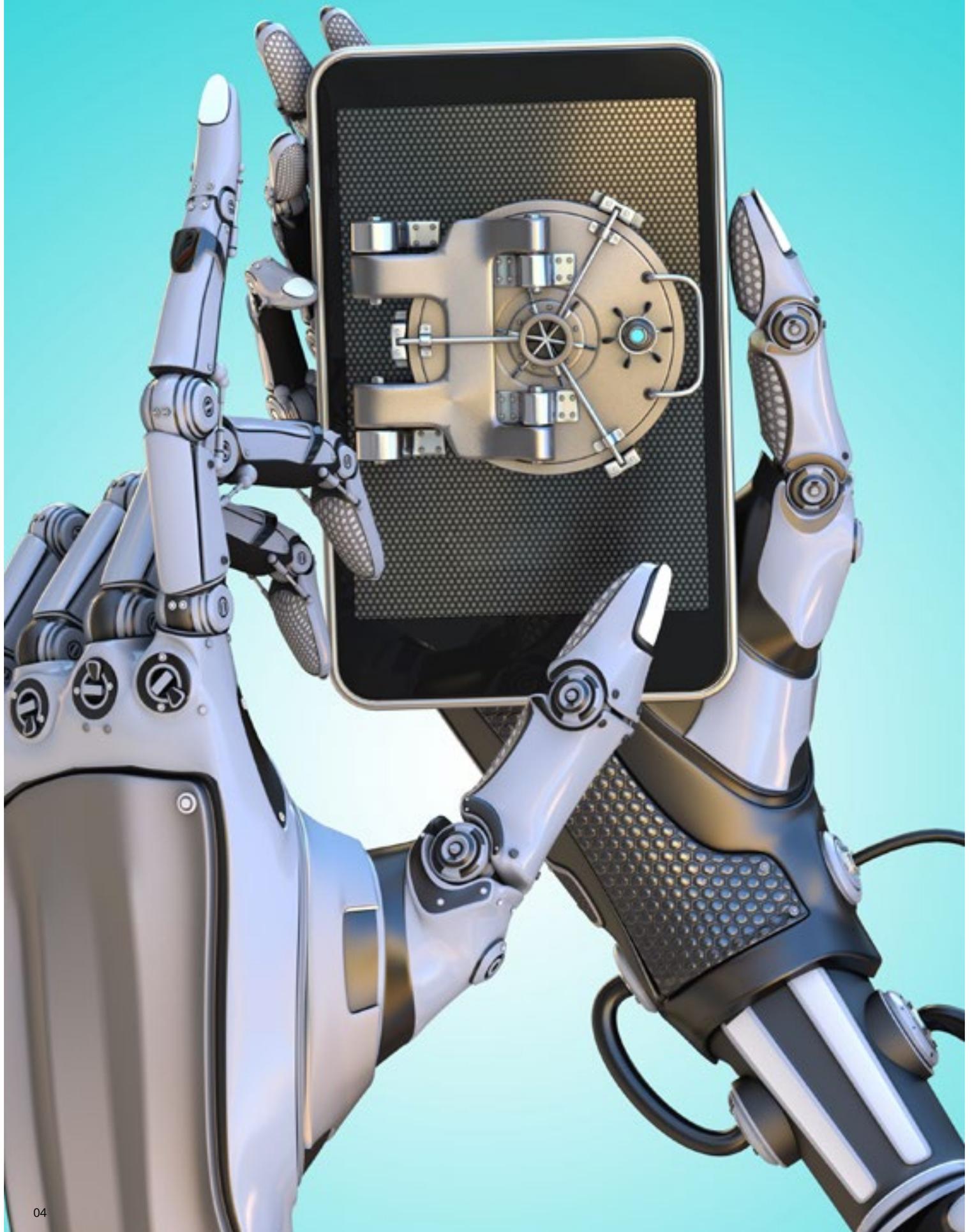


Contents

Foreword	05
Introduction	06
Banking and Financial Services: Powering services for mainstream adoption and balancing security of data	08
Digital disruption: Trends, exponential technologies and challenges	16
Evolving Role of Regulator in Digital India	26
Glossary	30
Additional References	32
Acknowledgements	33



Foreword

The banking model is being unbundled with the range of service providers widening, technologies making service offerings more personalized and on demand, and customers making informed decisions, leveraging advances in data science. Players are using agile processes, so that products and services can get to markets sooner and be adjusted along the path. “Mutualization” is a case in point. The evolving regulatory and market landscape is requiring companies to gradually realign their operating model to protect margins. Industry efforts to rationalize costs through down-sizing, outsourcing and automation have not yielded the savings and improvement in service quality that was originally envisaged. Mutualization, or the use of common standards and/or market infrastructure, is enabling non-core activities to be packaged and provided as a service to market participants. It is allowing financial institutions to share costs, boost efficiency in the back & middle office and restore focus on core business activities. It has applications in optimizing collaterals, movement of securities, KYC record management, and is already showing significant results in reducing KYC/AML costs.

Incumbent players have up their ante and are embracing these changes, as well as emerging competition. They are seeking to convert banking consumers who use digital touch-points to brand loyalists, as also to widen their user base. All sectors with large connect to customers, leverage disruptive tools when doing financial settlements with their customer base. Due to ecosystem

partnerships forged by service providers across sectors, customers are exposed to a host of additional choices offered by the partners. Use of data to deliver the right customer experience, leveraging innovations to make offerings simplistic and to give the customer complete control are the new guiding principles for service providers. Some firms are choosing to bridge gaps in internal capabilities and adopt a more holistic and value-based approach by understanding that all these applications are not always a panacea. Organizations will have to make choices, that include trade-offs. They will need a vision of their future, the applications of these in the context of their overall strategy, culture and structure. They have to evaluate the key considerations in implementing changes and aligning them with their ambitions.

At an ecosystem level, development in banking infrastructure and implementing regulations that are receptive to innovations and data requirements are also required.

We are not there yet and have a lot to learn from other players and markets where this is being/has been done well. Moving to a future state where financial services make our lives better requires heavy investment in emerging technologies, skillsets, risk management. To leverage disruptions players across sectors must:

- Think Exponential – Set bold goals and allow failures
- Execute Agile – Allow ideas with short iterative sprints with empowered teams

- Protect the People – Avoid departmental silos and allow uniform information distribution
- Place your Customer First – Fulfilling customers should be the priority
- Avoid status quo – Try new ideas in solving old industry issues
- Focus on Value – Revenue should always be the key driver for any idea
- Make design thinking the way of work
- Acquire capabilities to catalyse the culture
- Balance the risk approach – encourage controlled risks in right circumstances, while remaining cautious when engaging in high-risk activities

We hope you find this report useful in rethinking your value propositions to win over tomorrow's demanding customers.



Kalpesh J. Mehta

Introduction

The confluence of technology, new initiatives powering banking such as FinTech, data security, and a progressive regulatory environment, are offering radically new possibilities to achieve the Government's vision of a Digital India.

Our state of readiness - is far from ideal, as a serious divide exists between the unserved and the served. For financial services to make our lives better, there are costs to be borne, but the end-goal is desirable.

Insights gleaned by us from our experience in the industry have been reflected in this Point of View, as we put the spotlight on the key factors that can help achieve the vision of a progressive, responsible, and digitally powered India.



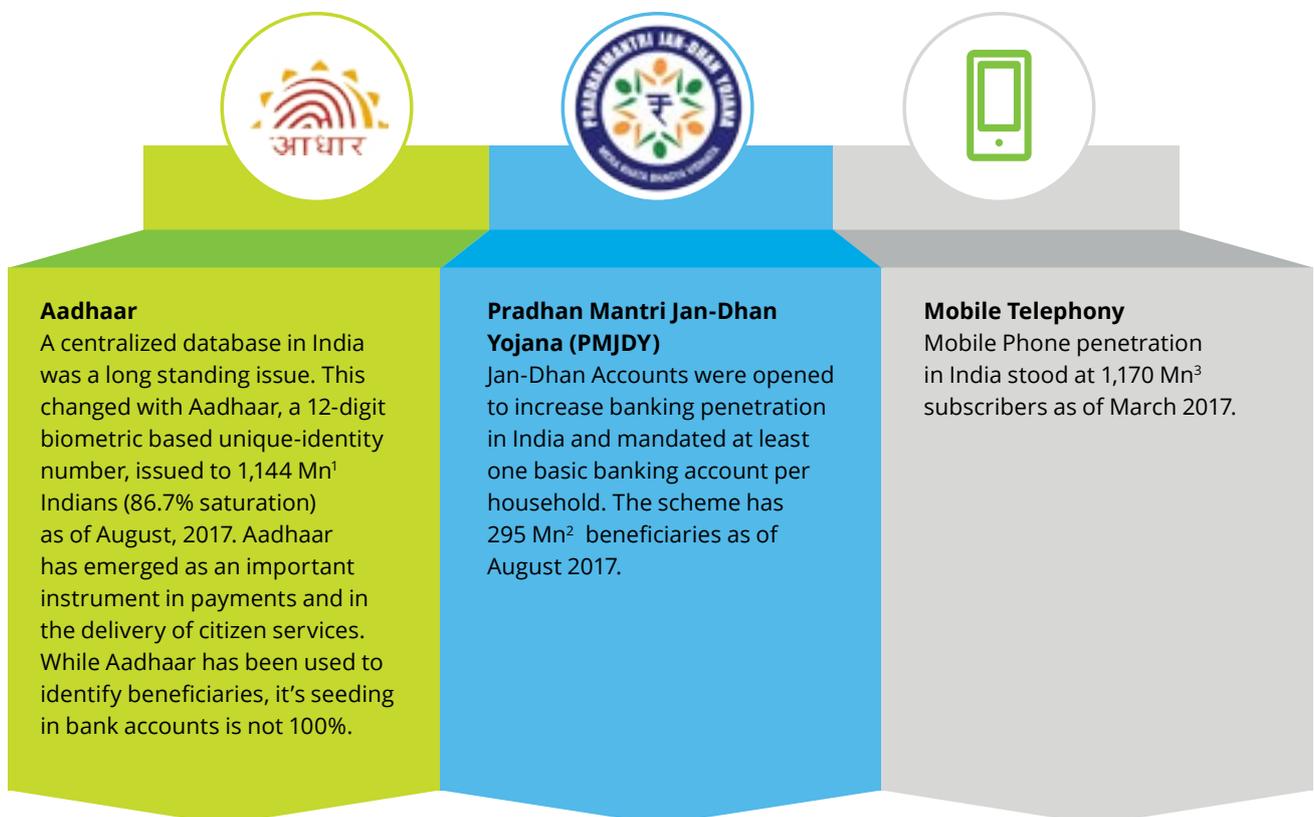


Banking and Financial Services: Powering services for mainstream adoption and balancing security of data

Introduction

The financial ecosystem in India is undergoing a transformation. Trends that are taking root cause in financial services and emerging business models, are bringing a larger no. of people under the financial inclusion umbrella. These are changing financial services delivery, and a new financial system is emerging.

The vision for a Digital India requires immense interoperability between data, mediums, identity systems, bank accounts. Leveraging Jan Dhan, Aadhaar and Mobile (JAM trinity), for beneficiary enrolment has been the logical next step in the rollout of financial services.



¹UIDAI portal, https://uidai.gov.in/images/StateWiseAge_AadhaarSat_24082017.pdf

²PMJDY portal, <https://www.pmjdy.gov.in/account>

³TRAI portal, http://www.trai.gov.in/sites/default/files/PR_No.37of2017_English.pdf

Aadhaar can have concrete impact in beneficiary identification and authentication; Jan Dhan accounts seeded with Aadhaar can be used for direct transfer into bank accounts, reducing the dependence on cash and related inefficiencies such as leakages; mobile technology can be used for information dissemination and as a medium to conduct transactions. With Aadhaar penetration high, Jan Dhan Aadhaar enabled PDS – (Cashless AePDS) being mobile phone agnostic, is well-placed to take advantage of this discrete identity network and target the masses. E-Wallets are gaining popularity due to the user's growing comfort with wallets. Mobile wallets are being used for a variety of purposes with JAM trinity and average transaction sizes for wallets have been on a rise. Data sources and Electronic KYC (EKYC) can do massive back end enrolment of beneficiaries, with people receiving credits directly into their wallets. Other developments in Financial Services such as Unified Payments Interface, offering ease of use by facilitating instant transfer of funds to a virtual address using smartphones; differentiated banks such as Payments Banks, many of which possess existing large customer bases; India-Stack, bringing parity among players via its open Application Programming Interface (API) policy for five key programs; and FinTech start-ups upending traditional delivery models; are all set to transform the delivery of financial services in India.

Penetrating and serving the underserved segments & businesses

With improved prospects of tapping into new the underserved/used, there is a strong business case for building the financial services architecture at the back-end, in a way that it is running seamlessly.

i. Payments eco-system heft to increase accessibility, availability, interoperability and security in payments

For building an eco-system of electronic payments by reducing paper based instruments, the Reserve Bank of India (RBI) vision 2018⁴ to develop Payments and Settlement Systems in India focuses on **“Coverage”, “Convenience”, “Confidence”, “Convergence”, and “Cost”**. To this end, strategic initiatives to be undertaken by participants in the payments industry include:

1. Responsive Regulation
2. Robust Infrastructure
3. Effective Supervision
4. Customer Centricity

These initiatives are expected to result in a decreased use of paper based instruments, increased users of mobile banking, growth in acceptance infrastructure, increased use of Aadhaar based payments, as well as growth in other modes of electronic payments.



⁴Payment and Settlement Systems in India: Vision-2018, Reserve Bank of India, June 2016 : <https://rbi.org.in/Scripts/PublicationVisionDocuments.aspx?Id=842>

1 Responsive Regulation **2 Robust Infrastructure** **3 Effective Supervision** **4 Customer Centricity**

A Regulatory framework that allows for enhanced coverage, interoperability in payments, along with convenience and security for end users. Some tenets of such a framework include:

- Framing new policies and reviewing existing policies, to orient them with new innovations.
- Setting up Payments System Advisory Council (PSAC) for industry and Government representatives to strengthen the consultative process. Recommendations of the Watal

Committee under Ratan P. Watal⁵ to promote digital payments in India, also emphasized the need for setting up a separate payments regulator and improving acceptance infrastructure in India.

- Amendments to Payment and Settlement Systems (PSS) Act, 2007, to ensure better governance.
- Strengthen Financial Stability by identifying legal entities in financial transactions and taking steps to settle transactions in central bank money, to avoid credit and liquidity risks.

1 Responsive Regulation **2 Robust Infrastructure** **3 Effective Supervision** **4 Customer Centricity**

There is an urgent need to simplify and accelerate payments penetration in India. Lack of sufficient IT infrastructure and end to end digitization is leading to challenges in driving digital payments. For greater proliferation of digital payments, the entire supply chain must be digitized. To increase accessibility, availability, interoperability and security of payments systems, RBI has recommended:

- Facilitating faster payments services. A host of options have been introduced in the market including multi device solutions, all options on one device e.g. a multi functionality POS, and a more lightweight -software based solution. While introduction of Point of sale terminal (POS), mobile point of sale terminal (mPOS), Near field communication (NFC) based, Aadhaar enabled, Mobile wallets (m-wallets), other pre-paid instruments, Immediate Payment Service (IMPS), National Electronic Funds Transfer (NEFT/EFT), Unified Payments Interface (UPI)/ Bharat Interface for Money (Bhim), Bharat QR, Bharat Bill Payments System

(BBPS), and online marketplaces, will likely induce electronic payments activity in a diverse and vast country like India where all modes are welcome, these options now need to be stabilized to create trust in the minds of participants. Payments also need to be made scale-able for mass adoption to become the norm. In response to this, mobile based payment solutions are recommended to service providers. The back end of banking systems must be adapted to accept any payment volume, allowing products to scale. More frequent settlement cycles for NEFT, is one such recommendation to help achieve this.

- Improving accessibility by way of improved acceptance infrastructure. Significant growth in acceptance infrastructure is seen as a primary outcome of RBI's vision 2018. Key lacunae in acceptance infrastructure are, it is currently skewed in favor of issuers, with the issuer banks (of POS terminals) getting majority of Merchant Discount Rate (MDR) and



⁵Committee on Digital Payments: Medium Term Recommendations to Strengthen Digital Payments Ecosystem, Ministry of Finance, GOI, December 2016 : http://mof.gov.in/reports/watal_report271216.pdf

merchant acquirers have to invest in POS terminals, aside from paying high interchange fee. As a result, banks issuing POS terminals are many. Merchant acquiring banks, on the other hand are few in numbers. Banks are still grappling with on-boarding merchants to penetrate for financial inclusion. Remedies that can bring merchants on board include, low cost options for smaller merchants, merchant training and support, using National Payments Corporation of India (NPCI) innovations such as Bharat QR (non-hardware based model). More options in the market imply the Merchant acquiring business will see intense competition

from traditional acquiring banks (as POS aggregates the multiple solutions).

- Promoting inter-operability across providers – UPI aims at allowing customers this convenience of using payment instruments across service providers. Toll collection and Mass Rapid Transit payments to be made electronic in an interoperable environment are also to be prioritized.
- Enhancing safety in payments to cement customer relationships
- Eliminating paper flow in Cheque clearing systems and complete migration to CTS-2010 Standards

1 Responsive Regulation **2 Robust Infrastructure** **3 Effective Supervision** **4 Customer Centricity**

The RBI proposes:

- Testing the resilience of the payments and settlements infrastructure including Financial Market Infrastructures (FMIs) and System Wide Important Payment Systems (SWIPS) in the country
- Designing the oversight framework for new and existing payment systems, to make the payment infrastructure more resilient
- Strengthening the reporting framework and monitoring fraud occurring in various payment systems
- Analyzing data emerging out of and publishing reports on payment systems

1 Responsive Regulation **2 Robust Infrastructure** **3 Effective Supervision** **4 Customer Centricity**

Payment options that offer customers & merchant’s convenience, build trust, are frictionless, put in place adequate customer redressal mechanisms, and create awareness and education among customers, will give the customer holistic control over their payments experience.

Some key tenets include:

- Necessary guidelines and trainings to strengthen customer grievance redressal
- Customer education and training about electronic banking, fees, terms
- Protecting consumer interest by limiting his liabilities and managing risk of fraud
- Positive confirmation messages to remitter in Real Time Gross Settlement (RTGS), similar to NEFT
- Conducting customer surveys to gauge changes in payment choices of customers



ii. Drawing lessons from a framework such as European Central Bank's (ECB's) "Payments Service Directive 2" (PSD2) for India

PSD2 requires Banks to open their data infrastructure to third parties, by adopting APIs to enable them to provide improved products and services to customers. With PSD2 the European Union (EU) has the chance to create an "EU digital single market".

ECB⁶ and European Banking Authority (EBA) worked closely to emphasize standards on strong customer authentication and secure communication to promote safety and efficiency of electronic payments in the Euro. Payments Service Directive 1 (PSD1) has been in place since November 2007 and coordinates supervisory and oversight approaches to ensure safety and focus on consumer protection and rights of service providers and users. As the market for payments underwent changes thereafter, the EU institutions proposed aligning the EU and national legislations with the increasing no. of players (smaller payment companies and FinTech companies), and activities of the payments industry. PSD2 was put in place. PSD2 is a set of new rules to protect consumers when they pay online and changes the "territorial" and "currency" scope of PSD1.

- It makes cross-border payments safer, as also increasing Pan-Europe participation in the Payments industry. For instance, it ensures consumer protection, even if the service provider is located outside the European Economic Area (EEA), or the transaction is in non EEA currencies.
- It promotes innovative online payments, mobile payments, as also increasing participation from non-banks (increased competition).

- PSD2 facilitates customer convenience and protection. It mandates strong customer authentication. Payment service providers are also required to set up incident management procedures.
- In order to provide consumers with convenient and easy-to-use services within a complex market, PSD2 aims to ensure the efficient and regulated exchange of information between players.

India is on a similar growth trajectory as the EU in electronic payments i.e. has diversity in banking practices, variance in technologies adopted across the country, and is looking at achieving Pan Indian implementation of a frictionless Payments system. With RBI's Vision 2018, PSD2 creates implications for the path that can be taken on home turf. Some takeaways for India:

- By opening up their APIs, customer information that was earlier restricted to Banks, will now be available to a wider set of industry participants (with customer consensus), encouraging greater competition, more innovation, and a greater likelihood of achieving the inclusion objective.
- By capping interchange fee, PSD2 reduces the overall cost of a card transaction, gives a boost to digital transactions, and reduces dependence on cash.
- Seeing a consolidated customer bank portfolio (across various banks), in one screen, application of analytics to real time data monitoring allows improved advice under PSD2.

⁶The ECB cooperates with the EBA to improve the security of electronic payments in Europe, European Central Bank, February 2017: https://www.ecb.europa.eu/paym/pol/shared/pdf/20170223_ECBcoopEBAimprsecelpaym.pdf

iii. Ensuring security of sensitive data leveraged for Digital Financial Services (DFS), while also facilitating its use

Engagement models of the future are riding on the back of huge amounts of emerging Data, as we move rapidly to digitization. Although data is a competitive resource (access to data will lead to more products, opportunities to cross-sell to better drive customer engagement, greater competition, lower cost innovations) and has a lot of scope, data breaches are on the rise. These breaches will likely grow as sophisticated threat vectors emerge and attack severity

increases. Ensuring data security and protecting consumer interests is critical for keeping in-tact reputational risk of service providers, while also mining new revenue streams. There is an urgent need for security protocols to minimize breaches. We need to raise the bar on security methods by increasing our defenses and reducing attacks. Companies that are generating insights using data, while have the promise of efficiencies, their success will depend on their ability to offer/leverage solutions which can encrypt and secure data.

Some important considerations towards ensuring data security are:



Evolving Infrastructure

Security infrastructure needs to keep evolving, as the focus on threat prevention increases



Analytics for fraud detection

DFS will have potential for misuse, but analytics can be leveraged to avoid frauds



Customer Awareness

A part of ensuring security is creating awareness among users



Data-Ownership

Customer expectations on defining ownership of data are evolving



Cost of Security

Data Security isn't free and needs to be factored into the cost of a digital transaction. Digital audits and forensics must claim a larger share of digital spend and become a CFO level agenda

iv. If DFS needs to grow exponentially, its pricing needs to be appropriate

The Government's vision of a Digital India entails DFS be made available to all. If DFS is to become mainstream, we cannot ignore the ever-present "pricing" question. Pricing DFS needs to be correct to drive uptake, spurring the need for the right pricing models. India, by virtue of its price-sensitive character, calls for

customization of products and prices, else it risks low accessibility of DFS. The product mix selected by customers will largely be impacted by pricing. For instance, due to the costs associated with card based payments, a push toward mobile phone based payments was done on the back of IMPS.

Amidst these developments, can growth be inclusive and percolate to the lowest segments?

Few illustrative digital applications across the spectrum



Improved prospects for Credit Decisioning

Traditional lending methods are unable to serve people with limited credit data i.e. credit score/history, especially underbanked individuals. Low penetration of retail and Micro-Small and Medium Enterprises (MSME) credit is causing a huge credit gap in the MSME segment. This lacunae is being looked at as an opportunity by new-age lenders, given the applications of vast amounts of emerging data and the exponential benefits in analyzing it in a digital environment. Customer insights are paving the way for “data driven” revenue models, in the face of unsustainable “transaction-only” revenue models. Data helps tapping into customer behaviors. By drawing out unique patterns from micro data, adding data-points (service providers are also linking customer

data across ecosystem partners), and the application of technologies, lenders can increase the quality of the loan being disbursed, and reduce costs of disbursing these loans (efficient customer acquisition, approval, servicing). Alternate lenders, including Person to Person (P2P) platforms, credit scoring platforms, and marketplace platforms are being able to address credit needs of underserved segments by harvesting rich customer data, using analytics to detect key patterns from these data sources, building credit profiles of customers in minutes and, providing actionable credit decisioning. By making more accurate risk predictions based on data and technologies, loan approvals are likely to be quick, in real-time, and at a fraction of the current costs.





Direct Benefit Transfers (DBT)

Cashless payment in DBT is likely to:

1

Incentivize merchants to deliver better quality of goods sold in the open market, at market prices

4

Beneficiaries have a wider choice of goods and unused amounts can be carried over

2

The right amount of entitlement that is to be credited to a beneficiary can be identified

5

Leakages in the transfer of subsidies are eliminated (due to end to end digitization of the supply chain)

3

Subsidies that were earlier being transferred to the same beneficiary repeatedly, will now be transferred only once

6

Beneficiaries can avoid the hassle of physically withdrawing cash, the subsidy amounts will be used for the intended purpose only



Payment Banks (PBs)

Due to their dependence on, and need to generate “transaction based income”, PBs are being forced to come up with innovative methods to be inclusive, e.g. focus on biometric authentication to bring down the cost of customer

acquisition, forge partnerships with Banks, FinTech companies to expand product offerings, and use Aadhaar for payments (using a smartphone with in-built biometric scanner).

Conclusive Remarks

An interoperable platform by way of JAM trinity, other developments such as UPI, use of analytics in lending have been adequately leveraged by providers of financial services, for greater proliferation. Upcoming releases of products and services by service providers will be largely keeping with

customer demands. Market participants that focus on data security and invest in improved infrastructure are likely to dominate the agenda. PSD2 has some key takeaways in the Indian context and to that end, the regulator is an important catalyst driving change, and in taking financial services to the lowest segments.

Digital disruption: Trends, exponential technologies and challenges

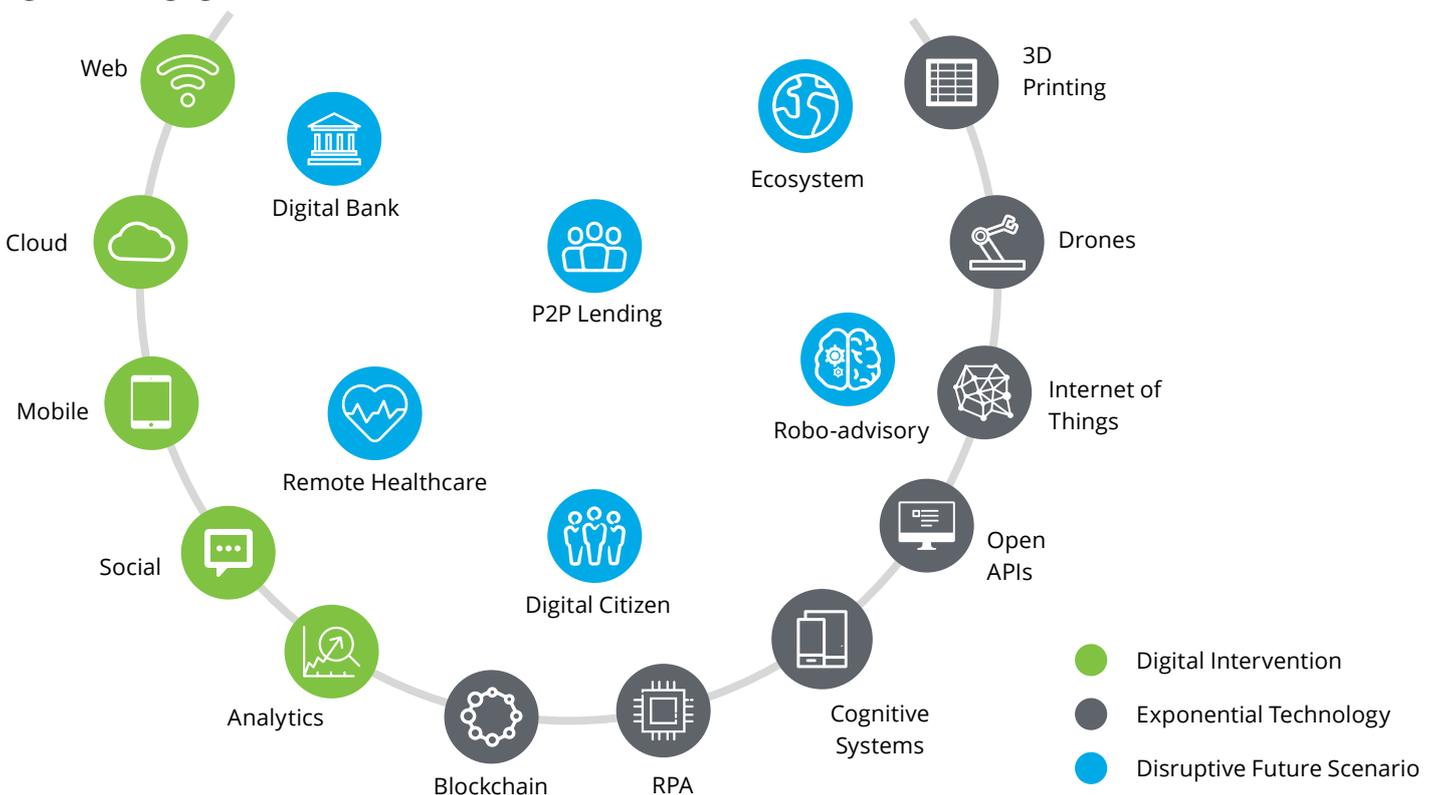
Introduction

We are in the era of digital disruption wherein constant change is the new normal. Adapting to increasingly digital market environments and taking advantage of digital technologies to improve business are important goals for nearly every contemporary business. The rate of technology change and its convergence is accelerating exponentially, thereby making it difficult for executives to understand its implications to their industry and organizations. The digital interventions of social, mobile, analytics, big data and cloud technologies are laying the foundation for any transformation today. When these are

combined with exponential technologies like robotics, cognitive computing, internet of things, blockchain, drones, 3D printing and autonomous vehicles, the impact is profound. This will lead to emergence of multiple disruptive scenarios adding pressure on business leaders to understand their implications and respond quickly. Some of these future scenarios include digital banks, P2P lending, remote healthcare, robo-advisory, digital citizen and many more as illustrated in Figure 1:

Digital disruption and exponential technologies are blurring the lines from an industry perspective, with leading practices and learnings from one industry being applied to other industries. In India, the financial sector has been at the fore front of leading the way in terms of digital adoption, however, other sectors like healthcare, manufacturing and government are catching up fast. In this chapter we will explore how organisations are reinventing themselves through innovative business models, achieving growth & profitability, and bringing in efficiencies in their operations, by tapping into some of these exponential technologies.

Figure 1: Emerging Future Scenario



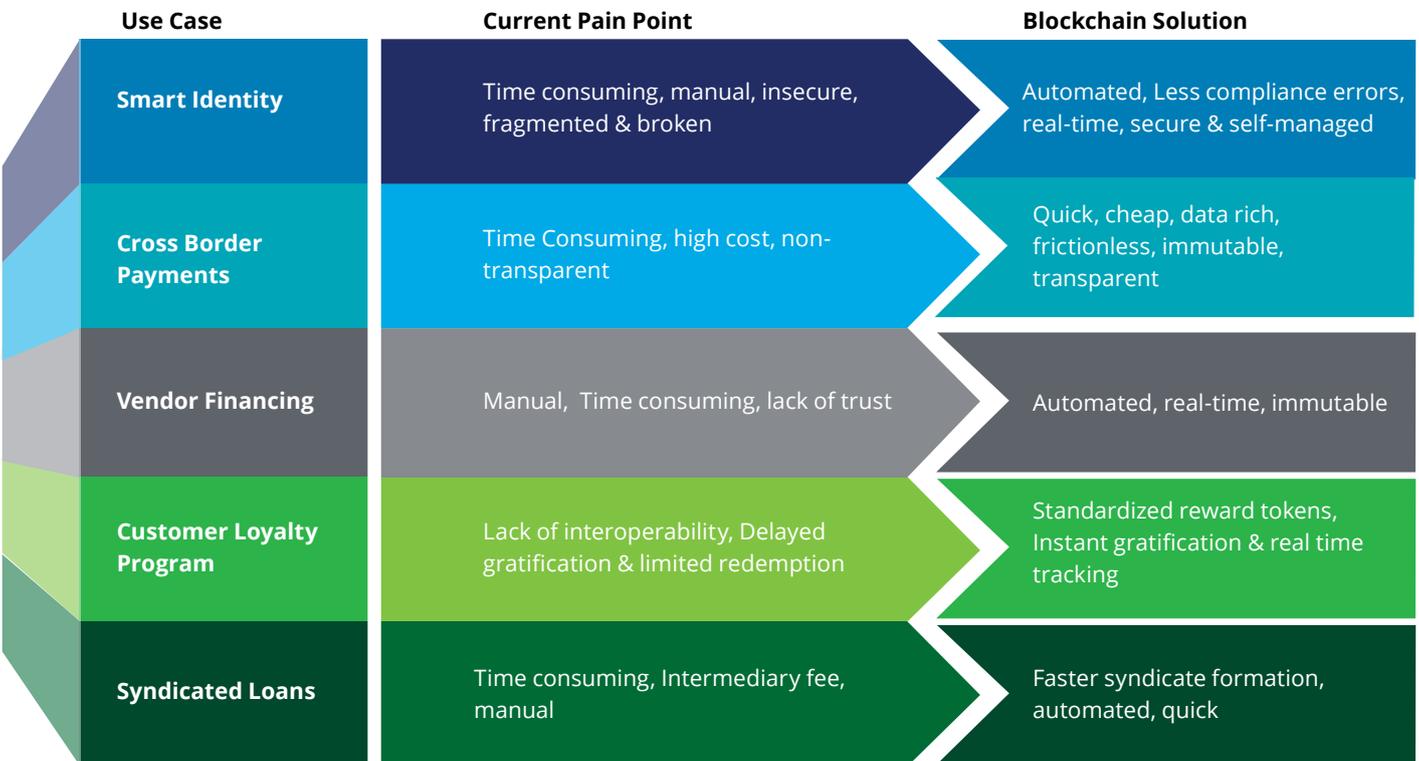
Blockchain

Blockchain is being widely debated and has become the new buzz word for multiple industries, especially banking. Banks across the country have successfully initiated collaboration with specialized firms (FinTech) and/or consulting firms, to build proof-of-concepts and explore various potential use-cases. This implies how seriously banks are considering blockchain technology and how eager they are to understand the ways this technology can help reinvent business models or address some of their pain points.

In the recent past, aggregators like Uber and AirBnB have disrupted mainstream businesses by redefining business models. Blockchain has a potential to disrupt these disruptors since it removes the need of intermediaries in doing business.

Banks are continuously exploring new ways to perform transactions faster, for enhanced customer service, while ensuring cost efficiency in their operations, and assuring transparency to their customers and the regulators. For this, blockchain potentially provides a solution for banks as it inherently helps eliminate intermediaries, maintains an immutable log of transactions, and also facilitates real-time execution of transactions. This could potentially optimise the TAT for banking transactions, reduce costs of manual work, and enhance customer experience. Like any other industry, choosing the right 'use case' is the key for banks to leverage the full value of blockchain.

Figure 2: Potential use cases for blockchain⁷



⁷<https://www2.deloitte.com/in/en/pages/strategy/articles/blockchain-in-banking.html>

A leading private sector bank in India has implemented a multi-nodal blockchain transaction to fully digitize vendor financing for a consumer electrical equipment manufacturing company. The implementation has been done on a blockchain-based smart contract written by a FinTech start-up. The solution also leverages IBM Watson Conversation, a cloud-based cognitive service, to enhance the digital experience of partners, corporate clients and developers.

Kotak Mahindra Bank has partnered with Deloitte to enable end to end trade financing for one of its clients by utilizing blockchain technology, thereby reducing the time taken for a letter of credit (LC) to few hours from 20 to 30 days. It not only eliminates data duplication, but also integrates data to a central cloud-based access system for participants in a transaction.

Though blockchain is a powerful solution, it is still in its exploratory stage and comes with its own set of challenges which include:

1. Non – clarity around regulatory status:

Few of the blockchain use cases involve usage of cryptocurrency. Such transactions require changes in regulations from government bodies like RBI. While regulators are required to drive adoption of blockchain, they also need to be part of a blockchain network to get visibility from a regulatory compliance perspective. Hong Kong Securities and Futures Commission is working with member banks and technology providers to test online ledgers to record and settle securities and futures transactions.

2. Integration procedure and change adoption: Blockchain applications offer solutions that require significant overhaul of existing systems. In order to make the switch, companies must strategize the transition.
3. Cost: Blockchain offers tremendous savings in transaction costs and time, but the initial cost of investment in the technology might be high.

Though the potential of blockchain is widely claimed to be at par with early commercial Internet, it is important that firms understand the key features of the technology and how it can solve current business issues. Companies need to identify opportunities, determine feasibility and impact, and test proof of concepts. This will involve answering a series of fundamental questions related to the dynamics of transactions and regulations underlying the transaction. Lastly, due to lack of any precedence, firms will have to opt for a trial-and-error approach, either through internal trials or partnering with a specialized firm.

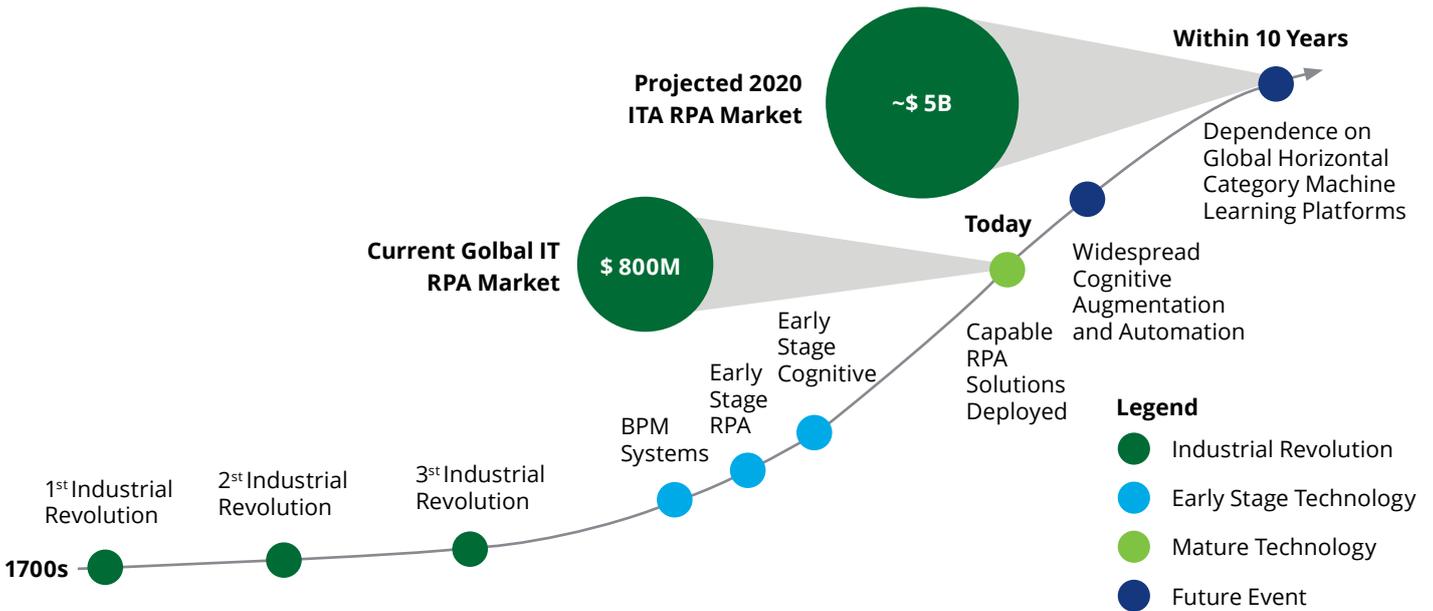


Robotic Process Automation (RPA)

According to World Economic Forum report titled Future of Jobs, more than 5 mn jobs will be lost to Automation, Robotics and Artificial Intelligence by

2020 across the globe, and 2/3rd of these will be in the office and administrative sectors. The global RPA market is expected to experience a 60% CAGR through 2020⁸.

Figure 3: Robotic Process Automation market evolution⁹



RPA tools evolved quietly over the last decade, but have now reached a level of maturity where process automation is possible at a significant scale. In most organizations, there are many routine processes performed manually that lack the scale or value to warrant automation via IT Transformation, but for which macros and other such desktop automation tools are too limited to effectively address the issues. RPA can fill this gap by reducing the 'minimum viable scale' of process automation as compared to its traditional counterparts.

Organizations using RPA solutions typically achieve operational efficiencies, improved quality, cost reduction, decreased cycle times and improved throughput. Automated processes provide flexibility to change quickly, ability to scale-up exponentially and produce valuable audit trails for

regulatory compliances¹⁰. With improved accuracy, operations can now be carried out round the clock. It results in improved employee morale as employees are freed from mundane jobs and redeployed for value creation.

Digitization of white collar jobs via robotic and cognitive automation, and advances in data science have sparked a mini revolution of sorts. RPA when applied at the right scale, can be truly transformative for organizations however it is important to identify the right candidates for automation, clearly define the success criteria and build a business case with expected ROI articulated. It is important to drill down to various attributes while identifying a process for automation and analyse them from ease of implementation vs. benefits point of view.

⁸<http://www.transparencymarketresearch.com/pressrelease/it-robotic-automation-industry.htm>

⁹https://www.km.deloitteresources.com/sites/live/crossfunctional/_layouts/DTTS.DR.KAMDocumentForms/KAMDisplay.aspx?List=26eeb191-7a3b-4609-9f91-b8fa5fc169f0&ID=844856

¹⁰<https://www2.deloitte.com/in/en/pages/finance-transformation/articles/robotics-cognitive-influencing-finance.html>

A leading private bank in India implemented RPA across 200 processes across the organization, including Retail Banking Operations, Agri-Business, Trade & Forex, Treasury and Human Resources Management, among others. Today, robots are processing over 10 lakh transactions daily, bringing in unparalleled operational efficiency, higher accuracy, and a massive reduction in processing time for customer services¹¹.

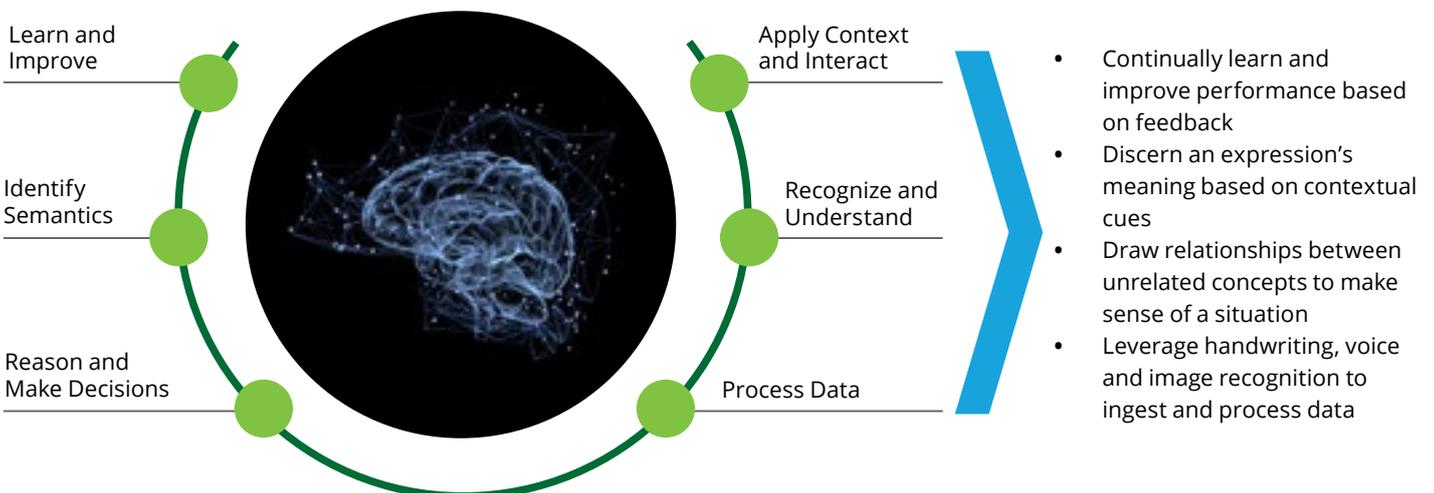
Another large bank deployed a full Robotics Process Automation (RPA) implementation using 100 robots running 18 processes to handle more than 85,000 requests each week. The output capacity delivered by the robots was equivalent to roughly 230 Full-time equivalents (FTE) delivered at 30% of the cost of recruiting more staff. Additionally, two of the top five quality fails were eliminated following the introduction of robots.

Cognitive Computing

Today, cognitive technologies working alongside the existing ERP systems and robotics can upend operational finance and bring about unprecedented speed, agility, and transparency to processes. Examples of cognitive technologies include computer vision, machine learning, natural language processing, speech recognition, and robotics. This technology provides significant advantages such as cognitive automation, cognitive insights and cognitive engagement.

Cognitive Computing is “a self-learning system that uses data mining, pattern recognition, and natural language processing to mimic the way the human brain works. The goal of cognitive computing is to create automated IT systems that are capable of solving problems without requiring human assistance”¹².

Figure 4 : Cognitive Systems mimic and learn like humans



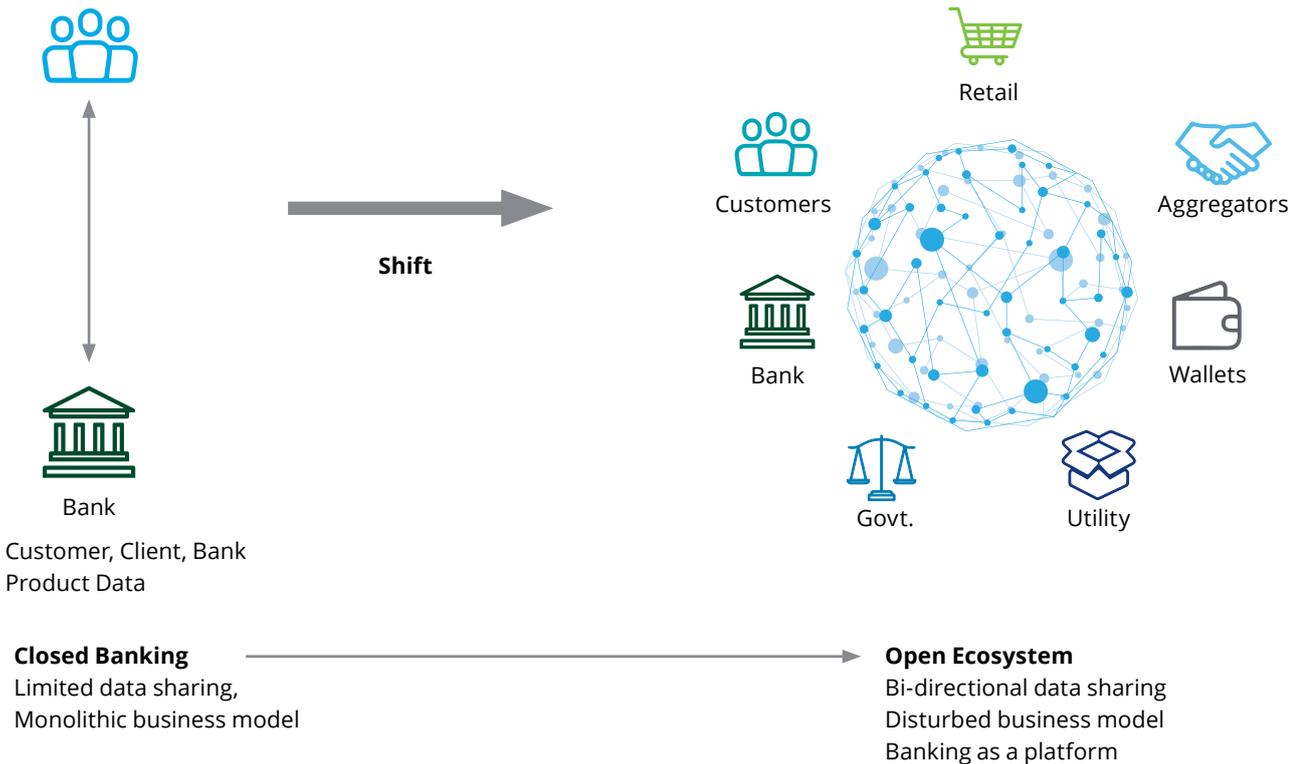
¹¹<https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance-transformation/in-ft-crunch-time-future-of-finance-in-digital-world-noexp.pdf>

¹²<https://www.ibm.com/think/marketing/things-you-can-do-with-cognitive-computing-right-now/>

In a quest to create this ecosystem, banking platforms are evolving from a closed to open banking model which involved shared use of bank products,

services, functions and data with 3rd parties to add additional value and create new business models.

Figure 5: Evolution on Open Banking



This ecosystem will allow customers to make personalised comparisons between accounts at different providers. This will help them choose which account would be best for them. It will also allow banks to provide better offers on products. Opening up this data to third parties would clearly level the playing field. Moreover, armed with customer banking data, both banks and third parties could ultimately offer new propositions such as money-management and budgeting tools. Open banking, therefore, could lead to customers performing all their banking activities at different banks, using a third-party application that

provide data-enabled tools to help them manage and optimise their finances.

Open APIs give banks in India an opportunity to increase their geographical boundaries, create value added services and monetize their business assets by partnering with FinTech companies, NBFCs, payment banks and retailers. In November 2016, Citibank launched an API developer hub, which expanded developer access to APIs across several categories. Wells Fargo also expanded access to APIs, but it is invitation-only at this point in time.

The BHIM app. also leverages this API ecosystem wherein it is a one stop shop for all the UPI based payments. If one has signed up for UPI-based payments on their bank account, which is also linked to the mobile phone number, the BHIM app. can be used to carry out digital transactions.

Data privacy regulations have been quite stringent in some of the countries and factoring them in APIs becomes quite challenging. In India, “right to privacy” is becoming a prominent ask by citizens and the government is taking a serious look at it. The regulation and laws around data privacy are still evolving, and hence the API frameworks need to be designed in such a way that they keep pace with changes without compromising on flexibility and agility.

By providing their APIs to third parties, banks are exposed to a greater risk of cyberattacks and can no longer hide their critical applications behind firewalls. On the other hand, banks will have difficulty in maintaining their own strict security requirements. Banks will still be responsible for customer data ownership which makes them liable for third party failures as well.

Although, open APIs give a plethora of opportunities to banks to change their value propositions, banks will need to use customer data in innovative and more individually tailored propositions. Adapting to a digital marketplace also requires more than simply upgrading IT architectures and embracing new technologies. To succeed, banks will need to reshape their organisational structures and cultures to a significant extent. Innovation will need to be placed at the very heart of the business, and be encouraged at all levels of the organisation. In addition to addressing these issues, banks will also face the cultural challenge of working within an ecosystem with FinTech companies and other tech-enabled firms.

Think Big, Start Small and Scale Fast

It is highly challenging to keep up with the changes wrought by exponential technologies. Some of these technologies might seem like a buzz word at the moment, however, they are here to stay and it is a matter of time before they become part of the mainstream. Organisations that have adapted the digital and exponential technologies are rapidly disrupting the traditional businesses. The key characteristics that set these organisations and business leaders apart are:

- Ability to create value through ecosystem, network, and platform based business models
- By being multi-modal i.e. ability to manage different velocities of change within your organization
- Inculcating a culture of innovation imbuing the principles of fail-fast and learn-fast

By embracing exponential and digital technologies, organization will not only achieve growth, operational efficiencies and customer centricity, but also stay ahead of the competition. This is the right time for business leaders and organisation to identify opportunities and invest in innovation that can benefit from the exponential technologies.







Evolving Role of Regulator in Digital India

Introduction

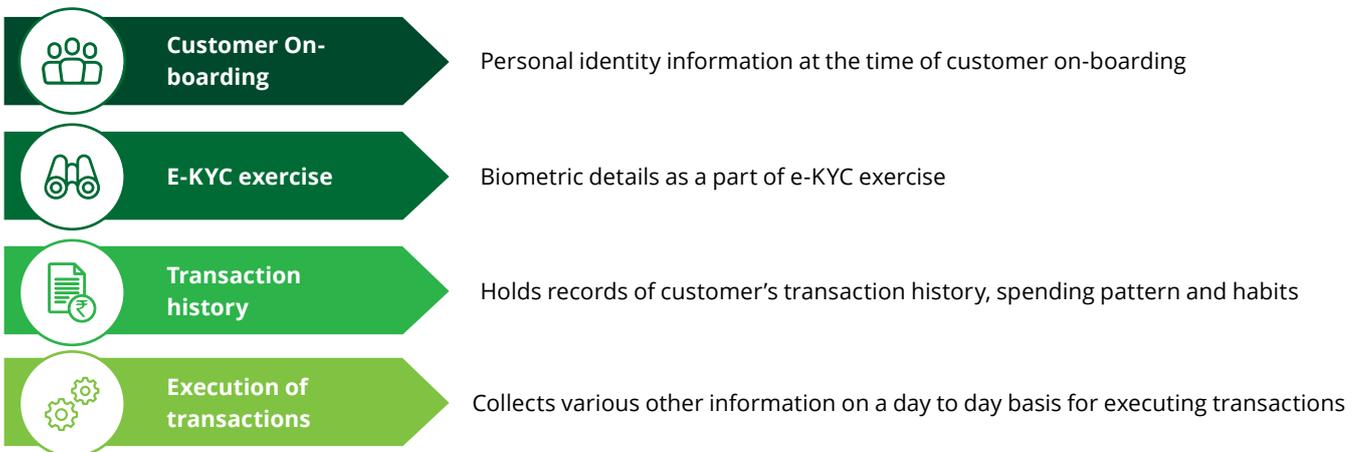
The Banking and Financial Services Industry (BFSI) has been witnessing vast disruptions, as detailed in the previous section. Emerging technologies such as Blockchain, Robotic Process Automation, Cognitive Computing, Cloud based Technologies, Biometric etc., have increased cyber security risks across the banking industry.

Further, the emergence of FinTech entities, including prepaid instrument

providers, Payment Solution providers, Digital Lending companies, Account Aggregators, Data Analytics solution providers, Social Network based payment service providers, Telecom companies providing integrated payment solutions etc., has seen a wide spread increase in the recent past.

These entities today collect significant amount of customer's personal sensitive data at various stages, as mentioned below:

Various stages for collecting customers personal data



Accordingly, it is imperative for the financial institutions to ensure protection of customer's personal data and use it as per the customer's consent. The entities also need to ensure adherence to extant laws and regulations issued by the Government and the Banking Regulator, Reserve Bank of India.

While the financial services space has a larger impact considering the sensitiveness of customer data that is collected, in the current scenario, industries such as telecom, healthcare, social networking etc., also collect /

have possession of customer's personal data. Similarly, various Government and quasi Government agencies also collect personal data for the purpose of various social welfare schemes. Accordingly, it is critical for these entities as well, to ensure the protection of sensitive customer data.

Current Statutory and Regulatory Environment on Data Governance in BFSI

Statutory Laws enacted by the Government of India

While there is no separate act currently on Data Privacy and Data Protection, India

has enacted the Information Technology Act, 2000 under which the rules on "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011" have been issued¹⁶. The provision requires a body corporate who 'receives, possesses, stores, deals, or handles' any 'sensitive personal data' to implement and maintain 'reasonable security practices', failing which they are held liable to compensate those affected.

Majorly, the rules require that the body corporates collecting sensitive personal

¹⁶Website of Ministry of Electronics and Information Technology, <http://meity.gov.in/cyber-security>

information of customers shall disclose to their customers, that information is being collected and for what purpose the same will be used. Obtaining consent of the provider of information is a critical requirement of the rules. Further it also requires that the body corporates must implement reasonable security practices to ensure protection of data collected from their customers.

Regulations issued by the Reserve Bank of India

RBI had, in 2011, formed a working group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, and based on the recommendations of the committee, has issued guidelines on nine broad areas across IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal aspects.¹⁷

The guidelines require that each Bank shall have a Board approved information security policy. Among other things, they require that Banks shall classify the information based on their sensitivity and criticality, and accordingly implement appropriate security measures to ensure protection of such information.

Further, RBI has also issued guidelines on the Cyber Security Framework in Banks in 2016, which emphasises on a Board Approved Cyber Security Policy and Cyber Crisis Management Plan covering Detection, Response, Recovery and Containment.¹⁸

RBI has also issued guidelines to Non Banking Finance Companies (NBFC) on the Information Technology and Information Security Framework.

Currently, there are no defined guidelines issued by the RBI to FinTech Entities such as payment service providers, prepaid

instrument service providers on Data Protection, Information Security or the Cyber Security framework.

Recent Steps by the Government / Regulators

Government of India, has on 31 July 2017, constituted a Committee to deliberate on the data protection framework for India and submit a report on the same by 30 September 2017. The committee shall look at aspects such as data sovereignty, data retention, and responsibilities of the Government, companies as well as individuals while handling third party data. The Committee shall make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India, and suggest a draft data protection bill.¹⁹

Further, under the provisions of Information Technology Act 2000, the Government has also issued draft rules for the Security of Prepaid Payment Instruments in March 2017, which emphasise on the following key aspects:²⁰

- Protection of personal information
- Contractual arrangements to ensure that merchants handling any authentication data have security measures in place to protect personal information.
- Customer identification and authentication, both at the time of issue of Prepaid Instrument (PPI), and at the time PPI is accessed by customer, or when a payment is initiated.

The Government of India plans to enact a separate law on Data Protection and Data Privacy by the end of 2017, which is expected to create a robust legal framework.

While the Reserve Bank of India, has issued guidelines on information security and cyber security for Banks, such a regulation is not available currently for other FinTech entities. However, the RBI



¹⁷<https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=6366&Mode=0>

¹⁸<https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10435&Mode=0>

¹⁹http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf

²⁰<http://meity.gov.in/draft-rules-security-prepaid-payment-instruments-under-provisions-it-act-2000>

has recently issued draft guidelines for prepaid instrument service providers, which among other things, seek to address the following:

- Adequate information and data security infrastructure
- Security operations centre
- Vendor risk management
- Data loss prevention

Comparative Regulatory Environment in other Geographies

European Union

EU superseded the Data Protection Directive with the General Data Protection Regulation (GDPR) in 2016 and the same Regulation will be enforceable from 2018. The Regulation will be applied to all 28 of the European Union members. Data processors will be held under the law which would include individuals, as well as companies processing bulky data.²¹

In common with the rest of the European Union, the United Kingdom will adopt the General Data Protection Regulation (GDPR) from May 2018. When the United Kingdom leaves the European Union, it will be free to adopt its own data protection laws.

In Germany, the main legal source of data protection is the Federal Data Protection Act (BDSG). Additionally, each German state has a data protection law of its own. In principle, the data protection acts of the individual states intend to protect personal data from processing and use by public authorities of the states, whereas the BDSG intends to protect personal data from processing and use by federal public authorities and private bodies.²²

United States

The United States has about 20 sector specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50

states and territories. California alone has more than 25 state privacy and data security laws.

In addition, the large range of companies regulated by the Federal Trade Commission (FTC) are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data.²³

Asia

Japan introduced a separate central legislation for protection of data as the Act on the Protection of Personal Information (APPI).²⁴ The Act took partial effect in 2016 and has been enforceable from May 30, 2017. The law defines the scope of the legislation and states on whom the law is applicable under Article 2-4 of the APPI. As per the Act, it is applicable to four entities - state institutions, local public bodies, independent administrative agencies, and an entity not having over 5,000 individuals' personal information for more than six months. Similar to the EU law, consent of a data subject forms the essence of the legislation, and has been stated as mandatory in case of transmitting data to a third party, or for any use beyond communication purposes.

China has recently passed a Cyber Security Law in November 2016, which will come into force from June 2017. The new law, introduces a range of new rules relating to networks and online activities in the People's Republic of China, including enhanced data protection/ security obligations.²⁵

Singapore enacted the Personal Data Protection Act 2012 on 15 October 2012. The Act has extraterritorial

²¹<http://www.eugdpr.org/>

²²https://www.gesetze-im-internet.de/englisch_bdsgr/

²³<https://www.ftc.gov/>

²⁴<https://www.ppc.go.jp/en/>

²⁵<http://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>



effect and so applies to organisations collecting personal data from individuals in Singapore, whether or not the organisation itself has a presence in Singapore. The data protection obligations under the Act do not apply to the public sector, as separate rules apply to the public sector.

An analysis of the above indicates that many countries have recently updated / enacted laws on data protection and data privacy and the emphasis seems to be on obtaining consent of the customer on collection and utilization of sensitive data, and establishing a reasonable security framework to ensure protection of such data collected from customers.

Conclusive Remarks

Recent amendments to the Information Technology Act 2000, formation of a committee by the government of India to deliberate on data protection framework, RBI's guidelines on cyber security framework for Banks are steps in the right direction to enhance the legal / regulatory framework on Data Protection.

Hon'ble Supreme Court of India has on 24 Aug 2017, held that right to privacy is a Fundamental Right and it is protected under Article 21 of the Constitution of India. This judgment is expected to have a significant impact on the proposed legal framework on Data Privacy and Data Protection.

Next steps may include enactment of laws on Data Protection, covering the entire landscape of Government Agencies, Banks and Financial Service Providers, FinTech Entities, Telecom, Healthcare, Social Networking and Communication Applications, integrated with Payment Services, among others.

The following may be the next steps in the right direction, to enhance the data protection framework:

- Enhancing the regulatory framework on cyber security and data protection for Payment Service Providers as envisaged under the draft regulations issued

- Regulatory framework on cyber security and data protection at par for Banks, NBFC's and other FinTech Entities

While enactment of laws and regulations would be the way forward, the success or failure of such implementation may depend on the following aspects:

- India, being a country with a large population, is one of the most diverse countries across socio – cultural factors, and in its demography. Accordingly, any central law should consider the impact of such diversity on successful implementation.
- The central government and various state governments / their agencies have been collecting personal data of citizens on various occasions for multiple purposes, either for social welfare schemes (pension schemes, subsidies, scholarships etc.), or for creating databases for various purposes (voter database, income tax permanent account number, Aadhaar database etc.,). Therefore any legal framework that will be created should address the potential risks emanating from such welfare programmes and protecting the personal information of citizens.
- Usage of internet and digital based payments has witnessed a wide spread increase recently due to the penetration of mobile networks into rural India and the encouragement provided by the government / Banks for increased usage of digital payments. Hence, creating awareness among the citizens, particularly in rural India, on the risks of sharing sensitive personal data and making them aware of their rights pertaining to protection of data shared, will be the key to the successful implementation of any legal framework.

Glossary

AePDS	Aadhaar enabled PDS
APPI	Act on Protection of Personal Information
API	Application Programming Interface
BDSG	Bundesdatenschutzgesetz (Federal Data Protection Act, Germany)
BPPS	Bharat Bill Payments System
BFSI	Banking and Financial Services Industry
BHIM	Bharat Interface for Money
B2B	Business to Business
CFO	Chief Financial Officer
CAGR	Compound Annual Growth Rate
DFS	Digital Financial Services
DBT	Direct Benefit Transfers
EKYC	Electronic KYC
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EU	European Union
FMI	Financial Market Infrastructures
FTC	Federal Trade Commission
FTE	Full Time Equivalents
GDPR	General Data Protection Regulation
IMPS	Immediate Payment Service
IS	Information Security
IT	Information Technology
JAM Trinity	Jan Dhan, Aadhaar and Mobile
KYC	Know Your Customer
LC	Letter of Credit
M-Wallets	Mobile wallets
MDR	Merchant Discount Rate
MSME	Micro-Small and Medium Enterprises
M-Wallets	Mobile Wallets

MPOS	Mobile Point of sale terminal
NBFC	Non-Banking Finance Company
NEFT	National Electronic Funds Transfer
NLG	Natural Language Generation
NLP	Natural Language Processing
NPCI	National Payments Corporation of India
NFC	Near Field Communication
NBFC	Non-Banking Finance Company
PSS	Payment and Settlement Systems
PBs	Payment Banks
PSD1	Payments Service Directive 1
PSD2	Payments Service Directive 2
PSAC	Payments System Advisory Council
PRC	People’s Republic of China
P2P	Person to Person
POS	Point of sale terminal
PMJDY	Pradhan Mantri Jan-Dhan Yojana
PPI	Pre-Paid instruments
RTGS	Real Time Gross Settlement
RBI	Reserve Bank of India
RPA	Robotic Process Automation
SWIPS	System Wide Important Payment Systems
TAT	Turn Around Time
UPI	Unified Payments Interface

Additional References

1. <https://www.automationanywhere.com>
2. <https://www.uipath.com/automate/robotic-process-automation>
3. <https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/manufacturing/ch-en-manufacturing-industry-4-0-24102014.pdf>
4. <https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-16/cognitive-technologies-business-applications.html>
5. <https://www2.deloitte.com/in/en/pages/strategy/articles/future-of-banking.html>
6. <https://www2.deloitte.com/us/en/pages/deloitte-analytics/solutions/cognitive-analytics.html>
7. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-sdt-process-automation.pdf>



Acknowledgements

Kalpesh J. Mehta

Monish Shah

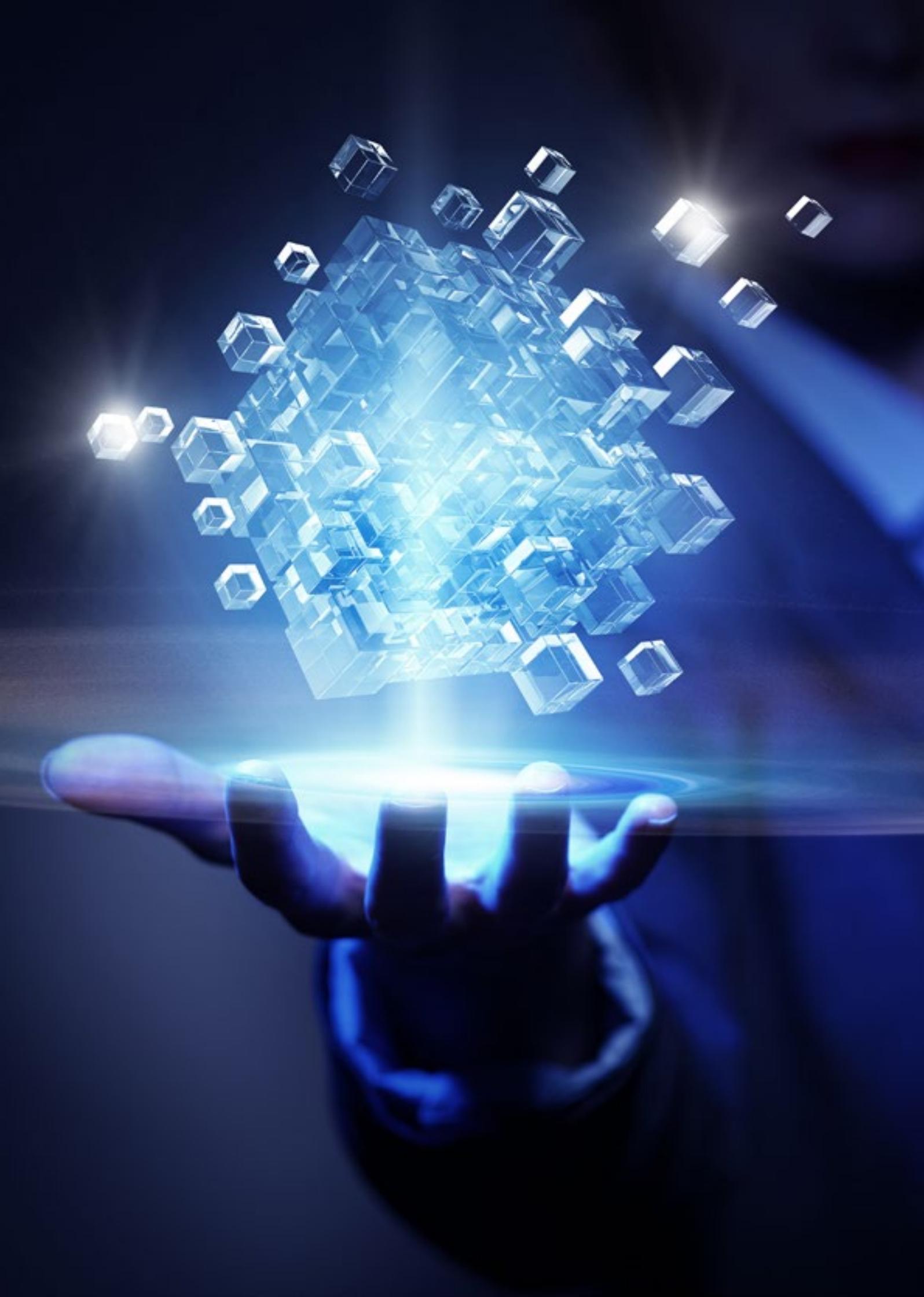
Ashvin Vellody

Himanish Chaudhuri

We would also like to acknowledge the contribution of
Bhaskar Tondale, Mayank Rausaria, Rabani Gupta, Rami Reddy

Deloitte Touche Tohmatsu India LLP
For further information you may write to us at :
infsinetwork@deloitte.com









Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.