has become the fastest growing payment network in India, achieving 2.5 billion transactions in May 2021 (NPCI, n.d. -b). Since the UPI switch is controlled by NPCI, which is an organization incorporated in India, UPI is relatively immune to sanctions. In the case of

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

card networks, if sanctions cut off access to MasterCard and Visa networks in India, customers will be able to switch over to the indigenous RuPay card network with relative ease. Therefore, UPI and RuPay networks insulate the country from sanctions that could lead to denial of technology.

5.4.2 Economic Autonomy and Competition

Economic autonomy, and the ability to foster self-reliance, innovation ecosystems, and sustained local businesses, is another articulation of sovereignty. The provision of a technical "infrastructure" and open[5] APIs lower the cost of innovation for local entities through lower barriers to entry. The NPCI structure and the open APIs under the UPI system theoretically enable innovation. Additionally, the NPCI has also made significant efforts in helping local businesses to innovate through hackathons.

However, the ability to leverage this infrastructure remains with corporate players. Large corporations have access to capital, data, networks, technical skills, and resources to develop and deploy a range of services very quickly. Despite the relatively open payment rails, October 2020 figures reveal that two US-owned entities – PhonePe (Walmart) and Google Pay – had 83% of the total volume of UPI transactions. This has prompted NPCI to issue a circular that no TPAPs can exceed more than 30% of the total volume of UPI transactions to curb the risk of a few parties dominating the UPI ecosystem.

Some of our interviewees highlighted the risk that by offering savings, investments, and a basket of financial services, TPAPs could control the consumer interface and reduce banks to back-end service providers. At a later stage, if they acquire a banking license, the need to rely on banks as PSP will also be eliminated. Therefore, there needs to be a deeper assessment of the risks involved in the consumer interface of UPI residing in two foreign-owned entities. If nothing else, the dominance of foreign-owned TPAPs on top of the UPI platform indicates that the task of protecting a country's digital sovereignty is not a static task but a dynamic one that involves technological, institutional, regulatory, and programmatic efforts.

Shifting from Cash to Digital: Cash is the most widely accepted form of payment. If an economy wants to move people from cash to digital, ensuring that digital modes of payment are widely accepted is absolutely essential. If a payer on network X is not able to pay a merchant on network Y, the utility of each network is greatly diminished for the payer and the merchant.

For merchants, cost is another factor that impedes adoption of digital modes of payment. Card networks entail a one-time payment for the point-of-sale terminal and minimum monthly transaction fee guaranteed by the

[5] NPCI code is not open source. It offers open APIs for innovation. See https://partners.apisetu.gov.in/directory/api/npci?ref=blog.quickwork.co. Accessed June 11, 2024.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

merchant, apart from relatively high transaction costs. With UPI, merchants need to set up a QR code connected to their bank accounts to start accepting payments. UPI transactions are free so there are no set-up or recurring fees. Merchants also like the fact that the money is credited immediately into their accounts. This has brought many new merchants into the ambit of digital payments.

For users, a high credit score is required to get a credit card, which restricts its reach to the relatively well-off section of Indian society. Since UPI (like debit cards) is attached to the bank account, there are no additional know-your-client (KYC) requirements to establish a customer's identity and identify risk factors. It is also easier to use since payments can be made and received using virtual payment addresses (similar to email addresses) or QR codes. This has helped take digital payments beyond the major metros in India to tier 2 and tier 3 cities in India.

Therefore, the UPI network has accelerated the shift from cash to digital by virtue of ease of use, interoperability, and lower transaction costs. The incentives and cashbacks offered by UPI players have also helped speed up adoption by consumers and merchants.

Encouraging Competition and Innovation: NPCI has conducted many hackathons to encourage innovations on top of the UPI platform. NPCI has also made it easier for small banks and third parties to provide payments as a service. Once an organization connects to the UPI switch, their customers can make payments to anyone else within the UPI network. This open-loop architecture enables firms to direct their energies to providing customer-facing innovations, instead of negotiating interoperability agreements and other related tasks that closed-loop networks would have to undertake.

UPI is also a payment system that has been built with open application programming interfaces (APIs) at the core. This has enabled players to build their customer-facing and merchant-facing apps on top of these APIs.

Preventing Monopolies and Duopolies: Policymakers have found it very difficult to regulate the winner-take-all model that results from network effects in the areas such as payments. Classical competition theory states that one should not regulate monopolies, but the *abuse* of such monopolies. However, this is easier said than done. Competition theory has not kept pace with the exponential growth of digital networks and their winner-take-all nature. China, which started with a light-touch regulatory regime, has moved to create NUCC, an NPCI-like organization, in response to concerns that capital flows through direct payment tools could be misused for money laundering and other illicit activities. NUCC allows the government to ensure interoperability among payment instruments and provides greater oversight of the payments ecosystem. In Kenya, mobile money interoperability became a reality eleven years after M-Pesa was introduced (Mburu, 2018) but reports indicate that such interoperability is quite cumbersome for consumers (Cook, 2018).

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

Payment networks can easily function as quasi-regulators. This helps the state keep direct control over the playground and its participants, as well as keep a check on monopolies. In the hands of a well-intentioned state, this can be a boon and in the hands of an ill-intentioned state, it can be a bane. However, the scope of this chapter centers around a state's *capacity* to maintain digital sovereignty, and not so much state *intent*, which could be the subject of a separate paper.

Interestingly, the rapid growth of UPI has also raised concerns within RBI that NPCI has become too big to fail. RBI therefore issued a policy paper on Authorisation of New Retail Payment Systems (Reserve Bank of India, 2019). Subsequently, RBI invited bids from organizations wishing to operate NUEs and seven consortia applied for the NUE license. This included a consortium led by a leading telco, Reliance Jio, which had members such as Facebook and Google, while another consortium was led by Amazon. Hariharan (2021) has criticized this move as it is likely to fundamentally alter the nonprofit, utility-pricing, and Indian-banks-owned nature of India's payments infrastructure. In August 2021, RBI put the plans for issuing the NUE licenses on hold. A MINT news report cited RBI's concerns over data security and compliance with its data localization norms as the reasons for this freeze (Gopakumar, 2021).

5.4.3 Individual Self-Determination and Inclusion

A third component of digital sovereignty is the ability to foster individual self-determination and inclusion. In countries such as India, social structures intersect with economic conditions to mediate vulnerable populations' access to technologies. This is increasingly being demonstrated in the context of areas such as payments (Borgonovi et al., 2018; Demtschenko, 2020) and governance technologies (Sharma, Natarajan, & Udhayakumar, 2020). These barriers are being observed across geographies as well. The literature suggests that across contexts, the already disadvantaged, and those who are on the vulnerable side of the digital divide are doubly disadvantaged when systems shift toward digital ones (Sharma, et al., 2020). The digital gender divide, for example, hinders the ability of women to participate freely in the economy. This circumscribes opportunities for economic development, including by limiting access to markets, or worse, to entitlements and welfare from the state.

Examining the accessibility of the NPCI in this context and the ways in which its design and implementation encourage inclusion and agency is the third element of sovereignty. The structure of the UPI that fosters interoperability across different payments systems is a critical element of this accessibility. M-Pesa, another digital payment system, is similarly interoperable, though it is far less so than the UPI. This type of technological interoperability lowers the barriers to entry as all banks can "communicate" with each

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

other. Interviewees identified interoperability as a critical element in driving inclusion and agency for users. Interoperability encourages firms to innovate and reduces friction and risk in everyday transactions. Together, these enable inclusion and agency.

Interoperability also allows firms to develop applications to service preferred market segments, distributing the costs of widening reach and allowing the development of innovative methods. For instance, Google has developed Google Pay/Tez to provide a payments interface application to its users; PhonePe and Paytm operate on a similar premise. Our interviewees pointed out that this offers significant advantages in that firms are then incentivized to innovate in order to make payments available to wider segments of the population and expand their customer bases. This widens the choices available to individuals, in turn supporting agency and inclusion.

Additionally, interoperability also reduces friction in everyday payments transactions. An example of this is the reduction in the need for communicating bank account numbers. Payments are immediately credited, reducing the latency between the issue and receipt of payments. This allows for reduction risk in the payments process.

However, as our interviewees pointed out, neither increased agency (as choice) nor reduced friction are adequate for inclusion. Nor are they addressable through technology alone. Indeed, as established earlier, there are profound challenges of inclusion and these fault lines map onto existing social cleavages of gender and geography in the Indian context. This requires institutional structure and programmatic efforts to be critical elements of this process. In this regard, the NPCI's structure as a not-for-profit and its programmatic efforts are noteworthy.

The NPCI is structured as a nonprofit entity. The multi-stakeholder governance approach (representation from stakeholders) ensures that the NPCI represents diverse voices (NPCI, n.d. -f). The involvement of public sector banks also carries connotations of stakeholder engagement. However, the NPCI may additionally need to make efforts to make the process of governance itself inclusive. For example, the structure imagines the inclusion of civil society. In reality, no civil society organization is a part of the NPCI's formal governance. Nor is there any subcommittee of the board or formal mechanism to consider financial inclusion.

Additionally, programmatic efforts are also an important component of inclusion. Given the difficulties in developing an application that is widely available and accessible, the NPCI developed the BHIM application.[6] This is a reference application to work in low resource settings, available in multiple languages. The design and maintenance of BHIM by the NPCI ensure that it continues to be available to those who need it. This programmatic effort is valuable

[6] BHIM is a low-frill app provided by the government that leverages the UPI.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

for inclusion. However, the NPCI needs to be mandated and incentivized to continue engagement with voices and actors who may further widen reach and address problems of ability and access to infrastructure on the ground.

5.5 DISCUSSION: ASSESSING THE NPCI

In this section, we assess the impact and effectiveness of the NPCI from a state digital sovereignty perspective. The empirical evidence and the interviews gathered so far suggest that the NPCI addresses some aspects of digital sovereignty. The fact that the UPI payment rails are hosted and governed within the territory of India offers insulation against denial of technology regimes. However, the fact that the dominant entities on the UPI rails are foreign entities who might leverage their hegemony to enter adjacent areas such as savings, insurance, and loans opens up a new set of challenges from a digital sovereignty perspective for regulators.

An additional concern is that the character of the NPCI, which can be classified as a state-sanctioned monopoly, may result in institutional capture. The NPCI structure has representation from a range of actors. However, over time, representation may exclude those entities (e.g., civil society) that lack the capacity to participate and engage in national-level institutions.

Equally, corporate power may impact the process of inclusion. To address this, RBI has proposed the setting up of New Umbrella Entities (NUEs) for retail payments, which would compete with NPCI, while interoperating with it. If Big Tech companies win the NUE licenses, it might invert the power relationship between banks and Big Tech. Currently, Big Tech companies operate as Over the Top (OTT) players on top of UPI Payment Services provided by banks. If Big Tech NUEs become a reality, banks will become OTT players on Big Tech payment platforms. Concerns have been expressed that since the bidders for NUEs include telecom giant Reliance Jio and firms such as Facebook, Amazon, and Google, the NUEs might undo the work of NPCI in ring-fencing India's digital sovereignty and keeping the power of Big Tech in check (Hariharan, 2021).

In addition, since the NPCI is a government-regulated entity, fears of government surveillance remain. Threats from bad actors should not be leveraged by the state to acquire more power to the detriment of citizens. In particular, executive actions without judicial scrutiny must be guarded against.

Insulating the economy from state sanctions: NPCI controls the switch that routes the vast majority of payments within India. The major foreign payment players in India are the card networks, MasterCard and Visa. If US sanctions pull the plug on these card networks, it would immediately benefit the indigenous RuPay network that is the dominant network with 60% of credit and debit cards issued in India. On UPI, the biggest players are foreign-owned

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

entities such as Google Pay and PhonePe (owned by Walmart), which collectively operate 80% of the UPI transactions. In a worst-case scenario, if they were to be switched off, it would not impact the underlying UPI network, which is controlled by NPCI. Given that UPI is an interoperable network, the cost of switching from one UPI app to another is negligible for customers. It is likely that they will switch to NPCI's BHIM app or one of the 200 plus banks that offer UPI as part of their mobile banking services.

India's ATM networks, Real Time Gross Settlement (RTGS), Immediate Payment System (IMPS), National Automated Clearing House (NACH), and others are also operated by NPCI. Therefore, India is well protected from shocks that might result from sanctions imposed by foreign states.

Deepening Digital Payments: Having control over the payment infrastructure can be helpful for attaining policy goals. A major policy goal in India has been to move the economy away from cash to digital, as this reduces black money transactions and encourages better tax compliance and financial inclusion. High Merchant Discount Rates (MDR), which is the transaction fee that merchants pay to the card networks, has been one of the factors that hindered the growth of digital payment networks. With retailers usually operating on a 5% margin, an MDR of 2–2.5% can cut into their profits. Therefore, retailers would sometimes include this fee in their total bill, which incentivized customers to pay in cash instead of card. Regulatory intervention in 2012 brought down MDR on debit cards from 2.5% to between 0.75 and 1% since debit card transactions are directly debited from users' bank accounts and carry no credit risks (Reserve Bank of India, 2012). MDR on debit cards was further reduced (Reserve Bank of India, 2017). Similarly, NPCI trimmed the ATM interconnect fee in 2012 from INR 8 (0.11 USD) charged by MNC networks to INR 0.45 (0.0061 USD), which enabled greater debit card usage (Baruah, 2016).

Reducing the cost of cash: RBI estimates that the net cost of cash amounts to 1.7% of the GDP, compounded by the possibility of abnormal losses of cash via accidents.

Regulating the domestic payments ecosystem: For context, the Chinese government pulled the plug on Alibaba's IPO because it had become too big to fail (Salmon, 2020). Beijing also tried to bring in interoperability among domestic payment systems through NUCC (Knowledge at Wharton, 2018). Imposing interoperability post-facto is difficult unless the regulator brings a strong hand to bear on the implementation because dominant players have every incentive to thwart its success and retain customers within a closed-loop, non-interoperable network. By design, UPI has avoided this problem. Once a bank connects to the NPCI's UPI backbone, its users could make payments to anyone else on the UPI network. To reduce the systemic risk of any one TPSP becoming too big to fail, NPCI issued a volume cap of 30% for each TPSP (NPCI, 2021) on January 1, 2021 and gave organizations two years to comply. Implementing such rules might have been difficult if NPCI was not run and operated as a DPI.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

5.6 RECOMMENDATIONS

Besides sovereign "control," a well-implemented payments infrastructure can have a multiplier effect on an economy and help achieve policy goals such as financial inclusion, better regulation of an economy, and transfer of benefits directly to citizens' bank accounts during pandemics such as COVID-19. Therefore, policymakers may consider implementing a UPI-like payment network, keeping the following factors in mind:

Interoperability: If the policy objective is to give citizens an alternative to cash, interoperability must be strictly enforced. An open-loop network such as UPI, with regulatory oversight and strict action against bad actors, can help countries provide their citizens with an attractive alternative to cash. This involves significant investments in technology, regulatory capacity, branding, marketing, and enforcement.

Multi-stakeholder governance: Interoperability has to work hand in hand with sovereign control over core elements of the stack (e.g., registries and API design) and robust governance of private parties. While the government manages and regulates the payment network, private sector players who build on top of this network need a stable policy regime to enable their investments to be amortized over a reasonable period. Voices of civil society, privacy advocates, and financial inclusion activists must also be factored into the network's roadmap. This includes establishing robust integrity measures and checks as well as feedback loops.

Ownership: The consortium model followed by India (NPCI) with majority of the ownership of the infrastructure company being held by Public Sector Banks is one model that can be considered. In this model, the infrastructure company offers utility pricing and is run as a nonprofit. For-profit entities such as banks and TPAPs operate on top of this network. This enables regulatory oversight and prevention of money laundering and other illegal activities that would be hard to trace in a closed-loop network. If the infrastructure layer is operated by for-profit companies, countries must invest in significant regulatory capacity to ensure speedy dispute resolution and smooth functioning of the network.

Institutional checks and balances: A critical element of sovereign function, especially in the liberal democratic construct, is the requirement to serve and be available to all citizens. Access to payments can be interpreted as a component of life and liberty. Moreover, the unregulated institutions can end up amplifying powerful voices at the expense of others, causing harm in the process. Since payment is a sovereign function and norms of inclusion and access are central to sovereignty, exploring some measure of judicial scrutiny and review of actions may be useful. This may be done through the power of writ in the hands of citizens or widened applicability of legal frameworks.

Risk mitigation: Policymakers must conduct periodic risk assessments of the payment network from technology changes such as crypto currencies and cybersecurity risks.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press

5.7 CONCLUSION

As a DPI, India’s UPI has succeeded beyond most expectations. UPI, which is housed inside the NPCI and governed by the RBI, operates as a nonprofit utility. In the month of August 2021, UPI recorded 3.5 billion transactions worth Rs 639,116 billion (or USD $86 billion). India has the technological, institutional, and regulatory capacity to pull this off with a sizeable domestic market that supports such a massive scale of transactions.

However, many countries might lack such deep state capacities. Such countries could consider a variety of other options. Open-source DPGs such as the MojaLoop project could provide some technological infrastructure. Multilateral agencies could also support the deployment of these infrastructures for specific contexts, and the creation of regulatory capacity. For countries that do not have populations to support large-scale transactions, technology service providers could support cloud-based deployments. These deployments could be based on open standards and APIs that allow payment networks in different countries to work with each other.

India’s UPI and NPCI offer a case study that demonstrates that a DPI-based approach can provide a viable alternative to private sector-payment networks. More work is needed to understand the different ways in which countries with and without the capacity to build digital payment systems might need to grapple with these issues of sovereignty. There are emergent efforts to promote DPGs in payments and other areas (Digital Public Goods Alliance, 2021), which may become available. Indeed, the New Delhi Leaders’ Declaration acknowledges India’s commitment to establish the One Future Alliance, which aims to bring financial and technological capability to countries in need (G20 New Delhi Leaders’ Declaration, 2023, p. 22). The hope is that these efforts, in addition to driving resources, can foster a culture of inquiry and engagement.

https://doi.org/10.1017/9781009531085.008 Published online by Cambridge University Press