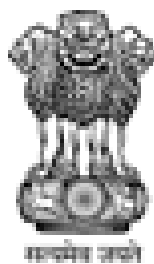


23rd National Conference on e-Governance

7th & 8th February 2020, Mumbai (Maharashtra)

Organizers



**Department of Administrative Reforms & Public Grievances
Ministry of Personnel, Public Grievances & Pensions
Government of India**

**Ministry of Electronics and Information Technology
Government of India**

Knowledge Partner

NASSCOM®

Contents

A. Digital Payments & Fintech

**B. BlockChain for effective Governance &
Service Delivery in Public Sector**

**C. Building Digital Trust - Transparency,
Security and Privacy**

23rd National Conference on eGovernance

White Paper

on

Digital Payments & Fintech

Developed by



Authors:

C.N Raghupathi

Monisha Borthakur

Sridhar Bhagawan Bukkarayasamudram

Sandeep Kumar

Contents

1. BRIEF SITUATION ASSESSMENT.....	5
2. RISE OF DIGITAL PAYMENTS & FINTECH INVESTMENTS AT GLOBAL LEVEL.....	6
2.1 COMMON INDUSTRY TRENDS AT GLOBAL LEVEL THAT DRIVE FINTECH DISRUPTION IN PAYMENTS MARKET.....	6
2.2 CONSUMER FINTECH ADOPTION RATE BY SERVICE CATEGORY	6
2.3 SYNERGIES BETWEEN PLAYERS – FINTECH AS A DISRUPTOR.....	7
3. DIGITAL PAYMENTS & FINTECH INVESTMENTS –TRENDSETTERS IN INDIA.....	8
3.1 AADHAAR ENABLED PAYMENT SYSTEM	8
3.2 INTEROPERABLE BILL PAYMENT APPLICATION – BHARAT BILLPAY (BBP).....	8
3.3 UNIFIED PAYMENTS INTERFACE (UPI) –BHIM APP	8
3.4 PAYTM.....	8
3.5 PRADHAN MANTRI JAN DHAN YOJANA.....	8
3.6 START-UP INITIATIVES FOR FINTECHS IN INDIA.....	8
4. SHARED BENEFITS AND VALUE CHAIN CREATED BY FINTECH	9
4.1 FINTECHS IN PAYMENT VALUE CHAIN.....	9
5. NEED OF THE HOUR – INNOVATIONS IN DIGITAL PAYMENTS & FINTECH.....	10
5.1 INNOVATIONS IN DIGITAL PAYMENT & FINTECH	10
5.2 LEADING FINTECH INNOVATORS IN INDIA	11
6. FINTECH GROWTH IN INDIA – KEY OPPORTUNITIES	13
6.1 UNMET FINANCIAL NEEDS	13
6.2 INCREASING INVESTMENTS IN FINTECH	13
6.3 AVAILABILITY OF POLICY FRAMEWORK.....	13
6.4 PENETRATION OF SMARTPHONES/ BROADBAND.....	13
7. OUR RECOMMENDATIONS.....	14
7.1 NEXT GENERATION BANKING MODEL – DIGITAL TRANSFORMATION ACROSS EACH STEP	14
7.2 REAL TIME DECISIONS TO SOLVE INDUSTRY PROBLEM USING BIG DATA.....	14
7.3 DESIGN ACCELERATOR PROGRAM.....	14
7.4 COLLABORATIVE APPROACH	14
7.5 SECURITY ARCHITECTURE	14

1. Brief Situation Assessment

In today's era, the advances in digital technology is seen to be one of the major disruptors, which has provided a level playing field for developing countries like India to stand up and compete with economic superpowers across the world. Such advances have led to an extraordinary boom in information access and infrastructure, communications and e-commerce. Recognizing 'e-Development' as the engine of Development, 'Digital India' movement was launched in India in 2015, which stands as a powerful enabler to meet the developmental goals of our country to create new economic and social networks. It allows entire ecosystem to become multifunctional and flexible for tailored solutions to meet diverse needs of the people. **Digital Payments** is one such example - which makes possible for users to acquire services directly from the original provider, reducing the need for intermediaries. As per the first Global Findex Report released by the World Bank in 2011, only 40% of adult Indians had a bank account. This has increased to 80% of adult Indians who have bank accounts, according to the Global Findex Report published in April 2018.¹ This has largely been an outcome of the unprecedented effort made by the government to sensitize the common man by rolling out a host of schemes², which has resulted into this size of growth as shown in Figure 1.

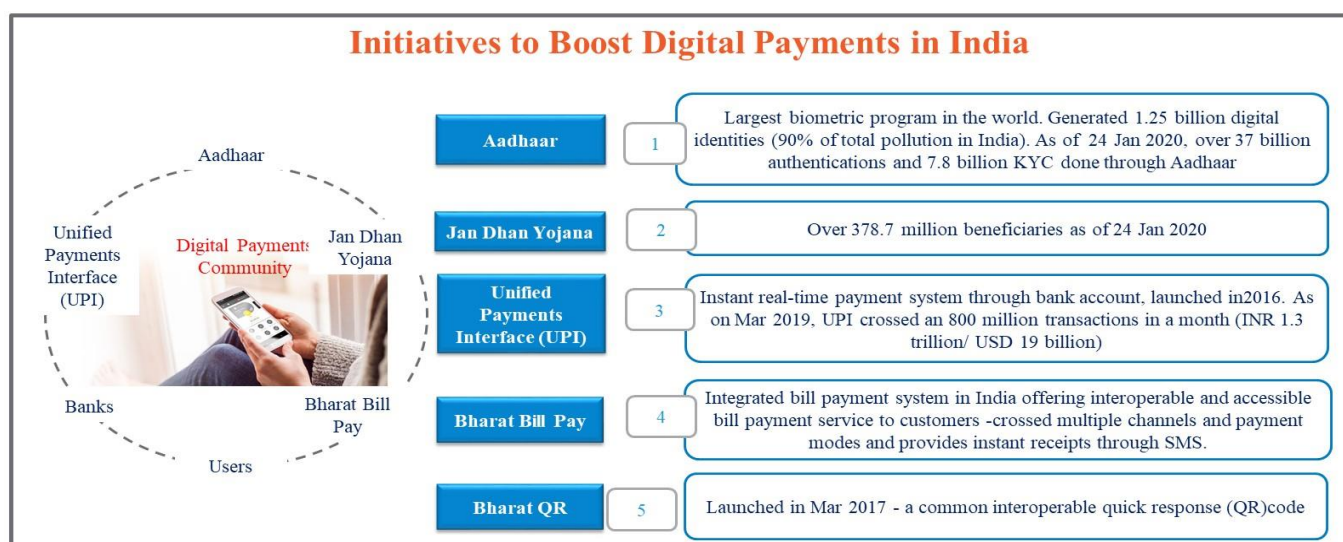


Figure 1. Initiatives to Boost Digital Payments in India

In the following sections, a brief analysis on banking penetration, access to the public, trends in technology, innovations and key enablers of Fintech growth are examined. The white paper also attempts to identify potential opportunities that lie ahead of both government as well as private entities.

¹ World Economic Forum, 2020, Article published by Mahindra Finance

² Fintech Ecosystem Playbook, EY, 2018, pmjdy.gov.in, uidai.gov.in

2. Rise of Digital Payments & Fintech Investments at Global level

As per EY's study³, in the first half of 2019, 28% of Fintech investment went to global payments technology. The study also indicates that, global transactions are becoming increasingly electronic leading to diversification of payment methods of businesses and consumers. The percentage of user sending and receiving payments through digital medium - mobile or web-based internet increased from 67% to 76% globally and from 57% to 70% in the developing world³. Adoption rate by service category and synergies between players are summarized in below sections.

2.1 *Common Industry trends at global level that drive Fintech disruption in payments market*⁴

- Worldwide, non-cash transaction is likely to exceed USD 1 trillion by 2024, driven by growth in APAC, which is likely to comprise 40% of transactions by 2024.
- Fintech start-ups are leveraging distributed ledger for cross border payments by connecting banks and payment providers using blockchain technology. Blockchain architecture meets regulatory requirements and ensures data privacy and can process up to hundreds of transactions per second.
- China is the global leader in digital payments, which had 85%+ of all payments in 2018 made via mobile payment applications, such as Alipay and WeChat Pay.
- Regulations like PSD2 (Payment Service Directive) of EU, Open Banking Standards are obliging banks to open their systems and data to third parties.
- US launched The Clearing House (TCH) network in 2017 to replace antiquated payments system.
- Federal Reserve has announced its plan to promote a round-the-clock real-time payment (RTP) and interbank settlement services by 2024.
- Real-time payment systems like New Payments Platform (NPP) in Australia is designed to support real-time data-rich payments (similar to UPI in India).
- API dependent services and business models have transformed the financial markets. 'Get /Accounts' is an API request type which returns comparable data such as ATM locations or details of banking products offered (credit card, etc.)

2.2 *Consumer Fintech adoption rate by service category*

Fintech industry is seen to be trending towards multiple financial services. Out of all, Payments landscape is experiencing high adoption rates (75%) as compared to other services of Fintech that were examined between 2015 to 2019⁵ as shown in Figure 2. Payments category is the most commonly used with below services:

- P2P (Peer to Peer) payments
- Non-bank money transfers
- In-store mobile payments

Other categories are savings, insurance, borrowing and financial planning

³ Fintech Ecosystem Playbook, EY, 2018

⁴ Infosys Analysis, 2019

⁵ Infosys Analysis, 2019

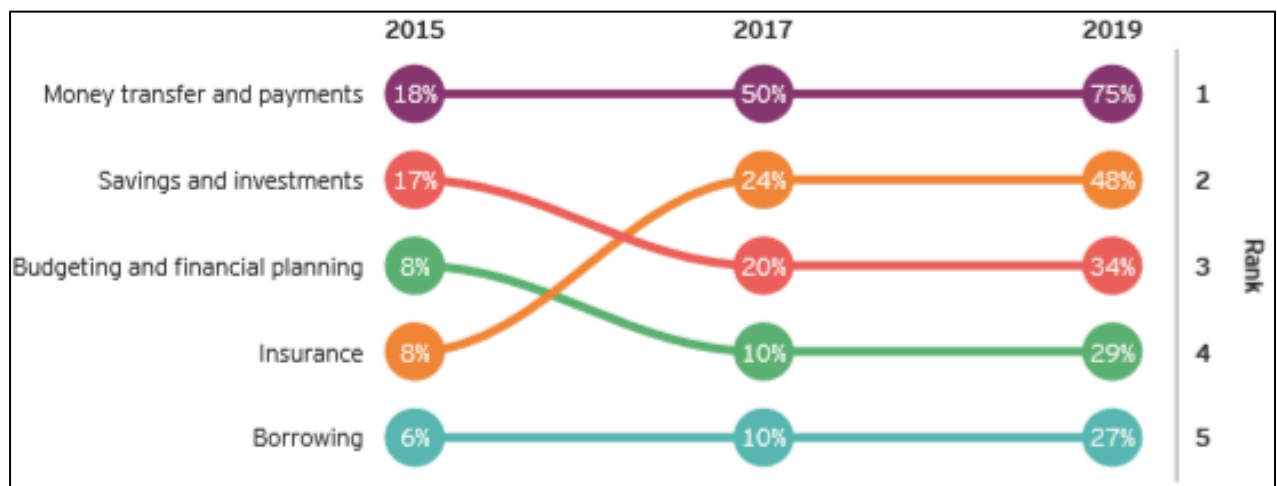


Figure 2. Consumer Fintech Adoption Rate by Service Category

2.3 Synergies between players – Fintech as a disruptor

Multiple players are involved in the synergy of payment processing. Out of all, Fintech has the potential opportunity to stand as a real disruptor as shown in Figure 3:

- Fintech can yield rich dividends by using overlay services
- Fintech can do brokering between corporates, SMEs and clearing houses causing real disruption in electronic payments processing
- Fintech can generate Account Tokens and Social Tokens

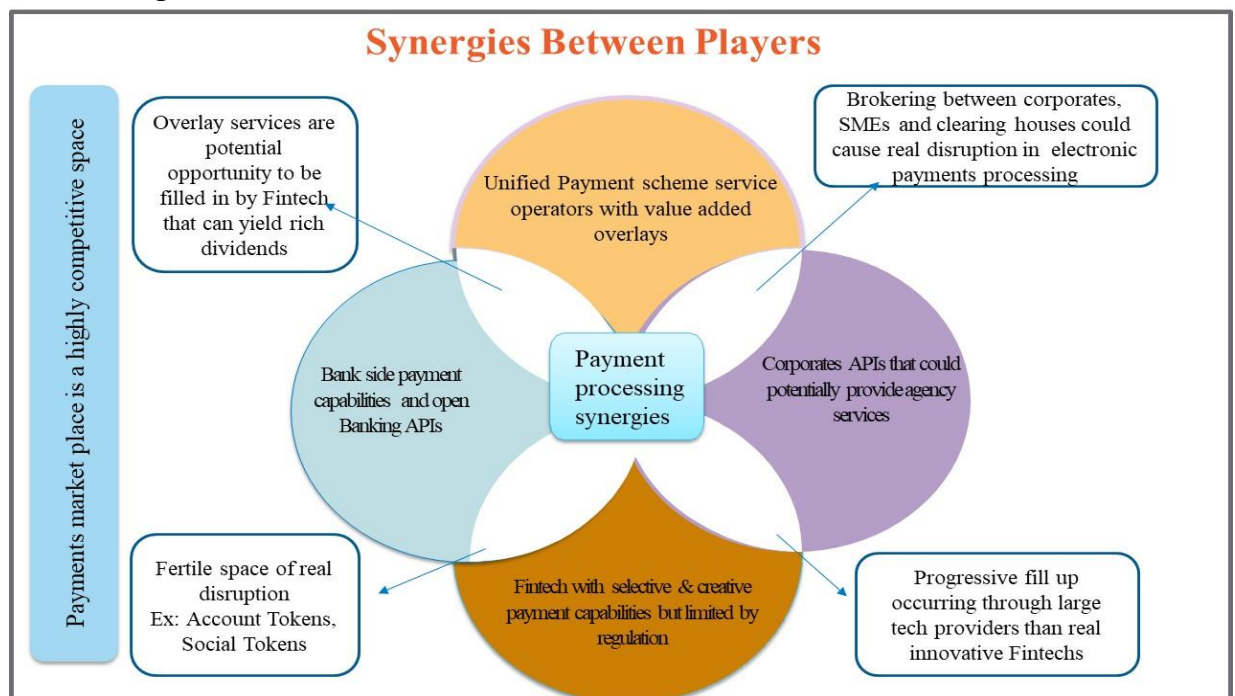


Figure 3. Synergies between Fintech Players

3. Digital Payments & Fintech Investments –Trendsetters in India

3.1 *Aadhaar enabled Payment System*

Aadhaar is the largest biometric program in the world -generated 1.25 billion digital identities (90% of total population in India). Over 100 million people withdrew money through the Aadhaar-enabled payment system to open a bank account using their Aadhaar based e-KYC (electronically Know Your Customer) and draw money in their village just by using their fingerprint⁶. Further, in the recent past, the Reserve Bank of India (RBI) launched Account Aggregator allowing financial information users to access financial records after obtaining consumer consent.

3.2 *Interoperable Bill Payment Application – Bharat BillPay (BBP)*

Government of India launched BharatBillPay (BBP) in 2016, an interoperable payment platform that allows users to make bill payments across multiple payment modes. Instant receipts are sent through SMS. In 2017, the Government launched Bharat QR - a common interoperable quick response (QR) code to make digital payment in stores.

3.3 *Unified Payments Interface (UPI) –BHIM App*

UPI was launched by NPCI in 2016 as instant real-time payment system through a mobile phone to facilitate inter-banking transaction. As of Mar 2019, UPI crossed an 800 million transactions in a month (INR 1.3 trillion/ USD 19 billion)³. BHIM App (Bharat Interface for Money) is one such example based on the Unified Payments Interface.

3.4 *Paytm*

Paytm with 70% share in offline merchant payments⁷ is one of the leading players in the digital payments sector which has penetrated deep into the remote corners of the country. Paytm is accepted at over 14 million retail outlets and is targeting to increase 25 million outlets by the end of FY 2020.

3.5 *Pradhan Mantri Jan Dhan Yojana*

Jan Dhan Yojana with over 378.7 million beneficiaries as of 24 Jan 2020⁸, aims to expand and make affordable access to financial services, eg bank accounts, remittances, credit, insurance and pensions.

3.6 *Start-up Initiatives for Fintechs in India*

Start-up India initiatives was introduced by Government of India in 2016 through which, USD 1.5 billion FOF (fund for funds) was made available for Fintech start-ups in India³. One of the key objectives of the start-up movement is to make India's massive workforce future ready. Recognizing this, Fintech focused talent programs were introduced by Bombay Stock Exchange in association with University of Mumbai in 2017 by launching an MBA program to develop talent pool to meet the global level competition. It is apt to mention here that, many of the current global world economic, technology and leadership forums, including the recently concluded Davos 2020 Summit, have realized the importance of upskilling the existing talent pool that is future ready.

⁶ World Economic Forum 2020, Article published by Nandan Nilekani

⁷ Best Media Info, Oct-2019 (bestmediainfo.com)

⁸ pmjdy.gov.in,

4. Shared Benefits and Value Chain created by Fintech

4.1 Fintechs in Payment Value Chain

Fintech gives the opportunity to create value across the payment value chain where multiple channels can come together under the same umbrella with shared benefits. As shown in Figure 4 , payments value chain involves, at a broad level the following stages where a payment will have its journey to traverse through:

- Payment Initiation
- Payment Validation
- Risks & Compliance Checks
- Settlement & Accounting
- Payment Gateways/ Switches

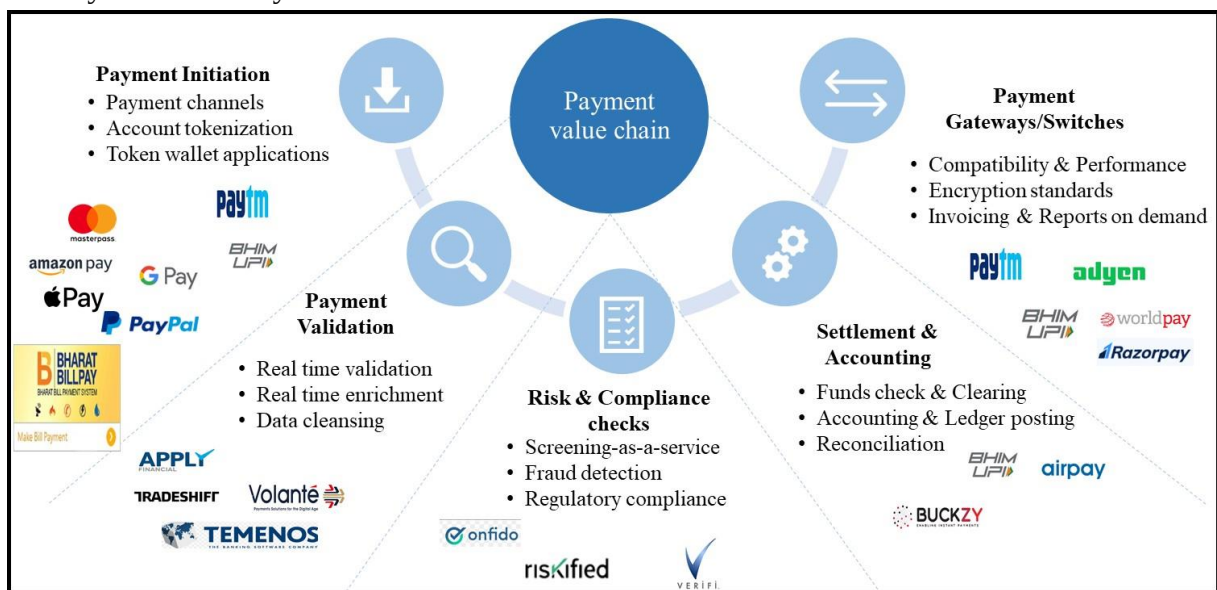


Figure 4. Shared Benefits and Value Chain Created by Fintech

Figure 4 provides an idea of the density of Fintechs in specific buckets of payments value chain, which motivates:

- Revenue generation opportunities
- Regulatory restrictions

Thus, the Fintech ecosystem is skewed heavily on both ends of the value chain. Payment initiation is predominantly driven by regulation. On one hand, the symbiotic relationship between the Fintech and FI in leveraging the data and payments propensity is used to cross sell banking services; however, on the other hand, payment gateways are critically involved connecting banking to all other lines of businesses; thereby creating extended ecosystems for banks and the service companies. For example, the symbiotic relationships between banks and telecom service providers have resulted in synergies on one hand but created differentiating entities like payment banks on the other hand.

5. Need of the Hour – Innovations in Digital Payments & Fintech

Keeping in view of the fact that, demand and awareness is growing exponentially, a good user experience has become essential. Therefore, the need for technology that addresses pain-points and supports contextual awareness is seen to be critical. That is where innovations come into play - using science of availability (automatic, quick, little or no effort), leveraging AI on Public Big Data, Blockchain and so forth. Refer illustrations provided in Figure 6 and Figure 7.

Few emerging service categories are listed below-

- Real-time customer available platforms – contact customers at the right time when they are physically and mentally available
- Transact across currencies, countries, family members and friends as easy as texting (quick cashout/ group pay introduced by Circle Pay (App))
- Walk into the unmanned store and take your product using mobile phone- (Watasale) Figure 5
- Virtual Super Markets accessible in trains/ walls of Metro Stations using QR code through mobile phone and delivered in door step (Tesco in South Korea)
- Social tokens with asset value that can handle agnostic digital wallets and can create new generation of asset class.
- Account tokens: contact less payment method at POS -Figure 6
- Connected vehicles (Pay by car) Figure 6
- Robo advisory/ Conversational AI - online financial advisor or Chatbots
- Make productivity tool like Microsoft Excel to track payments receivable/payables (PayU money)

5.1 Innovations in Digital Payment & Fintech

5.1.1 Deep Learning and Sensor to develop unmanned store

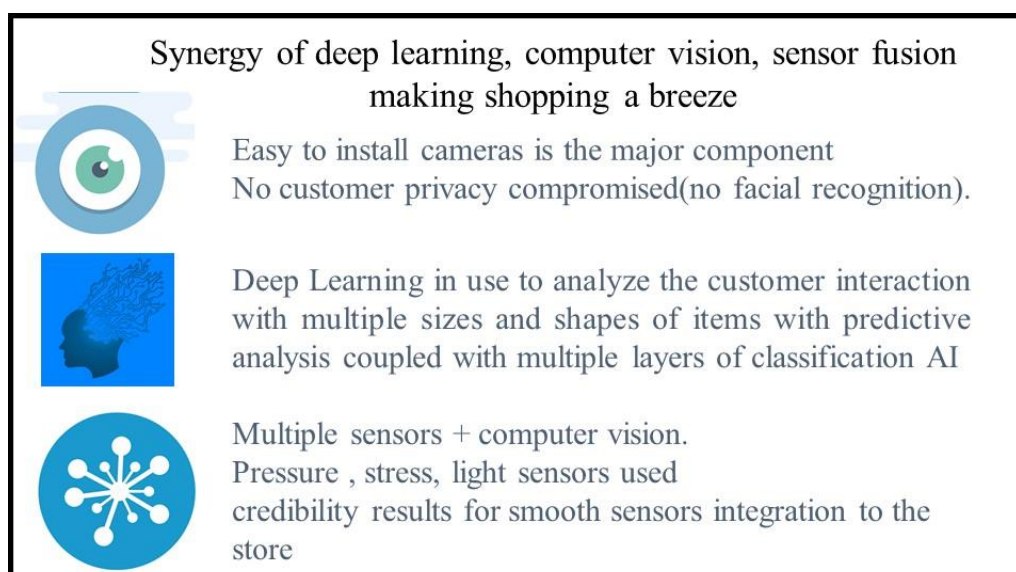


Figure 5. Technologies in Unmanned Store

5.1.2 Pay by Connected Vehicles

YOU ALREADY HAVE A CONNECTED CAR THAT PAYS FOR YOU

PAYBYCAR RECOGNIZES YOUR TOLL-TRANSPONDER TAG/STICKER IN COMBINATION WITH YOUR SMARTPHONE.

Enhanced User Experience of payments at...

- Gas Stations,
- Drive in Restaurants
- Drive in Departmental stores
- Comes with loyalty offerings

ENROLL

As Easy as 1-2-3

EASIER

No Confusing Apps

SECURE

2-Step Security

SAVE \$\$\$

Special Offers

Tokenize your Account

Ease Enrolment & Token creation

Go Contactless with multiple tokens

Figure 6. Pay by Connected Car and Tokenize your Account

5.1.3 Tokenize your accounts

This Fintech solution puts one bank native mobile app at the center of the everyday consumer experience, by letting consumers pay for purchases directly from their bank account or combination of accounts. Consumer can purchase through Mobile App with unique payment method using QR code without any contact with the POS. Refer Figure 7. Further, tokenized accounts with asset value can co-exist in these wallets.

5.2 Leading Fintech Innovators in India

Leading Fintechs in India			Categories	Solutions	Possible vendors
Market Place Lending  	Next Generation Payments  	Wealth Management/ Robo Advisory 	Process improvement	E-sign / Consent	 
	OCR				
	Multiple payment methods	 			
	Automated Dedupe	 			
	Digital Locker				
Blockchain	Financial Inclusion	Securities/ Biometrics	PAN/Voter/Account ID Validation	  	
			Business Rules Engine	  	
			eNACH	 	
			Automated income assessment		
			Property valuation aggregators	 	
	Address verification				

Figure 7. Leading Fintechs in India

5.2.1 Other Innovative Technologies

There are other compelling Fintechs such as, payment insurance/guaranteed payment delivery ensuring that payment reaches the right receiver, real-time cross border multi-currency payments, switches, risks and compliance capabilities related innovations as highlighted in Figure 8.

 Payment Insurance	 Blockchain	 Cross Border Payments
Osko	Vajra	BUCKZY
Founded In: 1997 Head quarters: Australia Features: - Secure payments services which enables you to send/ receive payments using PayID on NPP - Real time faster payments Differentiators: - P2P payments uses PayID - Located within online banking and backed by BPAY	Founded In: Nov, 2019 Head quarters: Mumbai Features: - Uses distributed ledger technology - Reduces manual reconciliation and reporting - Handles dispute management due to decentralized and distributed data storage Differentiators: - Provides a legitimate audit trail - Enhanced security due to block chain cryptography	Founded In: 2018 Head quarters: Toronto, Canada Features: - Two-factor authentication on the back-end - Adherence to ISO 20022 - AI tool for sanctions screening and KYC Differentiators: - Cross border P2P real-time ecosystem with Zero Transaction Fee. - Real time FX quote.
Large Player Innovations		
Finastra - Fusion	Nets- Denmark	FSCM Payments
 Founded In: 1979 Head quarters: London, England Features: - Deliver leading-edge digital payment, remote deposit capture and card technologies - Retail payment product suite – Fusion Card payments, Fusion DPXPay, Fusion NetCapture Suite Differentiators: - Integrate with core systems	 Founded In: 2009 Head quarters: Copenhagen, Denmark Features: - Micro-services architecture based instant payment solutions - Also provides open banking platform Differentiators: - Wide range of service offerings – core payment infrastructure, PSD2 solutions and fraud detection	 Founded In: 2016 Head quarters: Mumbai, India Features: - Covers Accounts payables and receivables + payments - Provides options to drive working capital loans and overdrafts on the flow Differentiators: - FSCM + Payments processing orchestration
Payment Gateway/Switches		
2checkout	Braintree	Adyen
 Founded In: 1998 Head quarters: USA Features: - Advanced fraud protection, PCI DSS level 1 certified - Intelligent Payment Routing, gives the highest possible payment authorization rates Differentiators: - Supports multiple checkout cart integration, including Shopify, WooCommerce etc.	 Founded In: 2007 Head quarters: USA Features: - Gives access to PayPal, Venmo with host of other payment options - Offers the most popular local payment types Differentiators: - Seamless integration with tools to prevent fraudulent transactions and optimizing business with key insights	 Founded In: 2007 Head quarters: USA Features: - Account updater - Batch processing - Enables import of data from different payment provider Differentiators: - Have developed automated marketplace onboarding capabilities and KYC services, which support marketplace customers
Risk & Compliance Checks		
Riskified	BreachRX	Verifi
 Founded In: 2013 Head quarters: Tel Aviv, Israel and NY USA Features: - Riskified provides fraud detection and chargeback prevention technology for merchants by using ML, behavior analytics, IP, geolocation - Every order is risk-profiled to determine a Go/ No Go Differentiators: - E-commerce fraud prevention system - Orders placed against any payment channel can be proof-tested (except COD, bit-coins)	 Founded In: 2017 Head quarters: Washington, USA Features: - Incident response to data breaches and cyber security incidents in a financial institutions. - An employee can log an incidence in the dashboard - Creates a single system of record and reporting engine Differentiators: - Breach simulators to post-breach analytics - Auto-response to Reg compliance	 Founded In: 2005 Head quarters: Los Angeles, USA Features: - Fights omni-channel fraud with 'Intelligence suite' a turn-key risk management platform - Claims to stop upto 55% of chargebacks (fraud and non-fraud) and recovery rates upto 20% (On declined billings and lapsed customers) Differentiators: - Cardholder Dispute Resolution Network (CDRN) to stop chargebacks 'Intelligence suite' for fraud protection

Figure 8. Innovations in Digital Payments & Fintech

6. Fintech Growth in India – Key Opportunities

6.1 *Unmet financial needs*

Despite the wide branch network in India (138,294 branches as of March 2016), the financial services ecosystem still lags in terms of coverage. These gaps in access to formal financial services have created a large untapped market potential for FintTech startups to develop a variety of offerings.

6.2 *Increasing investments in Fintech*

There has been a significant increase in Fintech startups in India over the last few years, primarily in the payments space (driven by regulatory changes and market demand). In addition, there is increased willingness by domestic, as well as international VCs/PEs and incubators to heavily invest in this sector in India. Further, it is important to emphasize on security aspects in remote parts of the country where speed of technology is still a challenge.

6.3 *Availability of Policy Framework*

RBI has been steadily promoting a digital agenda to deepen and broaden financial inclusion services in the country. Initiatives such as UPI, Unstructured Supplementary Service Data (USSD), Bharat Interface for Money (BHIM), Aadhaar Enabled Payments System (AEPS) are expected to further strengthen the financial services infrastructure

6.4 *Penetration of Smartphones/ Broadband*

India is expected to have 800m smartphone users in 2022, up from 400m in 2017 as per Cisco. This will propel India's per capita data consumption to nearly 14 GB by 2022 from 2.4 GB in 2017

A recent study has also revealed that India cheapest mobile data in the world. Indians pay on an average ₹ 18 for one GB of data against a global average of ₹ 600⁹.

⁹ Infosys Study

7. Our Recommendations

7.1 *Next generation banking model – digital transformation across each step*

- Coreless Bank - modernised banking software which helps the bank to source and adopt new business services- a faster, cost effective and relevant for today's digital-first customers. This will help solving perpetual challenges faced in legacy core infrastructure.
- Digital Process - Process connecting core and channels, driven by micro services and API economy/share economy/creator economy
- Digital Channel - Self-contained and seamless transfer across mobile, branch, internet, ATM, kiosks, Facebook, Twitter
- Digital Commerce - Digitalized cards on your wallet, commerce from Banks and its partners
- Digital Ecosystem - Provide partners and consumers a platform to collaborate and leverage the Banking API cloud

7.2 *Real time decisions to solve Industry problem using Big Data*

Data management and Analytics can be used for fraud analysis, real time recommendations, client 360 and customer insights, risk and exposure analysis, market data analysis, ATM fault prediction.

7.3 *Design Accelerator Program*

Banks are encouraged to provide funding, mentorship, tech support, domain expertise, networking opportunities to Fintechs through accelerator programs. Banks can conduct collaborative hackathons with cross industry digital champions to encourage cross pollination of ideas. Accordingly, start-ups can build solutions leveraging futuristic technologies in the banking sector.

7.4 *Collaborative Approach*

Collaborative approach is needed to leverage Fintech's product and platform offerings using innovation. Banks should work towards creation of offerings through state-of the art digital touchpoints with robust back-end platforms in collaboration with partners. This would score high on usability which has relevance to digitally native or Gen X customers. As the digital markets evolve, increased collaboration is expected between incumbent banks and Fintech in their joint pursuit of making digital payment seamless, simple, friction-less and secure.

7.5 *Security Architecture*

As more and more services are offered through digital mode, data security has become a major challenge for Fintech. Security architectures need to be designed taking into account financial trends, fraud analysis. Collaboration is key here. Cyber industry must work alongside Fintech against a common challenge. Coordinated efforts is a must between start-ups, corporates, government and academia to find the best possible solutions for the cyber age.

23rd National Conference on eGovernance

A white paper on the
**BlockChain for effective Governance & Service Delivery in
Public Sector**



Authors: Vijayalakshmi G and Nagesh C R

Vijayalakshmi.gopalakrishna@sap.com Nagesh.caparthysap.com

Abstract

Traditional client-server architectures are vulnerable to cyber-attacks due to their single point of security intelligence on the server. A foundational characteristic of a blockchain is trust. Blockchain, a Distributed Ledger Technology (DLT) is a technology that has been acclaimed as a revolutionary new means of secure and transparent record-keeping and data sharing, with seemingly endless potential uses in a wide variety of sectors. Today, the public sector and governments have been actively researching new technologies to enable the smart services transformation and to achieve strategic objectives such as citizens satisfaction and happiness, services efficiency and cost optimization.

The Blockchain is playing a crucial role in many sectors transforming the way we think about trust as it enables transacting data in a decentralized structure without the need to have trusted central authorities.

Many government entities in countries such as the United Kingdom, Estonia, Honduras, Denmark, Australia, Singapore and many others have taken steps to unleash the potential of Blockchain technology. Dubai Government is aiming to become paperless by adopting the Blockchain technology for all transactions by 2021 [1].

The objective of this whitepaper is to emphasize on the key benefits of using blockchain and the potential to deploy applications to speed up access to data, ensure the integrity of data, and reduce overall cost.

The question for executives is no longer “Will blockchain work?” but, “How can we make blockchain work for us?”

Keywords: Blockchain Technology, Supply Chain, KYC, global blockchain traction, Benefits, Challenges.

Introduction to Blockchain

The simplest blockchain definition? **“A reliable record of who owns what, and who transacts what.”**

A technical explanation of it would be, a blockchain is a ledger of digital transactions, but instead of being centrally controlled and located, as most databases are today, it is decentralized and not under the control of any single entity or individual. Individual transaction data files (blocks) are like new pages in a physical ledger. Newer blocks are linked to older ones, forming a chain, hence the term blockchain. These are managed through specific software platforms that allow the data to be transmitted, processed, stored, and represented in human-readable form. This is pictorially shown in Figure 1.

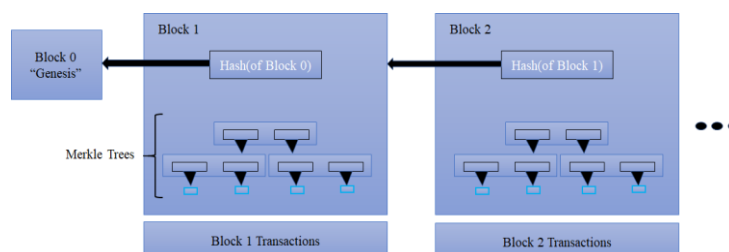


Figure 1: Example of a blockchain containing n blocks, in which each successive block contains the hash of the previous block, Merkle Tree and transaction information

Blockchain can be public, private, or a hybrid of the two, which are described as follows:

Public blockchains: A public blockchain is an open blockchain that can be read by anyone in the world without any restrictions; anyone in the world can post transactions to this kind of blockchain and also see them added to the chain if they are valid. A public blockchain is a totally transparent ledger. Some of the largest and most commonly known public blockchains are Ethereum and Bitcoin.

Fully private blockchains: In fully private blockchains, write permissions are managed centrally by one organization. All other parties can have read access that is either complete or restricted. This will involve database management, auditing, and so forth, which will be internal to the company managing the blockchain.

Consortium blockchains (hybrid): In a consortium or hybrid blockchain, the consensus process or a general agreement is controlled by a preselected set of nodes. Consider the example of a consortium of 5 financial institutes: each operates a node, and each must sign every block for the block to be valid. The read access can be given to the entire public or be restricted to a few participants. These can also be considered “partially decentralized.”

Today there is an increasing demand to have traceability and transparency across the supply chain system. Blockchain is best suited when 3 or more stake holders are involved with minimal or no trust among them. Blockchain offers us to create communication channels with the required members of the program to securely share data among each other for business. Figure 2 shows the evolution of blockchain from Blockchain 1.0.

Emergence of Blockchain 3.0 and its comparison to earlier versions

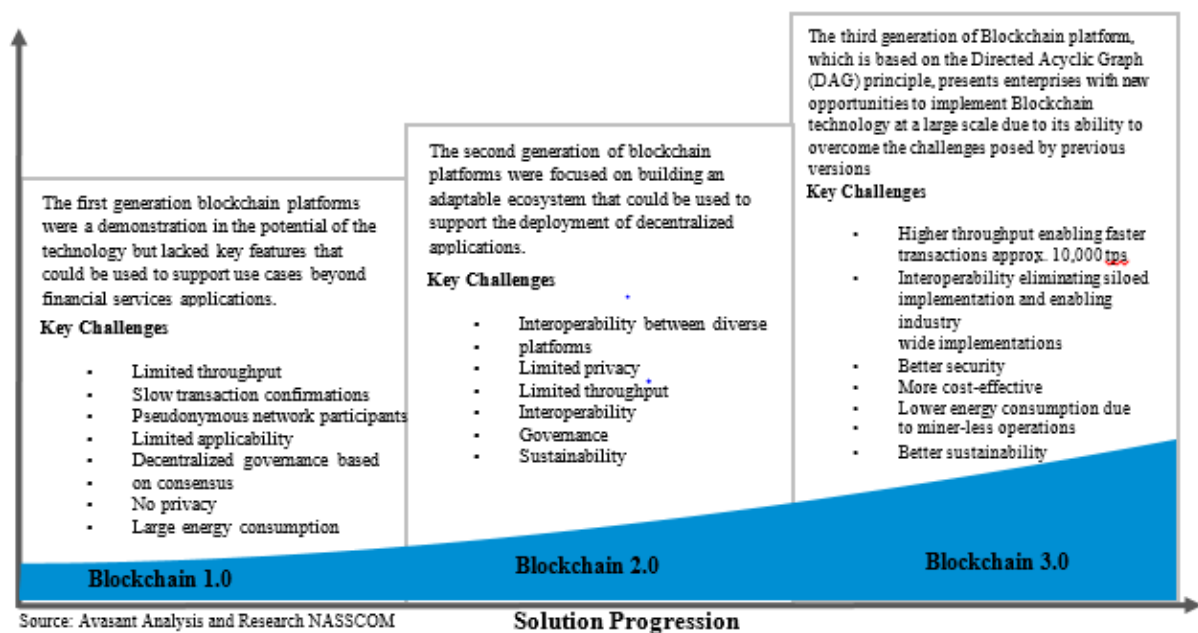
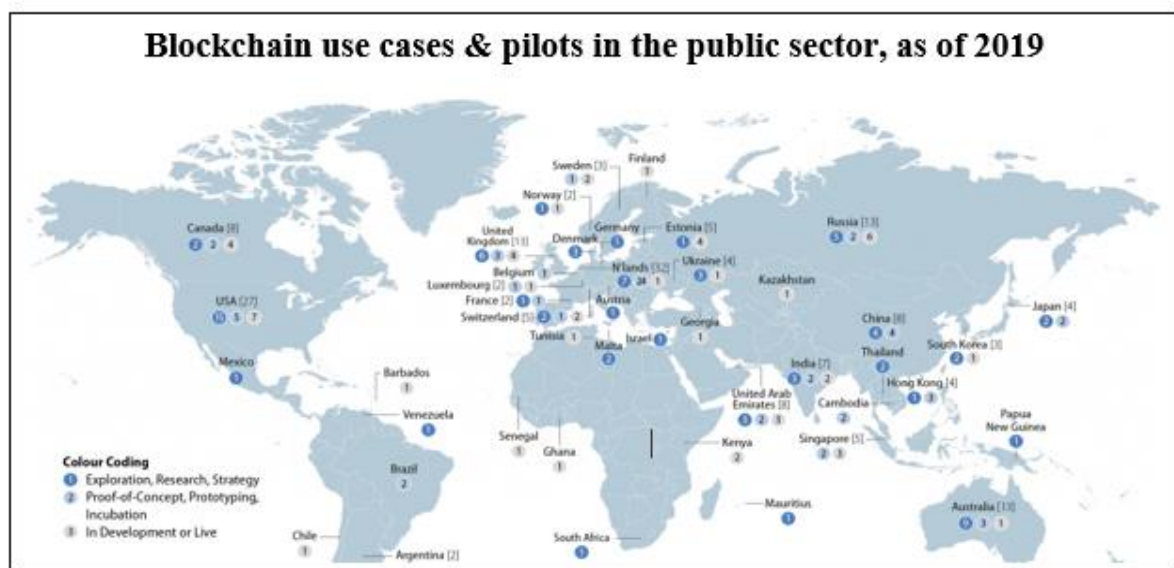


Figure 2: Emergence of Blockchain 3.0 and its increased security, interoperability and scalability, enterprise adoption is set to accelerate Blockchain 1.0

Adoption of blockchain and digital innovation

Blockchain has relevancy in a wide variety of areas, including tax filing, voting, land registry, healthcare, creating tamper-proof voting records, vehicle registries, fraud-proof government benefits disbursements, and digital identities for individuals, such as refugees, who lack government-issued identity documents. It not only provides a trusted mechanism of storing and transferring data but also provides transparency across the system. Several countries and states such as Canada, the United Kingdom, Sweden, Ghana, India, Estonia and Georgia in the USA are researching blockchain-based solutions by running pilots, tests, and trials examining both the architecture's broad utility as a basis for government service provision and procurement. (refer figure 3)



Source: 2018 OECD analysis of data collected by the Illinois Blockchain initiative <https://illinoisblockchain.tech/> and <http://bit.ly/blockchain-govt-tracker>

Figure 3: Indicative list of blockchain experiments in the public sector

In Estonia, the government is rolling out a technology named Keyless Signature Infrastructure (KSI) to safeguard all data. Electronic health records of all Estonian citizens are managed using KSI technology. KSI allows officials to monitor changes within databases - changes of record, what changes are implemented, and when are they made, hence, any unauthorized tampering of the records can be detected and prevented [2]. They have also implemented e-voting mechanism since 2005 and has seen one-third of votes in parliamentary elections which are cast online over 110 countries.

Dubai is working its way through the blockchain technology and aims to become the first government by 2020 to implement blockchain to complete all of their transactions. They have estimated that this will significantly reduce their document processing charges.

Digitizing registration of land and property transactions is another use case where Sweden has successfully completed a pilot in which land registry copies are shared with all relevant parties to facilitate property purchases with each step of the sale is verified and recorded on the blockchain [3]. In addition to it, The Republic of Georgia has a blockchain-based land registry system. It was launched in 2016 by the country's National Agency of Public Registry. Working with the Bitfuri Group they

applied blockchain technology in their land title registry process. It has significantly reduced the cost and processing time of land registration from three days to a few minutes. But most importantly it has added transparency in the land registry system [4].

The Australian Securities Exchange (ASX) became the world's first major trading exchange to announce the adoption of blockchain technology to develop a new post-trade platform based on distributed ledger technology to record shareholdings and manage the clearing and settlement of equity transactions [5].

Government owned Australian post service is experimenting to a location agnostic, tamper proof voting which is traceable and anonymous. They also hope to expand the solution to handle full parliamentary elections [6].

Dubai Land Department employing three initiatives Ownership verification in DLD Mobile Application, Property sale by Developer and Smart Leasing Process, targeting the improvement of providing the services, collaboration with other parties involved in the real estate market and to create a secured digital asset [7].

Globally enterprise organizations are also recognizes the collaborative approach of consortium using blockchain based farm-to-consumer material traceability solution. It is an end-to-end supply-chain product traceability and recall management SaaS offering for the food industry which is helping farmers obtain maximum gain [8].

In India, blockchain saw early adoption in 2016 primarily among the players in the Banking and Financial Services industry. But with the beginning of 2017, India has seen blockchain adoption increasing amongst government bodies, Fast Moving Consumer Goods and Pharmaceutical industry. The **NITI Aayog** is working on building the country's largest blockchain network — IndiaChain, in a bid to reduce frauds, speed up enforcement of contracts and increase the transparency of transactions [9].

The Government of Andhra Pradesh & Telangana has started to pilot Land Title Registry to avoid tampering of data using blockchain technology. Andhra Pradesh is currently working on a development plan to make this effective [10].

Maharashtra and Gujarat are also holding discussions with start-ups in the blockchain space and setting up a Fintech Hub to promote blockchain-based start-ups. About 50% of the states in India are involved in blockchain-related initiatives, driving the public sector blockchain adoption in the country (refer to figure 4)

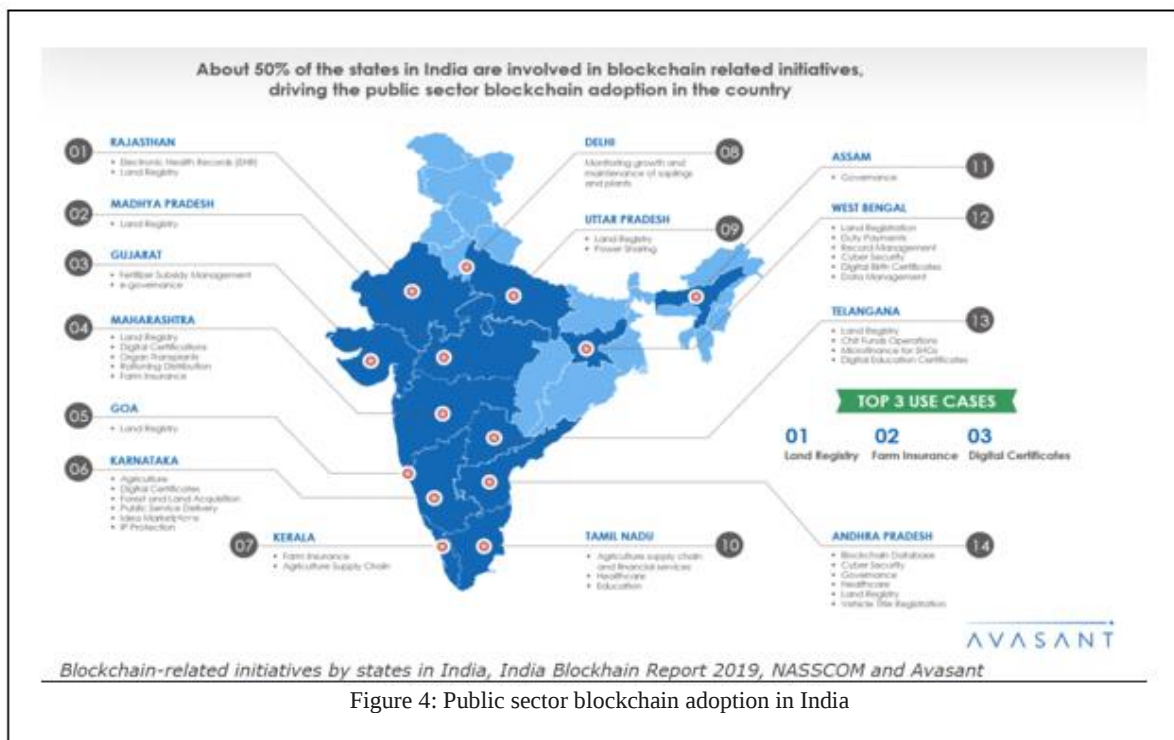


Figure 4: Public sector blockchain adoption in India

Potential Blockchain use cases for Public Sector in India

Blockchain has unlocked the potential to become an industry-wide technology standard and has many potential applications. Few examples:

1. **Know Your Customer/Citizen (Identity Management):** KYC is one of the most expensive ongoing tasks for a lifetime. It is a cumbersome process and used by every organization, both public or private sector. Every individual must submit their documents which will be verified by an authorized representative, and the digitized documents will be stored with a unique identity to serve further requests or services. This can help us to track required information such as citizenship, residential details, name, age(alive/dead), gender, dependents etc..

Blockchain-based KYC approach can cater to many services with multiple Government entities - public/private entities. It can digitally transform the nation and help to prevent fraud at multi-levels. Important opportunities are listed below:

1.1. Aadhar - National Registry of Citizenship

As a country, India had to spend huge effort and cost to implement Aadhar in the past which provides proof of residence. Today, we are looking at implementing NRC across India to track illegal immigrants. Hosting a central database approach may not help our system and may not scale in the future due to its limitations. KYC requires tamper-proof records which track all the important documents and capture information about the authority who has approved it too. Integration between the Aadhaar system and Blockchain-based KYC can make a tremendous change in the implementation mechanism and once implemented, Blockchain-based KYC can be an exclusive system for verification in the future and can eliminate duplicate systems.

Further research and efforts can be emphasized to make implementation success.

1.2. eVoting

India is one of the most expensive countries in the world spending huge money on voting mechanism. In 2019 Lok Shaba elections, ~4500 crores were spent on procuring EVM and estimates an amount of Rs 13,981.58 crore will be required for procuring new EVMs for the proposed simultaneous elections in 2034[11]. Despite efforts to make the voting mechanisms smooth to 900 million people, our turnout was only ~67% which is higher than the previous years. Approximately 40% of citizens are not able to vote due to various reasons such as difficulty in reaching the polls, non-residing Indians etc.

On the other hand, there is a huge challenge to monitor the election voting booths with the support of staff and police protection.

There is an enormous scope of converting this voting mechanism to eVoting with the help of Blockchain. Globally many countries have come ahead in experimenting with the blockchain-based solution.

1.3. Digital Passport & Immigration

Indian Government has made a tremendous improvement to our Passport Seva Kendra with online bookings systems. However, 50% of the applicants must reschedule their appointments due to missing documents. On the other hand, our immigration process is still manual. There is always a scope to verify the authenticity of Passport holders again tracing back to its issuing country which can help us to track fake passport and stop illegal entries. Globally many countries have implemented Automated Biometric immigration process and few countries, especially Canada and the Netherlands have launched a pilot program for paperless travel between the two countries at Montreal's largest Airport[12].

1.4. Land Registration and Digital Real Estate

Land/build plan records tampering in real estate is a giant business and many have fallen prey. Verification is a tremendous task at all levels and time-consuming. An individual with a lack of knowledge on the verification process depends on middlemen at an additional cost.

On the other and, construction plan requires approval from multiple entities such as local bodies, building approval from the respective government, engineers, water board approvals, electric board approval etc. is a tremendous task. There is a greater need to make all the parties involved well connected with all the entities to run the real estate effectively.

1.5. Supply chain

Today there is an increasing demand to have traceability and transparency across the supply chain system. For example, in the case of food tracking the entire supply chain of the food production to processing, packaging, storage, transportation and sale to a consumer must be tracked.

New economic models, powered by technology innovation like blockchain and artificial intelligence, provides full visibility of a product from the producer to the consumer—and even beyond to recycling and reuse. Blockchain along with advanced technology-based IoT devices such as Electrochemical Sensors to understand the pH and soil nutrient level, Mechanical Sensors to measures soil compaction or mechanical resistance, Dielectric Soil Moisture Sensors to assess moisture levels by measuring the

dielectric constant, Airflow Sensors to measure soil air permeability can assist a farmer to gain maximum yield in the agriculture sector.

Blockchain is best suited when 3 or more stakeholders are involved with minimal or no trust among them. In this case, farmers, certification operators, traders/exporters, customs, and consumers can all be a part of the blockchain network to increase traceability and transparency. All information such as farmer field, crop production, certifications obtained from the operators, trading information, etc., can all be stored on a blockchain system.

With the huge digital data from sources such as IoT sensors, crop production, domestic/global supply chain, we can add analytics to design forecast, prediction and best practices on all areas.

1.6. Other Blockchain Possibilities

- Disaster Relief Management with Blockchain. With Efficient Pooling & Sharing in Disaster Relief Missions
- Inter-agency Workflow for Governmental Administration
- Effective Farm Loan Waiver
- Tamper-Proof and Collaborated Crime Records
- Digital traffic and vehicle insurance management

Potential Challenges

Although, Blockchain is expected to offer many benefits to the traditional supply chains there are a few challenges the organizations must address the challenges have been categorized into 3 categories:

1. Organizational challenges such as Resistance from many organizations to alter their existing models, resistance from existing supply-chain intermediaries and other partners, as the blockchain aims to remove the intermediaries etc.
2. Technological challenges such as achieving an optimal combination of interoperable and compatible platforms may be a difficult task, issues such as moving from the existing centralized ledger systems (ERP) to a decentralized system and data ownership needs a possible justification in terms of what significant additional benefits the Blockchain Technology will be able to offer.
3. Environmental challenges like bringing all the supply chain and trading partners together to implement blockchain across the supply chain network is a difficult task.

Extensive research along with multiple government entities must be considered for a consortium-based blockchain implementation with all the policies.

Conclusion

Given blockchain technology's extensive applicability and transformational potential, policymakers may find it worthwhile to explore the spectrum of possibilities available within their respective departments. A blockchain-based approach could strengthen the efficiency of transaction processing and reduce, if not entirely prevent, fraud.

However, to unlock the full potential of this technology, the government will need to work as a facilitator, by providing an enabling environment to interested players. Government departments looking at digital technologies as enablers of competitive advantage, should not overlook blockchain.

There is also a need to develop uniform standards, assess infrastructure requirements, allay security concerns, raise stakeholder awareness, and build trust within the entire ecosystem. Though it may still take some time before we begin to see large-scale commercial applications, it is progressively likely that many industries, citizen services, and government programs will feel its impact, sooner rather than later.

References:

1. Dubai government website, <https://www.smartdubai.ae/initiatives/blockchain>
2. Estonia government website, <https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/>
3. Reuters, "Sweden's Land Registry Successfully Completes Blockchain Pilot," June 17, 2016, <https://uk.reuters.com/article/us-sweden-blockchain/sweden-tests-blockchain-technology-for-land-registry-idUKKCN0Z22KV>
4. Giorgi Mikhelidze, "Country of Georgia gets its first crypto exchange," Aug 19, 2019, <https://www.cryptopolitan.com/country-of-georgia-gets-its-first-crypto-exchange/>
5. Australian Securities Exchange website, <https://www.asx.com.au/services/technology-solution.htm>
6. Eloisa Marchesoni, "Blockchain e-Voting is real: where, how and when?", July 19, 2019, https://irishtechnews.ie/blockchain-e-voting-is-real-where-how-when/?_cf_chl_jschl_tk__=c337a6721807f5e2ef69c0b02e6d3721123b690b-1580399145-0-AcrfavvMH6Wgt3yTRQFij6G-mIAj-PlcpTTmyaYE8m-LIz-t-mehC4bYhGC41-RsNTn8fNO8z0n-w8QRFyaV2v_XL21KYy5jV9imDwJMjhlxy6tYyyXnY0S4iuRtShwx4phkh2LEZk0LppSGpALHKT39r-qdy4fymGOMM7m5lwL0CuJ_3m2pZygFZ8550vIcJ7i4v8HFEuo972h-4OREIap_pu6KaYt5ncG99rudANHXiV2D0XYpV05SIhks9bbmmV9GfMuyRV52l-54fLPzcq8JnZmVteNHygRLUCETde9YF9iLq8a9x_9tuaROO7TgTQ
7. Dubai government website, <https://www.dubailand.gov.ae/English/Pages/Blockchain.aspx>
8. SAP official website, <https://www.sap.com/documents/2019/11/865a4acd-707d-0010-87a3-c30de2ffd8ff.html>
9. Factor Daily, "IndiaChain: Niti Aayog starts on IndiaStack-linked, large-scale Blockchain projects," November 13, 2017, <https://factordaily.com/indiachain-indiastack-blockchain/>
10. Mugdha Variya et al. "Blockchain tech is joining e-gov dots in AP, Telangana", Jun 27, 2017, <https://economictimes.indiatimes.com/small-biz/security-tech/technology/blockchain-tech-is-joining-e-gov-dots-in-ap-telangana/articleshow/59330625.cms>
11. Press Trust of India, Rs 4,500 Crore Needed For Voting Machines For Simultaneous Polls: Report, Sep 03, 2018, <https://www.ndtv.com/india-news/rs-4-500-crore-needed-for-evms-paper-trail-machines-for-simultaneous-elections-law-commission-1910473>
12. Suzanne Rowan Kelleher, "Paradigm Shift: Biometrics And The Blockchain Will Replace Paper Passports Sooner Than You Think", Jun 28, 2019, <https://www.forbes.com/sites/suzannerowankelleher/2019/06/28/paradigm-shift-biometrics-and-the-blockchain-will-replace-paper-passports-sooner-than-you-think/#52b000045c7f>

23rd National Conference on eGovernance

White Paper
on
Building Digital Trust –
Transparency, Security and Privacy

**Authors: Team at
Tech Mahindra**

We live in a data-centric, data-dependent, world. Multinationals and large companies, today, are not able to do any meaningful business without having the ability to process data and access information. Data has become the most critical asset in any business that has, unsurprisingly, garnered the attention of State-Actors and criminal organizations seeking access to the “Crown-Jewel” systems for malicious and competitive reasons - which range from cyber-crimes, financial fraud, corporate espionage, and political ends - such as meddling with elections. Democratic countries are under assault for their Intellectual Property and Personal Identifiable Information (PII) of its citizens and subjects. Governments and businesses want to ensure that their data is safe.

CISO, a modern-day Arjun: In this era of great attention to data and data protection, corporations have appointed the function of a CISO (Chief Information Security Officer). As data gets generated and moves, boundlessly, in a multi-cloud enabled IT world, a high stakes battlefield ensues for the protection of Mission-Critical-Data, which is analogous to a modern Kurukshetra, for the CISO and his team, where CISO acts as a modern day Arjun. Like Arjun, a CISO has to wage war not just against all kind of external perpetrators but also has to be mindful of employees and contractors processing data in undesired ways, whether by intention to harm or by negligence. The CISOs have instituted a perimeter that is laden with Firewalls, Packet Security, Event Analytics as well as advanced Hunt and Detect capabilities utilising Artificial Intelligence and Machine Learning, which have not stopped the frequency and severity of cyber-attacks – and which are in fact, intensifying.

Data breaches: With the increasing frequency, scale and severity of recent data breaches such as Equifax (sensitive financial information for close to half of American population), British Airways (credit card data) or Cambridge Analytica (personal social media data), one can only empathise with the plight of Arjun. Further, this Arjun also needs to face the regulatory & media scrutiny.

Consumer trust & transparency: Strong data protection, or its lack, directly impacts a company's brand and reputation in the market. Bad press regarding companies that have been lackadaisical (lax) regarding protection, has sensitised consumers to do business with trusted companies. In surveys regarding Brand Perception, trust and transparency have been cited as key to a company's image.

Privacy laws & Regulatory fines for breaches: Data breaches, and its societal implications, have also led to the adoption of global regulations such as the GDPR and CCPA. Regulatory authorities, such as FTC (US), ICO (UK) and CNIL (France), have penalised large corporations with hefty fines in the past two years.

Indian landscape: India is about to get a new law passed for protecting personal data. This will be a landmark moment, because while such regulations existed in EU since 1995 and the US has had its privacy and consumer protection acts, India has never mandated a data protection-centric law. Experts tend to agree that such a full-fledged law for data privacy is long-overdue to become at par with the rest of the world, for the protection of sensitive details of Indians in our digital economy.

For companies and businesses operating out of India, this calls for a significant re-tuning of their data governance and data protection set up, with a clear regulatory demand for transparency and accountability in processing personal data. The coming regulatory penalties and actions will enforce harsh measures on non-compliant companies. But, the impact on a company's brand reputation, through exposure to the media, will, probably, be the single most important driver to its adoption of regulatory changes to safeguarding personal information.

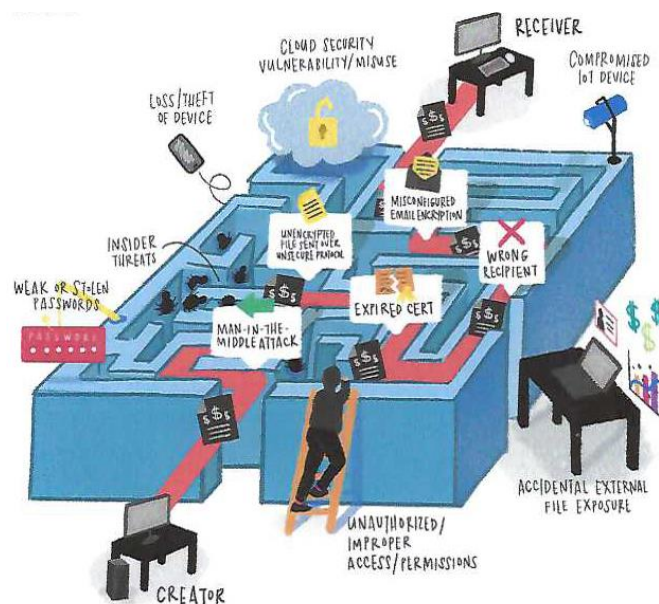
Upping the Ante in Data Security:

Traditional data security models involve safeguarding the data from various angles such as encryption, masking, data leakage prevention, identity control, access control and network security. However, as cyber-attacks and hackers get extremely sophisticated, traditional approaches associated with the current security fabric have become futile, and, mostly, lend themselves to control networks not data. The problems are: we can Trust and Verify the networks, applications, and users, through security

We at TechM think that the frequency and severity of breaches into data are compelling reasons to propose a rethink and re-model of our data-protection schemes to make it more granular and micro. Before we commence with our new orientation, we will highlight why macro controls, associated with the Perimeter, are weak and no longer enough.

“Trust”: Trust is a macro approach which is an outcome of a security paradigm premised on a “castle and moat” architecture. In this instance, it is really hard to gain access to the network for an outsider, but it, also, assumes that everyone is trusted.

The problems faced today:



It's time for a cutting-edge approach:

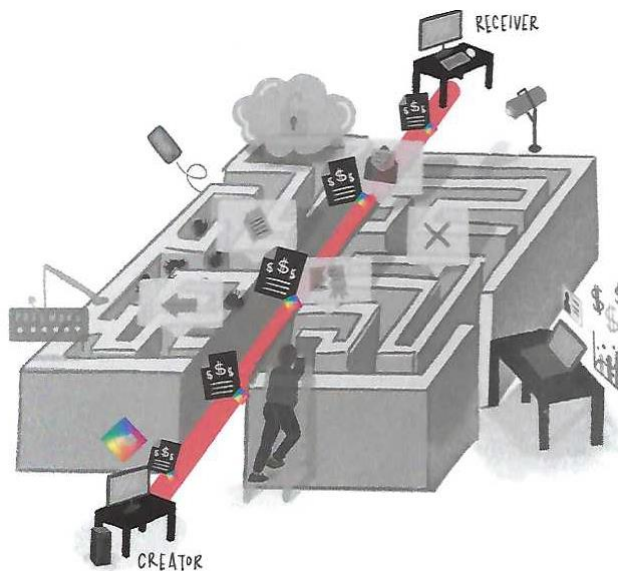
Emerging Technologies: TechM has been building a cybersecurity ecosystem for the latest protection schemes and to extend the existing security perimeter into the edge. One particular partner is asserting itself as the focal in the newly emerging Data-Centric paradigm and standard at the data-protection layer. It enables data to be controlled from its inception-to-expiration through an Intelligent Module infused onto a Data-File which embeds Governance (rules and policies),

Provenance and Protection (AES 256 etc.) into the data to imbue it with the abilities to Self-Protect and become Self-Aware.

This enables the data to be reactive and proactive to its surroundings and sets for itself a “micro-perimeter” that is agnostic to networks, applications, and infrastructure to defeat Zero-Day-Attacks, Advanced-Persistent-Threats and the Insiders and Super Users. This makes the deployment/implementation of a Zero-Trust Architecture possible as it safeguards data against its loss or theft. This, also, constitutes a defensive layer within the data to enable for Peer-to-Peer sharing of Data – whether between Machines, Applications, and Users and allow the data to cross-domains, siloes, and systems to make it Interoperable. The data becomes the carrier irrespective of the network or cloud topology.

As such, TechM has adopted the ‘zero-trust’ paradigm, which means do not trust anybody operating inside the network, even with an identity. Instead the zero-trust architecture involves micro-firewalls or micro-perimeters that help compartmentalise and protect the network from unscrupulous access. A user must authenticate across each IP address, servers, data and applications.

Tomorrow With TechM Approach:



This approach works to protect against both external parties as well as insiders who can no longer roam inside the network without re-authenticating at each step. It brings in stronger governance and works across technologies. It also prevents hacks from persisting for a prolonged period of time. Zero trust is commonly applied in more secure set ups such as military and certain government departments housing sensitive data. It is time to revisit its relevance to private and public sector companies, alike.

TechM Differentiation: What constitutes a breakthrough from the current convention of a Perimeter are means to infuse protection controls into the data at the micro level– data-file or at the packet level etc., so that even if data is out of the boundaries of a perimeter, it is still safeguarded and provides means of self-protection and compliance.

Effectively, such data even when hacked, cannot be used by malicious actors and prevents data breach and the penalties along with it. This approach is useful even when multiple users access the same data file and since it negates the need for replications which weakens the security.

Process Benefits: This help the companies because the protection can be adapted to build a new workflow depending on the data flow and data file movement or it be aligned to an existing workflow as well. For example, for the same bank transaction file, a customer or a customer service

representative may be only able to get ‘read’ access, a bank employee in the transaction processing team may have ‘read and modify’ access, while the system admin may have no access. Further, the access cannot be tweaked even when the data file is emailed, or replicated or is hacked, thanks to the inbuilt governance and provenance mechanisms.

People & Cost benefits: As the technology embeds data protection at the data itself, it simplifies the task of the CISO team and in fact less skilled professionals may be able to implement and monitor the data flow and take suitable actions. This will lead to cost savings.

Benefits to Governments:

A Data – Centric orientation coupled with a Zero-Trust security architecture provides absolute protection against Nation-State actors and their proxies. It exacts greater costs on the offense and turns the tide in favor of the defence! It, also, reduces dependencies on infrastructure and reliance on administrators, etc; which drops processing costs attributed to better and precise data-ingestion and reduction in data replications, which, effectively, will streamline need for data racks and personnel.

By adopting DevSecOps initiatives, any origination of data will carry Governance and Policies to enable monitoring and authentication within existing or new dataflows. This will provide perpetual line of sight into the data and ensure its compliance with regulation and protection requirements whether in flight, process, or rest. Shredding data, upon its digital utility, is also a possibility.

Meeting the Privacy Law requirements with TechM’s enhanced Data Protection Approaches

Regulations such as the GDPR, CCPA and upcoming India PDPA demand some key legal obligations from the companies processing personal data such as

- **Privacy by Design** – embedding data privacy from the design stages of a new product or system
- **Data Subject Access Rights** – individuals can control the data belonging to them and can demand access or deletion of their personal data from a company’s systems
- **Data Breach Management** – including notification to regulator – GDPR enforces a 72 hour period to notify the regulator from the time a company becomes aware of its data breach
- **Security of personal data** – security controls commensurate with the sensitivity of data and potential to harm the individual in case of a breach

Tech Mahindra will enable privacy and compliance for the stipulations above, through its Data Privacy Framework depicted below, in which data protection is a key pillar.

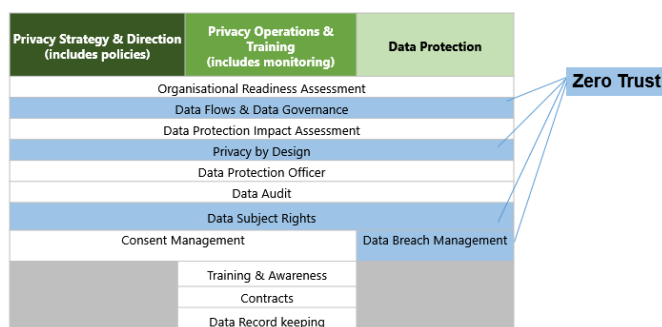
TechM Privacy Framework

Privacy Strategy & Direction (includes policies)	Privacy Operations & Training (includes monitoring)	Data Protection
	Organisational Readiness Assessment	
	Data Flows & Data Governance	
	Data Protection Impact Assessment	
	Privacy by Design	
	Data Protection Officer	
	Data Audit	
	Data Subject Rights	
	Consent Management	Data Breach Management
	Training & Awareness	
	Contracts	
	Data Record keeping	

How Zero-Trust Can Help Complying To Privacy Regulations:

- Privacy by Design:** All applications and networks are designed for need-based access
- Data flows & data governance:** Users are authenticated at every machine or server to reduce the risk as data travels from one point to another
- Data subject rights:** Due to re-authentication requirement, malicious actor cannot tamper with data under a ‘right to restrict’ request or with a data file sent under ‘right to access’

TechM Privacy Framework

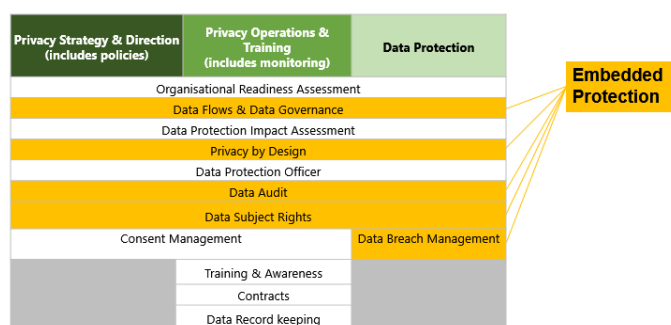


- D. **Data breach:** Negating anomalies associated with Zero-Day-Attacks, Advanced Persistent Threats, and stopping insiders from mal-intent are key benefits in adopting zero trust design

How Embedded Protection Can Help Complying To Privacy Regulations

- A. Data flow and Data Governance: Embedded governance and provenance allow for rules and policies to travel with the data to secure control and compliance whether In-Flight or at Rest. In essence, the data becomes independent and has a utility to it – across its lifecycle
- B. Privacy by design: Under this protection approach, even if data is exfiltrated or ransomed it remains inert and useless to the attacker. The Data remains in control of its originator and with no changes or deletions to it. This constitutes the cutting-edge to data privacy by design
- C. Data audit: Data Provenance provides audit and traceability capabilities to ensure irrefutability of the data and its integrity
- D. Data Subject Rights: Because of its interoperability, embedded protection can be used for providing the data files under right to data portability or right to access. A new service provider can easily use such data portability file for own workflow and to engage with the data subject, without being able to make unwarranted changes to the data

TechM Privacy Framework



- E. Data Breach Management: Embedded protection can address multiple scenarios of personal data breaches, irrespective of the type of data types, file formats, unstructured data etc.

Meeting the needs of Digital Enterprise & Digital Government

As a top 15 global company on Forbes Digital 100, TechM is deeply in tune with the changed realities of today's digital enterprises. Digital is no more a choice, but is now a core expectation from its customers, citizens, business partner ecosystem and employees. At the same time, being digital should not raise the risk profile of an enterprise or the government agency.

Following is a framework for the digital, data-secure enterprise and agency supported by TechM:

Digital Enterprise – Secure Business Enabled With TechM			
Strategy & Design Embed security by design & privacy by design principles	Digital Customer Share interoperable data files with customer or citizen with own 'micro-perimeter' & embedded protection	Intelligent Operations Design and manage cross-ecosystem workflows and data flows	Future Enterprise Globally connected employees, machines and mobile assets armed with self-protected, self-aware critical business data
Digital Insights Data flows boundlessly while providing irrefutability, audit trails and analytics			
Digital Foundation Protect data to thrive in the more tightly regulated digital economy with ease and confidence			

Conclusion:

We're into the third decade of the 21st century in which computing, and processing power of machines are enabling data to become dynamic. Owing to regulatory activism and newly established legal frameworks for data, the stakes in data protection by companies have never been higher with question marks over whether traditional broad-based security models still work.

It is time for the CISO to look beyond the old approaches and embrace a new Zero-Trust security model oriented at the Data-Layer. We think that our approach will become the standard for ensuring Privacy and Digital Trust since there are no trusted parties but trusted data!