BLOCKCHAIN: A PRIMER FOR INDIA

15th November 2019

By Anusha Madhusudhan

with inputs from Karan Saini and Mira Swaminathan

Edited and Reviewed by Elonnai Hickok, Siddharth Sonkar and Aayush Rathi

The Centre for Internet and Society, India
Table of Contents

BLOCKCHAIN: A PRIMER FOR INDIA 1

INTRODUCTION 3
   Used terms 4
   What is a blockchain? 7
   Technical considerations - how do they work? 8
   Distributed Ledger Technology and Blockchain 12
   What problems do blockchain technologies intend to solve? 13
   Types of Blockchains 16
      Public blockchains 16
      Private blockchains 18
      Consortium blockchains 18

INTERNATIONAL USE CASES OF BLOCKCHAIN TECHNOLOGY 20
   Decentralised Government 20
   Tax payments using cryptocurrency 20
      United States 21
   Notarization and related government registration services 23
      Dubai, United Arab Emirates 23
      Republic of Georgia 23
      Sweden 24
      Consortium of seven EU Member States 25
      United States 26
   Insurance Claim Management 27
   Financial Services 27
      Banking 28
INTRODUCTION

This paper aims to provide a comprehensive review of existing research and major debates surrounding Blockchain technology and its developments in select jurisdictions with a specific focus on India. In relation to the Indian context, the paper has sought to provide policy considerations and recommendations that could help inform a regulatory framework for Blockchain, both in respect of promulgating new and necessary rules as well as modifying existing rules and regulations to encompass utilities of the technology.

This paper tries to map and promote an understanding of the functioning of Blockchain and its diverse applications, domestic and international, potential and those already in use, for readers having varying degrees of engagement with the subject. This paper surveys scholarly pieces, articles, reports, research papers, policy briefs, books and other sources, analyses and synthesizes the information mapped while evaluating some sources and tracing progression in the field, generally.

The paper provides a readable landscape by systematically organizing the content into the following broad chapters – what blockchain is and how it works, the problems trying to be solved using this technology, differences between Distributed Ledger Technologies and Blockchains, types of blockchain, international and Indian use cases, an analysis of existing legal and regulatory frameworks governing blockchain technology in major jurisdictions and lastly, policy recommendations and considerations derived from other similar initiatives as well as international best practices, as adapted to the Indian context.

The information contained in relevant chapters of the paper is also indicative of the strengths and weaknesses of formally implementing this technology and may provide a background for further investigation and research.

Used terms

1. Blockchain - a shared, distributed ledger on which transactions are digitally recorded and linked together so that they provide the entire history or provenance of an asset. A transaction is added to the blockchain only after it
has been validated using a consensus protocol (see below), which ensures it is the only version of the truth. Each record is also encrypted to provide an extra layer of security. Blockchain is said to be “immutable” because the records are difficult to change and, transparent because all participants to a trade have access to the same version of the truth. ¹

2. Hashing – A hashing algorithm is a computational function that condenses input data into a fixed size. The result of the computation is the output called a hash or a hash value. Hashes identify, compare or run calculations against files and strings of data. Typically, the program first computes a hash and then compares the values to the original files.² In blockchain, hashes are used to represent the blockchain in its current state.

3. Mining - Mining, in the context of blockchain technology, is the process of adding transactions to the distributed public ledger of existing transactions, which is the blockchain. Mining is used to set the history of transactions in a way that is computationally impractical to modify by any one entity.³

4. P2P network - In a P2P network, the "peers" (sometimes called nodes) are computer systems which are connected to each other via the internet. Files can be shared directly between systems on the network without the need of a central server. Each peer is equal in authority, gives computing resources to the network (i.e. processing power, disk storage, or bandwidth) in order to use the network and no single party owns the network.⁴

5. Consensus protocol and algorithm - A consensus algorithm may be defined as the mechanism through which a blockchain network reaches consensus. Decentralized blockchains are built as distributed systems and since they do not rely on a central authority, the distributed nodes need to agree on the validity of the transactions. Protocols are the primary rules of a blockchain and the algorithms are the mechanisms through which these rules will be followed.⁵

6. Proof of Concept - Proof of Concept is a process of determining whether a (Blockchain) project idea would be feasible in a real-world situation. It is an exercise to test the design idea or assumption. While a POC shows that a

¹ Nigel Gopie, What are smart contracts on blockchain?, 2 July 2018
² Emily Kotow, What is Blockchain Hashing?, 26 February, 2019
⁴ See generally Mary Thibodeau, Peer to Peer Networks Defined, April 11, 2019
⁵ Binance Academy, What Is a Blockchain Consensus Algorithm?, 28 October 2019, recoverable at https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm
product or feature can be developed, a prototype shows how it will be developed.\(^6\)

7. Proof of Authority - PoA is a consensus mechanism for blockchain in which consensus is achieved by referring to a list of validators (authorities). Validators are a group of accounts/nodes that are allowed to participate in the consensus; they validate the transactions and blocks.\(^7\)

8. Smart contract - Smart contracts are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met. At the most basic level, they are programs that run as they have been set up to run by the people who developed them. The benefits of smart contracts are most apparent in business collaborations, in which they are typically used to enforce some type of agreement so that all participants can be certain of the outcome without an intermediary's involvement.\(^8\)

9. Cryptocurrency - A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that only exists online. Cryptocurrencies use cryptography to verify and secure transactions. Cryptography allows for a particular digital token to be generated, stored, and transacted securely and, typically, anonymously. Alongside this important “crypto” feature of these currencies is a common commitment to decentralization.\(^9\)

What is a blockchain?

There is no universal definition of a blockchain because there is a widespread disagreement over which attributes are essential in order to constitute a blockchain.

It is generally understood that a blockchain is a digital distributed ledger having 3 key attributes\(^10\):

1. **Recordation**: Where stored information is time-stamped.
2. **Transparency**: Depending on the type of blockchain, anyone can see the ledger of transactions.

---

\(^6\) See generally, Muthu Singaram, Prathistha Jain, *What is the Difference between Proof of Concept and Prototype?*, 13 January 2018


\(^8\) Supra., at n.1

\(^9\) Infra., at n.53

\(^10\) Lisk Academy, *What is blockchain?* https://lisk.io/academy/blockchain-basics/what-is-blockchain
3. **Decentralization:** The ledger exists on multiple computers.

In simpler terms, Blockchain is a “public registry of who owns what and who transacts what: The transactions are secured through cryptography. Over time, the transaction history gets locked in blocks of data that are then cryptographically linked together and secured. This creates an immutable, un-forgeable record of all transactions across the network. This record is then replicated on every computer that uses the network.”  

Once data is recorded in a blockchain, it is extremely difficult to alter. For example, although data stored on a blockchain is considered rather immutable, a 51% attack is an exception where someone controls the majority of mining power on a Proof-of-Work blockchain network. This means that the majority block verifier can prevent other users from mining and reverse transactions. However, 51% attacks have generally been considered undesirable and unprofitable option to take funds, as it would require a massive amount of computing power.  

---

**Technical considerations – how do they work?**  

As the name indicates, a blockchain is a chain of blocks that contains information. This mechanism was originally explained in 1991 when it was intended to timestamp digital documents, attempting to make it practically impossible to backdate them or tamper with them.  

Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size. It allows individuals to independently take input data, hash that data, and derive the same result – proving that there was no change in the data. Even the smallest change to the input (e.g., changing a single bit) should result in a different output digest. In blockchain, hashes are used to represent the current state of a blockchain. Normally, each block contains the data it is recording, as well as timestamps of when that information was recorded. It will also include a digital signature linked to the account that made the recording and a ‘unique’ identifying...  

---

11 Bettina Warburg, *How the blockchain technology will radically transform the economy*, retrievable at https://www.youtube.com/watch?v=RplnSVTzvnU  
13 See generally, Xavier Decuyper, *How does a blockchain work – Simply Explained*, 13 November 2017  
15 Supra., at n.11, p.7 check
link (the hash) to the previous block in the chain. It is this link that makes it difficult for information to be altered or for a block to be inserted between two existing blocks. In order to do so all following blocks would need to be edited too. As a result, each block may be thought of as strengthening the previous block and the security of the entire blockchain.

Thus, each block contains data, its own hash (hash of that block) and the hash of the previous block. Data that is stored depends on the type of blockchain. The bitcoin blockchain for example, stores details of a transaction such as the sender, recipient and the number of coins transferred. A block’s hash is comparable to a fingerprint and is mostly unique. While there have been some hash functions that are vulnerable to cryptographic attacks through which it is possible to produce non-unique hashes (i.e., two different inputs resulting in the same output), modern technologies, for the most, aren’t susceptible to this. A block’s hash identifies the block and all its contents. Once a block is created its hash is calculated. Changing something inside the block will cause the hash to change. Thus, hashes are useful when you want to detect any changes made to the blocks. The third element inside each block is the hash of the previous block. This effectively creates a chain of blocks and a system of security.

For example, in a chain of three blocks, each block has a hash and the hash of the previous block. Block three points to block two and block two points to the first block. The first block is the genesis block because it cannot point to a prior block. If the second block is tampered with, its hash changes and this will make the third and all following blocks invalid because they longer store a valid hash of the previous block.

Changing a single block will make all following blocks invalid. However, using hashes by themselves, may not be sufficient to prevent tampering. Modern computer systems are extremely quick and calculate thousands of hashes per second. Effectively, it may be possible to tamper with a block and recalculate all the subsequent hashes and make the blockchain valid again. To mitigate this, there exists proof of work.¹⁶

This mechanism slows down the creation of new blocks. In the case of bitcoin, it takes around ten minutes to calculate the required PoW and add a new block to the

---

chain. If one block is tampered with, the PoW must be calculated for all the following blocks. 17

The security of blockchain comes the creative use of hashing and PoW. Another way by which blockchains secure themselves is by being distributed. Instead of using a central entity to manage the chain, they use a peer-to-peer system and everyone is allowed to join the chain. The blockchain uses a special kind of network called “peer-to-peer network” (P2P) which partitions its entire workload between participants, who are all equally privileged, called “peers”. There is no longer one central server, now there are several distributed and decentralized peers. 18

Torrenting is a major use of the peer-to-peer network where multiple users can connect and share files; a user is able to not only download the file from the direct source but also from other users of the same torrent. Each of the peers acts as a mini-server. Because they do not rely exclusively on central servers, P2P networks are thought to both scale better and be more resilient than client-server networks in case of failures or traffic. 19

When a person joins this network, he or she gets a full copy of the blockchain. The node can use this to verify that everything is in order. A node is a device on a blockchain network, that is in essence the foundation of the technology, allowing it to function and survive. Nodes are distributed across a widespread network and carry out a variety of tasks. A node can be any active electronic device, including a computer, phone or even a printer, as long as it is connected to the internet and has an IP address. The role of a node is to support the network by maintaining a copy of a blockchain and, in some cases, to process transactions. 20

When someone creates a new block, that block is sent to everyone on the network. Each node then verifies the block to ensure that it hasn’t been tampered with. Then, each node adds this block to their blockchain. All the nodes in this network create consensus. They agree on which blocks are valid and which aren’t. Blocks that have been tampered with should be rejected by other nodes in the network. 21

Mining is the process of adding transactions to the distributed public ledger of existing transactions, which is itself the blockchain. Miners compete (for a reward either as cryptocurrencies or transaction fees) to solve a mathematical problem

---

19 Bradley Mitchell, An introduction to peer-to-peer networks, 26 September 2019
20 Id. at n.7 (How does Blockchain work?)
21 Kiana Danial, What is a Blockchain, and How Does It Work?, recoverable at https://www.dummies.com/personal-finance/investing/what-is-a-blockchain-and-how-does-it-work/
based on the cryptographic hash algorithm. The solution found is the PoW. This proof proves that a miner did solve the problem. When a block is 'solved', the transactions contained are considered confirmed.22

**Distributed Ledger Technology and Blockchain**

A distributed ledger is a database of replicated, shared, and synchronized digital data that is spread across multiple sites (or nodes) in a network. Rather than having a central administrator like a traditional database, distributed ledgers have a system of synchronized databases that provide an auditable history of information and are visible to anyone within the network. Each node replicates and saves an identical copy of the ledger. Updates to the ledger are constructed and recorded by each node. The nodes then vote on these updates to ensure that the majority agrees with the conclusion reached. This voting and agreement on one copy of the ledger is called consensus, and is conducted automatically by a consensus algorithm In broad terms, is a means to ensure the transactions written to nodes across a network remain in sync, are immutable, and prevent the network from many types of attack. To achieve these objectives, the process of consensus follows four steps:

1. Each node creates the transactions it wants to record.
2. The data is shared between the nodes (an obvious and critical step).
3. Consensus is established on the order of valid transactions.
4. Nodes update their transactions to reflect the consensus result.

Once consensus has been reached, the distributed ledger updates itself and the latest, agreed-upon version of the ledger is saved on each node separately. Blockchains are one form of distributed ledger technology. Therefore, although distributed ledger technology and blockchain share the same conceptual origin and purpose — a decentralized database or log of records, they are not exactly the same. A blockchain is a specific type of distributed ledger with a distinct set of features or operational processes. Unlike other distributed ledgers, blockchains package transactions or sets of data into the cryptographic hash-linked blocks in a sequential chain. Distributed ledgers do not require such a chain.23

---

22 Damien Cosset, *Blockchain: What is Mining?*, 5 January 2018
23 See generally, Anthony Stevens, Distributed ledger consensus explained, 29 April 2018, and Ray at n.23
In conclusion, it can be said that every blockchain is a distributed ledger, but not every distributed ledger is a blockchain, although each of these concepts requires decentralization and consensus among nodes.  

What problems do blockchain technologies intend to solve?

Blockchain initially set out to test the transfer a digital asset between two peers without an intermediary.

While there are many applications of this transfer, it is most often looked at it in the context of money. Imagine a person is selling a bike online. He/She does not actually know the person who is buying the bike, so the person has no way of knowing if the buyer actually has the money to pay for it. He has to trust an intermediary like PayPal for this information. PayPal is crucial to the transaction because it verifies what the seller cannot – whether the buyer has enough money in their bank account to make the purchase.

Block chain enthusiasts support the view that this new technology eliminates the need for trust between parties that don’t know each other and cannot test the veracity of each others’ claims and assertions.

It is argued that in blockchain, cryptography completely replaces third parties as the governor of trust. Participants on the network run complex consensus protocols to unanimously and securely agree on what should be added to the distributed ledger of blockchain, whilst also ensuring its integrity at all times. As it is these “failsafe” protocols providing the basis for trust, it allows for the removal of middlemen and, as a result, decrease in the cost of transacting, which is however, excluding the unsustainable nature of the energy consumed by computationally intensive processes of mining/verification. While decentralization seems to allow for scaling the number of nodes of a blockchain network making it more resilient to attacks by bad actors, by increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain could be reduced, but some experts opine that despite this, blockchains are ‘incredibly inefficient,’ and that “it's worth paying the cost when you need the decentralization, but it's not when you don't.”

---

24 Shaan Ray, *The Difference Between Blockchains & Distributed Ledger Technology*, 20 February 2018
25 Joshua Holley, *Blockchain was made to solve 1 problem. Here’s what that is*, 12 February 2018
26 Id. at n.7 (Why is Blockchain trustless?)
27 Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone, *Blockchain Technology Overview*, (United States Department of Commerce)National Institute of Standards and Technology Internal Report 8202, October 2018, pp.11, 43
Others argue that this looks at “trust” in a narrow sense, interpreting it to mean “verification” only. Additionally, these non-supporters also argue that any blockchain system will have to coexist with other, more conventional systems and what blockchain does is shift some of the trust in people and institutions to trust in technology, not eliminating the need for trust per se. It is also seen as a task to test how forthcoming communities are when they are required to trust cryptography, protocols, software, and the blockchain network, absolutely, because they’re often single points of failure.  

The first known ledgers date back 5,000 to 10,000 years to Mesopotamia, where simple clay tokens and stone tablets were used as markers of transactions. They were a centralized form of record keeping that helped people keep track of the price of barley, who bought the barley from whom, or who owned or purchased a piece of land. Over time, such ledgers allowed people to gauge who could be trusted, leading to the emergence of reputation, credit, and long-distance trade. Moreover, they helped resolve disputes about goods sold and money owed, recording and verifying transactions and terms of engagement.

The earliest translatable advantages of these ledgers thus included establishing a history of ownership and making supply chains more efficient and transparent.

**Types of Blockchains**

There are three primary forms of blockchains -

1. **Public blockchains**

   Their consensus algorithms (PoW) are open source and not permissioned. Anyone can participate, without permission. Anyone can download the code and start running a public node on their local device, validating transactions in the network, thus participating in the consensus process – the process for

---

See also, James Vincent, *Bitcoin consumes more energy than Switzerland, according to new estimate; though researchers acknowledge that reliable estimates are ‘rare’*, 4 July 2019

28 Bruce Schneier, *There's no good reason to trust blockchain technology*, 6 February 2019


determining what blocks get added to the chain and what the current state is. Anyone in the world can send transactions through the network and expect to see them included in the blockchain if they are valid. Anyone can read transactions on the public block explorer (an online block chain browser).

As a substitute for centralized or quasi-centralized trust, public blockchains are secured by certain incentives and cryptographic verification using mechanisms such as proof of work following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. The study of these incentives that secure the blockchain system is called cryptoeconomics. These blockchains are generally considered to be “fully decentralized”.

An example would be the Bitcoin protocol, which is open source so anyone could take the protocol, modify the code and start their own version of P2P money or other projects beyond the use case of P2P money.

Blockchain proponents argue that this creates potential to disrupt current business models through disintermediation and reduced infrastructure costs because of non-requirement to maintain servers or system administrators which radically reduces the costs of creating and running decentralized applications.

Others argue that because blockchain has a distributed architecture, it requires multiple processing nodes scattered across multiple participants, both increasing overall costs per transaction while also leading to issues of scalability and performance. Further, maintaining a distributed ledger, especially for cryptocurrencies, results in increased electricity consumption due to the additional units of energy required by high-end video cards. A report published by The Verge estimates that the global Bitcoin network consumes more energy than Switzerland.

2. Private blockchains

In this case, participants need consent to join the networks, transactions are private and are only available to ecosystem participants that have been given

---

32 Id., at n.12
33 Vitalik Buterin, On Public and Private Blockchains, August 6, 2015
34 Hussein Elasrag, Blockchains for Islamic finance: Obstacles & Challenges, 6 March 2019 at p.4
35 Jason Bloomberg, Don't Let Blockchain Cost Savings Hype Fool You, 24 February 2018
36 Bitcoin consumes more energy than Switzerland, according to new estimate, July 4 2019 retrievable at https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison
permission to join the network thus making them more centralized than public blockchains.\(^{37}\)

The distinction between public and private blockchains implicates who is able to write data onto that blockchain or onto that ledger and who cannot. There is also a secondary classification to be made between open and closed blockchain which implicates who's able to read that data and who cannot. If the chain is closed, transactions are not publicly viewable (transparent) and only selected nodes can access the ledger.\(^{38}\)

Accordingly, there may be blockchains that are public and open, public and closed, private and open, or private and closed.

A fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent.\(^{39}\)

### 3. Consortium blockchains

A consortium blockchain is a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants.\(^{40}\)

---

**TAKE-AWAYS**

A distributed ledger is a database that is spread across several nodes or computing devices. Each node replicates and saves an identical copy of the ledger. Each participant node of the network updates itself independently. Updates to the ledger are independently constructed and recorded by each node.

Not all distributed ledgers employ a chain of blocks to provide a secure and valid distributed consensus. The structure of the blockchain makes it distinct from other kinds of distributed ledgers. Data on a blockchain is grouped together and organized in blocks. The blocks are then linked to one another and secured using cryptography. This creates a practically immutable, unforgeable record of all transactions across the network.
INTERNATIONAL USE CASES OF BLOCKCHAIN TECHNOLOGY

This section surveys a diverse array of blockchain use cases globally. Irrespective of whether these use-cases are universally implementable or scalable, surveying a diverse set of Blockchain applications will be useful in understanding their potential advantages and drawbacks.

1. Decentralised Government

Administrative timestamps validate the exact time an action is taking place; events such as birth and death to when citizens receive new identity documentation, certificates of education or exchanging ownership titles. Much of these processes are done either on isolated databases or via brick-and-mortar bureaucracy, which is prone to error. The encrypted nature of the data stored on a blockchain may make it relatively more probable that these recordings will remain as they are and only be visible to the owner or permitted parties. This method of information storing could offer a relatively more responsive and user-friendly governmental interaction as Blockchain-backed governmental bodies could process transactions with multiple citizens at the same time, such as registering a vehicle or processing social security documents from their homes.  

Tax payments using cryptocurrency

The beginnings of mainstream blockchain use cases in ushering a new era of a decentralized government, was spearheaded by Europe's self-styled ‘CryptoPolis’ - Chiasso, Switzerland. Along with its sister city, Zug, often referred to as ‘Crypto Valley’, this community on the Swiss-Italian border has recently allowed its residents to use cryptocurrency to make small tax payments. While this option can be considered more a novelty, Chiasso's crypto-friendly fiscal policy provides a glimpse of how this technology can be implemented to bolster innovation and possible economic growth.

Having lost tax revenues from the diminishing banking sector in the wake of the financial crisis, Chiasso has been looking for replacement industries, explained Umberto Balzaretti, head of the town's administration. Local officials have sought to brand the municipality as

41 Id at n.7 (Use cases)
“CryptoPolis” in a bid to attract cryptocurrency start-ups. Chiasso's mayor is reported to have met with numerous cryptocurrency entrepreneurs in recent months, with the mayor claiming that eight start-ups have recently established headquarters in the municipality. Chiasso's government announced measures intended to foster innovation in its local cryptocurrency industry, including the development of “in-depth courses in upper secondary schools” designed to bolster cryptocurrency literacy among students.42

United States

Voatz is a Boston-based mobile voting platform that runs on blockchain. The company states that an encrypted biometric security system makes it secure to vote on a mobile device from anywhere in the world without fear of hacking or data corruption. West Virginia was one of the first states to use the company's platform to collect votes from eligible service people and travelers abroad during elections. Follow My Vote is another Virginia-based secure online voting platform using an open-source virtual blockchain ballot box. The technology claims to decreases spending on physical ballots and can be accessed via any device and implements the end-to-end tools in order to provide safety and confidence in the voting process.43

Voatz points to a few potential advantages of blockchain voting technology, such as voters being able to verify that their vote was cast as intended and detect tampering, governments and independent outside parties being able to confirm the vote results stored on the blockchain for better election transparency and practical difficulties in alteration of results without being able to hack a central system. However, skeptics are abundant, even among the digitally savvy. Princeton cryptography professor Matthew Green has a list of concerns about blockchain voting technology, the first being that it relies on computers in the first place. Blockchain voting also brings new twists to the age-old problem of voter coercion: "If I can verify that my vote was correctly recorded, then your local mob boss can also use my receipt to verify the same thing," he says. The National Academies of Sciences, Engineering, and Medicine -- a prestigious group of top researchers in the US -- also said no to blockchain voting in a September report on voting technology. "While the

42 Matthew Allen, Chiasso accepts tax payments in bitcoin, 8 September 2017 and Samuel Haig, Chiasso, Switzerland Municipality to Allow Citizens to Pay Taxes in Bitcoin, 10 September 2017
43 Sam Daley, 25 Blockchain Applications & Real-World Use Cases Disrupting The Status Quo, 5 December 2018
notion of using a blockchain as an immutable ballot box may seem promising, blockchain technology does little to solve the fundamental security issues of elections, and indeed, blockchains introduce additional security vulnerabilities," the report said. "In particular, if malware on a voter's device alters a vote before it ever reaches a blockchain, the immutability of the blockchain fails to provide the desired integrity, and the voter may never know of the alteration."\(^{45}\)

**Notarization and related government registration services**

a. **Dubai, United Arab Emirates**

Dubai is preparing to transfer their entire governmental infrastructure and economy on a blockchain. This metropolis is eager to use the technology to fully transfer and process complex government transactions on a ledger, or to use smart contracts (see used terms) to reduce clunky documentation of movement of goods within the state.

b. **Republic of Georgia**

As property titles become increasingly susceptible to fraud and labour intensive to administer, in 2016, The Republic of Georgia entered a deal with the Bitfury Group to develop a blockchain system for property titles.\(^{46}\) Noting that the Georgian government “like[s] how the work was done and how easy blockchain is implementable in the existing system,” Bitfury CEO Valery Vavilov has stated that the changes were all made on the back end, and the only difference for Georgian citizens was that they can now check if a land title is legitimate (if it’s been entered into the system). Calling the work so far a “phase one, beta stage” and declaring that the software will be “fully operational” this year, he said, “The big goal is to move [the process] to smartphones, so people can use it 24/7 and all transactions are secured, transferrable and accountable.” Eventually, Bitfury plans to also help put notary services and smart contracts (programmable contracts that self-execute when certain conditions are met) for services

---

\(^{44}\) See also, How secure is blockchain really?, Mike Orcutt, MIT Technology Review, 25 April 2018

\(^{45}\) Stephen Shankland, *No, blockchain isn't the answer to our voting system woes*, November 5, 2018

\(^{46}\) *Ibid.*
such as escrow in Georgia onto blockchains. While many of the technology’s enthusiasts tout the potential for blockchain to improve notary services, processes for verifying the accuracy of information that gets placed on the ledger have yet to be established. It is also noted that Georgia’s property registration systems were ranked third best in the world by the World Bank, which bodes well for any future notary products there.  


48 Marcell Nimfuehr, *Blockchain application land register: Georgia and Sweden leading*, 3 December 2017

**c. Sweden**

The Swedish Land Registration Authority completed a successful pilot to bring the Swedish land register onto the Blockchain. Sweden does not necessarily see this as a tool to fight corruption but as a means to satisfy a very future-oriented motivation for Sweden’s youth who want to digitize everything:  

48

**d. Consortium of seven EU Member States**

Cyprus, France, Greece, Italy, Malta, Portugal and Spain – collectively referred to as the Southern European Countries – have agreed to work together to promote distributed ledger technologies, 5G connectivity, Internet of Things and artificial intelligence; in order to boost the economies of southern Europe. The joint declaration on distributed ledger technologies lays out the Southern European Countries’ intention to become world leaders in emerging technologies. The signatories pledge to work towards expanding their “digital ecosystem” through investment in research and innovation, with the potential to develop collaborative cross-border distributed ledger technologies projects.

The joint declaration on distributed ledger technologies states: “As a technology based on trust, we see Distributed Ledger Technologies as being a potential game changer using – inter alia smart contracts in areas such as certifying product origin, education, transport, mobility, shipping, land registry, customs, company registry, and healthcare amongst others to transform the way that such services are delivered. This can result not only in the enhancement of e-government services
but also increased transparency and reduced administrative burdens, better customs collection and better access to public information.”

e. United States

The Delaware Blockchain Initiative aims to create an appropriate legal infrastructure for distributed ledger shares to increase efficiency and speed of incorporation services. This is important, given that half of all publicly traded companies in the US and 65% of the Fortune 500 are incorporated in Delaware. The 2017 Amendments to the Delaware General Corporate Law permit corporate records, including stock ledgers, to be created and maintained “on a blockchain to better track and verify stock ownership, and improve transaction time and proxy voting.” The Delaware Division of Corporations may cryptographically “sign” and transfer to new corporations all validly-authorized shares, enabling those shares to be tracked on a blockchain.

f. Denmark

Vehicle Wallet is a partnership between the payment service provider and the Danish Tax Administration. It is a supply chain management tool where data concerning the car is saved in one distributed ledger and creates one agreed and shared record of the vehicle history as it is transferred across the supply chain. This reduces risks for buyers and sellers, and ensures the Danish Government receives proper taxes.

2. Insurance Claim Management

Distributed infrastructure technology could significantly improve the claims management process. Currently, claims management is a cumbersome process for insurers, involving different parties who exchange lots of paper-based information in handling a claim. This is often centrally coordinated by the insurer itself, resulting in a highly administrative back-office process. A distributed ledger could enable the insurer and various third parties involved in the process to easily and instantly access and update relevant information

---

49 Joint declaration on distributed ledger technologies signed by seven Member States of the European Union, 7th December 2018, recoverable at https://www.governmenteuropa.eu/joint-declaration-on-distributed-ledger-technologies/91423/

50 My Say, Why The Delaware Blockchain Initiative Matters To All Dealmakers, 20 September 2017

51 Organisation for Economic Co-operation and Development-Observatory of Public Sector Innovation (OECD-OPSI), Blockchain and its uses in the public sector, 20 June 2018, at p.22
regarding a claim (e.g., claim forms, evidence, police reports, third-party expertise reports).\textsuperscript{52}

3. Financial Services

With multiple parties in multiple jurisdictions exchanging multiple physical goods and documents, trade finance — and with it, supply chain management — can be a very complex process. When dealing in cross-border transactions and relationships, the burden on a trusted centralized party can be significant. Consequently, a number of vendors and financial institutions are considering distributed infrastructure as a solution to manage the tracking of products and their associated financing, payment and documentation. With the ability for any party in the chain to record its activity and for any other party to verify the activity, the technology may allow for more efficient, less burdensome trade finance and supply chain management for buyers, suppliers, transporters and financiers.\textsuperscript{53}

1. Derivatives

They are financial instruments that derive value from underlying assets, which could include stocks, bonds, commodities or even interest rates. The White Paper which conceptualized Ethereum, an alternative to Bitcoin, called financial derivatives “the most common application of a ‘smart contract’”. Various industry experts have predicted that blockchain technology can lead to more customized financial engineering, “enabling financiers to customize derivatives consisting of individual cash flows to meet precise needs in terms of timing and credit risk.” This engineering can be done using specialized blockchain derivatives players.\textsuperscript{54}

Banking

Several financial institutions, investment funds, and financial infrastructure bodies have taken notice of the potential impact of blockchain technology on clearing and settlement. Two consortiums R3 and Enterprise Ethereum Alliance together boast several leading global financial institutions.

Investors in blockchain startups in the clearing and settlement space include SV Angel, Citigroup, JP Morgan, and Santander. The Depository Trust &

\textsuperscript{52} Ernst and Young, \textit{Implementing blockchains and distributed infrastructure}, p 6.

\textsuperscript{53} \textit{Ibid}, pp. 5-6

\textsuperscript{54} Nishith Desai Associates, \textit{The Blockchain - Industry Applications and Legal Perspectives}, November 2018, p. 10
Clearing Corporation (DTCC), the premier post-trade market infrastructure organization in global finance, announced a project to deploy blockchain technology for the clearing and settlement of a huge swathe of repurchase agreement transactions. Also, seven major European financial institutions, including BNP Paribas Securities, announced a venture called ‘Liquidshare’ to explore the development of a post-trade blockchain-based infrastructure for small and medium enterprises in Europe.\(^{55}\)

For example, last year Barclays placed themselves at the forefront of adopting Blockchain Technology by implementing the security and transparency aspects of blockchain technology into their transaction processes. This multinational bank did so by announcing a first of its kind, blockchain-backed credit transaction between Ornua and Seychelles Trading Company. It included the first trade documentation to be encrypted and managed on a blockchain network. Goldman Sachs announced that they are setting up a cryptocurrency trading operation. Similarly, US financial firms CME Group, Cantor Fitzgerald and CBOE have also listed cryptocurrencies.\(^{56}\)

**International payments**

Most international payments systems pass a payment through multiple banks en route to the final destination. While this provides important security benefits, it also makes the payments expensive, slow, and uncertain—the amount of money that will arrive on the other end is unknown until the payment actually shows up. Blockchain-powered cross-border payments could address many of these shortcomings, and many banks are already using blockchain in this way. More than a hundred banks have signed up with XCurrent, the blockchain-based messaging system developed by the fintech firm Ripple. XCurrent allows banks to coordinate the transfer of money within seconds.\(^{57}\)

**Clearing and Settlement**

One of the best-known examples of the restructuring of the loan and securities market is the Australian Securities Exchange, which aims

---

\(^{55}\) Ibid, at p.8  
\(^{56}\) Id. at n.7 (Blockchain in banking)  
\(^{57}\) Benjamin Karsch, *Five use cases for blockchain in financial services*, 10 October 2018
to shift much of its post-trade clearing and settlement on to a blockchain system. The project is being implemented by Digital Asset Holdings, the company led by Blythe Masters, the former senior executive with JPMorgan Chase. In the US, DTCC is working with IBM, R3 and Axoni to shift post-trade clearing of single-name credit default swaps on to a blockchain system by the end of next year.  

Securities

Nasdaq unveiled a blockchain-based system for its Nasdaq Private Market, which connects institutional investors with companies that are not yet listed on a public exchange. The new system offers electronic services to facilitate the issuance, transfer, and management of private company securities. The firm has even named one of its vice presidents its Blockchain Technology Evangelist. Numerous other exchanges and banks around the world, including the London Stock Exchange, CME Group, Societe Generale, and UBS, have formed the Post Trade Distributed Ledger Working Group to investigate how blockchain technology can be used to enhance clearing, settlement, and reporting of trades. Citigroup, Barclays, and Deutsche Bank are among the banks investigating incorporating blockchain into their payments system.

Anti money laundering and know your customer

The Singapore government is exploring the possibility of leveraging Blockchain technology and DLT to combat money laundering and terrorism financing. The monetary authority of Singapore launched project Ubin in 2016 with a consortium of banks to develop software for decentralized interbank payments and settlement. It has since then, released the code to the public.

The Singapore Infocomm Media Development Authority has also developed a Know Your Customer (KYC) blockchain in cooperation with a group of banks. Some individual banks have also partnered with outside providers to develop their blockchain and AI solutions, particularly in AML compliance.

---

58 Financial Times, The Future of FinTech: five ways banks are using blockchain, retrievable at https://www.ft.com/content/615b3bd8-97a9-11e7-a652-cde3f882dd7b
59 Haskell Garfinkel and Jeremy Drane, PricewaterhouseCoopers, Fintech Q&A; What is blockchain? P. 3
4. Cryptocurrencies

A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that only exists online. Cryptocurrencies use cryptography to verify and secure transactions. Cryptography allows for a particular digital token to be generated, stored, and transacted securely and, typically, anonymously. Alongside this important “crypto” feature of these currencies is a common commitment to decentralization; cryptocurrencies are typically developed as code by teams who build in mechanisms for issuance (often, although not always, through the process of mining).

Most crypto assets fall under one of the following categories:

- Payment currencies - these assets are mainly for payments. For example, they can be used to pay for goods or services, cash out from digital currencies to local currencies etc. While every digital asset can theoretically be used to pay for things, merchant adoption or acceptance by providers of goods and services is more widespread for Payment Currencies. Bitcoin is the first successful attempt at implementing digital cash without the need for a central party like a government to oversee it. It is now 10 years old and now has several other similar competing coins such as Litecoin, Dogecoin, Bitcoin cash etc. In Bitcoin consider there are 2 people, person A having 20 Bitcoin and person B having 30 Bitcoin. If A sends B 10 Bitcoin then the transactions result would be A-10 and B+10 which means A will now have 10 Bitcoin and B will have 30 Bitcoin. All of bitcoin transactions are really simple plus and minuses. It is simple yet powerful if your only goal is to track transfer of money.

- Blockchain economies - these platforms allow for creation of one’s own digital assets (usually referred to as tokens), decentralized applications (Dapps), etc. on their platform. Therefore, blockchain platforms become their own “Blockchain Economies” with different assets, applications, and more. Ethereum (ETH) would be an example. Ethereum can be best

---

61 Id. at n.7 (Cryptocurrencies)
62 Prableen Bajpai, The 10 most important cryptocurrencies other than Bitcoin, 28 May 2019
63 JP Richardson and Daniel Castagnoli, What are the different types of cryptocurrencies, Founders of Exodus, a web application to “Secure, Manage, and Exchange blockchain assets in one wallet”
64 Moresh Kokane, A brief summary of Blockchain, cryptocurrency and various token types, 6 November, 2018
understood as a set of lego blocks using which interesting things can be built on top of its Blockchain framework. Ethereum goes beyond single plus-minus transactions based state changes. With Ethereum, there is scope for more than one step and operators beyond simple plus and minus. So instead of just A-10 and B+10, it is possible to encompass a series of steps such as:

\[ A^3 \]
\[ A/2 \]
\[ A^5 \]

Before the transaction is complete, state changes can be programmed. These calculations can get complex and someone has to pay for the computing power. This is paid using GAS (which is 1/100,000 of one Ether).

This GAS is the fuel that powers smart contracts on the Ethereum Blockchain.

Ethereum goes beyond what Bitcoin does by adding the programming capability in it.

- Privacy coins - Some digital assets are created with a focus on privacy. In Privacy Coin transactions, only the sender and receiver know the number of coins transacted. Also, the balance of a Privacy Coin wallet address is only known by the owner of the wallet. This is in contrast to blockchains like those of Bitcoin, which show transaction amounts for each transaction as well as wallet address balances.

Crypto assets like ZCash (ZEC), Monero (XMR), PIVX (PIVX), and so on are examples of Privacy Coins.

- Utility tokens - They are digital tokens that are used for a blockchain-based product or service. They run on a blockchain platform. An example of a Utility Token is Golem (GNT). Golem is a platform where users can pay GNT to rent computing power for memory-intensive tasks.

- Stablecoins - These assets are popular among regular traders, as they always have the same price (or aim to), unlike other digital assets, which can fluctuate greatly in value. For example, if a trader thinks that an asset is going to lose value soon, they could sell the asset for a stablecoin to prevent financial loss. Different stablecoins follow different methods to maintain a stable price.

---

65 Ibid.
66 https://support.exodus.io/article/1084-what-are-the-different-types-of-cryptocurrency
Pioneered by Bitcoin, cryptocurrency transfer apps are especially popular in finance for the money and time it is expected to save financial companies of all sizes.

By eliminating bureaucratic red tape, making ledger systems real-time and reducing third-party fees, it is estimated that blockchain can save the largest banks $8-$12 billion a year. Gamers looking to buy rare skins, accessories and even emotes can use Bitcoin as a method of payment at the OPSkins online marketplace based in California. Sellers receive the bitcoin in their virtual wallet and either choose to keep the cryptocurrency or exchange it for cash. OPSkins processes more than two million virtual transactions a week.

Boston-based Circle oversees more than $2 billion a month in cryptocurrency investments and exchanges between friends. Circle’s investment and money transfer platform currently features seven different cryptocurrencies, including Bitcoin, Monero and Zcash. Chain builds cloud blockchain infrastructures for financial services. The San Francisco company’s cryptographic ledgers help financial institutions safely and efficiently handle the transfer of cryptocurrencies. Chainalysis builds tools to help financial institutions and governments monitor the exchange of cryptocurrencies. The company’s due diligence software monitors and detects fraudulent trading, laundering and compliance violations, and builds trust in blockchain.  

In May 2019, Facebook registered Libra Networks LLC to create a new digital currency Libra. In the White Paper issued, the Libra Association announced that “Libra’s mission is to enable a simple global currency and financial infrastructure that empowers billions of people.” The new digital currency will be built on the Libra Blockchain and fully backed by the Libra reserve, a basket of fiat currencies and ‘other assets’. The project claims to be decentralized and governed by the Libra Association. Libra will be used for peer to peer payments, commerce (online and brick-and-mortar) and applications & gaming. 

The Libra Association is an independent, not-for-profit membership organization headquartered in Geneva, Switzerland and its founding members include Mastercard, PayPal, eBay, Facebook/Calibra, Farfetch, Lyft, MercadoPago, Spotify AB, Uber Technologies, Inc., Vodafone Group and

\[67\text{ Id. at n. 23}\]
a host of other Blockchain and Venture Capital associations as well as non-profit entities.\textsuperscript{68}

The paper also states that, “The world truly needs a reliable digital currency and infrastructure that together can deliver on the promise of “the internet of money.” In addition, the Libra Blockchain will be open-source, allowing developers to build on it. The paper in its problem statement, stated, 1.7 billion adults globally remain outside of the financial system and that Libra will help connect the world in a unified financial ecosystem.\textsuperscript{69}

In light of the Cambridge Analytica scandal, where the analytics firm misused data of over 50 million Facebook users, CEO Mark Zuckerberg had been criticized for grossly misusing his power as the keeper of personal data. One of the major draws of cryptocurrencies and blockchain, is the idea that no centralized entity (such as a bank or government) controls our finances. With its history, many suspect that Facebook with use Libra as a way to gather extensive financial data on its users. In anticipation of these criticisms, Facebook chose to not directly control the coin, but rather share the control with members of the Libra Association, with some members running nodes to verify transactions and maintain records. According to the White Paper, “While final decision-making authority rests with the association, Facebook is expected to maintain a leadership role through 2019.” Keeping this network separate from Facebook’s platform also provides the social media giant with some regulatory cover.\textsuperscript{70}

Facebook has additionally created a management tool it has named Calibra, which will offer digital wallets to save, send and spend Libras. It will be connected to the billion-plus users of the Messenger and WhatsApp platforms as the network expands beyond social networking into the world of international finance. Every person who uses Calibra will have to go through a "know your customer" process, which verifies user identities to prevent financial crimes, Reuters reported. That means anyone who signs up must share a government ID and other personal information. Calibra will provide support to customers who lose phones or their passwords, and refund customers whose Libras are stolen by fraudsters, Facebook said. Calibra will only share user data with parent company Facebook and third parties when it has customer consent, or in other "limited cases"- such as when law enforcement requests information - according to a statement.

\textsuperscript{68} Tatiana Koffman, Facebook’s Libra White Paper Is Now Live, 18 June 2019
\textsuperscript{70} Supra, n.49
Facebook pledged not to use Calibra data to improve advertising targeting.  

Page nine of the Report also states that “An additional goal of the association is to develop and promote an open identity standard. We believe that decentralized and portable digital identity is a prerequisite to financial inclusion and competition.” A Facebook spokeswoman is reported to have said that the company had nothing to add about identity beyond what’s in the white paper.

5. Smart Contracts

Distributed ledgers can be enhanced by smart contracts, which are small computer programs that behave according to predefined logic. Once created, smart contracts are able to operate autonomously — independently of any party in the system, including its creator — and consequently thought to be capable of replacing legal contracts. That is, these smart contracts can be used to model the terms of a real-world contract and automatically enforce its clauses as contractual conditions are met. Despite the name, smart contracts’ capabilities are not limited to legal contracts and can be arbitrarily complex: that is, complete software applications can be placed on a distributed ledger to operate autonomously. Consequently, distributed ledgers enabled with smart contracts could become capable of performing trusted database operations in a distributed environment that today would require a centralized infrastructure. Given this potential for distributed ledger technology and smart contracts to allow the distribution of any centralized computing infrastructure, we consider this overall field to be distributed infrastructure.

It is also essential to note what is a smart contract in relation to the end user and how it can affect a variety of outward facing, business-to-customer industries. Smart contracts can signify particular business processes and can be coupled together on a blockchain in order to perform more sophisticated functions. Another exciting smart contract example is the emergence of blockchain applications, sometimes referred to as 'dapps' (decentralized applications built on a blockchain operating autonomously, incentivized by a cryptocurrency which are open source).

72 Ian Allison, Buried in Facebook’s Libra White Paper, a Digital Identity Bombshell, 26 June 2019
73 Id. at n. 30, p.6
Within the context of blockchain, blockchain applications can be understood as blockchain-based user-facing interfaces which connect the end user to the technology through a combination of underlying smart contracts.\footnote{Id. at n.7}

a) Prediction markets

Prediction markets allow participants to speculate on the outcome of events like elections, sports, sales results etc. Prediction markets can speed up decisions in companies or political parties because they go beyond betting. The predictions give valuable insights about the public opinion on the matter in question.

Gnosis and Augur are one of the well-known Ethereum-based prediction market platforms. Bringing blockchain to the prediction markets opens an option fewer fees, greater accessibility, and better accuracy than other markets. The use of smart contracts ensures that the predictions of large groups are recorded transparently, and this helps for better predictions.

b) Digital Identity

Smart contracts can be set to release only necessary personal data to the contract parties. No one can see or use the data unless the holder verifies it and since it is stored on the blockchain can’t be altered which ensures authenticity. Smart contracts also solve the problem for necessary storage for keeping personal data; it is all stored on the blockchain. This enhances KYC verification which becomes instant.

uPort is in identity protocol that “allows users to register their own identity on Ethereum, send and request credentials, sign transactions, and securely manage keys & data.” uPort is public and permissionless ledger which allows users to manage and, if they choose, share their identity data.\footnote{8 Smart Contracts Use Cases, 27th September, 2018, retrievable at https://dolare.com/blog/post/8-smart-contracts-use-cases}

c) Supply chain and trade financing documents

Blockchains can make supply chain and trade finance documentation more efficient, by streamlining processes previously spread across multiple parties and databases on a single shared ledger. All too often,
supply chains are hampered by paper-based systems reliant on trading parties and banks around the world physically transferring documents, a process that can take weeks for a single transaction. Letters of credit and bills of lading must be signed and referenced by a multitude of parties, increasing exposure to loss and fraud. A blockchain can provide secure, accessible digital versions to all parties in a transaction, and smart contracts can be used to manage the workflow of approvals and automatically transfer payment upon all signatures being collected.

Barclays Corporate Bank recently partnered with one of the start-ups, Wave, a platform that stores bill-of-lading documents in the blockchain and uses smart contracts to log change of ownership and automatically transfer payments to ports upon arrival. Bank of America, Standard Charter, and the Development Bank of Singapore are also among the banks pursuing proof-of-concepts of their own.76

6. Healthcare77

a. Taipei
The Taipei Medical University Hospital and Digital Treasury Corporation (DTCO) have recently released phrOS. It aims to increase transparency between medical institutions by putting all of a patient’s medical information on a blockchain.

It includes images, as well as various information concerning a patient’s condition. The information can be accessed by doctors and the patients themselves through a mobile app. It also increases the security of medical information through the Decentralized Ledger Technology (DLT).

b. United States
One of the most popular healthcare use cases for blockchain is patient data management. Medical records tend to be separated by health agencies, making it impossible to determine a patient’s medical history without consulting their previous care provider. This process can take a significant amount of time, and may often result in mistakes due to human error.

Developed on the Ethereum blockchain, MedRec is a “system that prioritizes patient agency, giving a transparent and accessible view of medical

76 John Ream, Yang Chu and David Schatsky, Upgrading blockchains Smart contract use cases in industry, 8 June 2016
77 Bryan Weinberg, 10 Major Real Use Cases of Blockchain in Healthcare, 28 January, 2019
MedRec is intended to store all of a patient’s information in one place, making it simpler for patients and doctors to view. In its current design, providers maintain the blockchain through the (see used terms) Proof of Authority (PoA) mechanism.

Using Hurricane Maria relief efforts as a point of reference, the United States Department of Defense (DD) in conjunction with the United States Defense Logistics Agency (DLA) analyzed the potential of blockchain for future relief efforts. Currently, the DLA tracks logistics through centrally managed systems, which are split between multiple agencies. This makes it difficult for relief services to collaborate efficiently.

7. Manufacturing

Manufacturers have to be able to rely on the parts they purchase. And reputable parts suppliers want their reputations recorded and known. Blockchain can provide information on suppliers, so that manufacturers are certain they are getting what they ordered and that those goods are without defect.

   a. United States

   California-based SyncFab is using blockchain to match manufacturers needs with the right suppliers, as well as develop smart contracts that will guarantee standards, protect intellectual property, and provide for secure payments.  

8. Media and Gaming

Media industries have been heavily affected by the ubiquitous availability and the subsequent “commoditization” of content and been undermined by widespread piracy of intellectual property (IP). Today, media users are largely accustomed to having free access to a wide variety of content, and most of them are still reluctant to pay subscription fees for “premium” content behind paywalls.

In addition, all media segments have suffered significantly from digitization, since content can be copied and distributed easily and without loss of quality. So far, the introduction of Digital Rights Management systems have not significantly eliminated copyright infringements. The ensuing revenue “leakage” has been only

---

78 Andrew Arnold, Use Cases Proving Blockchain Can Have A Massive Impact On The Manufacturing Industry, 29 September, 2018
partially recovered through new consumption models such as all-you-can-consumer streaming subscriptions and micro-payments for articles.\textsuperscript{79}

a. \textit{Protecting Intellectual Property}\textsuperscript{80}

A startup called Binded allows photographers to register unique images in a blockchain as evidence of copyright ownership. Artists receive a copyright certificate that can be used to prevent unauthorized use of the images on the web. Monegraph offers a service for artists to upload their digital work and sell different levels of usage rights to publishers and advertisers. In addition to using blockchain to store ownership and licensing information on individual works, it also provides a public and independent record of licensing transactions between content owners and distributors. The model attempts to fill a market gap: giving independent artists such as photographers an affordable mechanism for copyright protection. In this business model, startups typically don’t charge artists for registering their works in the blockchain. Instead, they often take a share of the profits their service enables. Monegraph, for example, charges a processing fee on the sales that artists generate on its platform.

b. \textit{Digital Advertising}\textsuperscript{81}

Digital advertising is ripe for blockchain solutions that increase transparency in reporting about ad placement transactions and settlement. NYIAX, enables trading and execution of ad contracts between advertisers and publishers, with higher transparency for advertisers and less fees since transactions are direct. The platform is powered by partner NASDAQ’s technology, which helps explain why its upfront marketplace is already in production with more than 100 buyers and sellers in various stages of listing.

Lucidity provides a blockchain-based platform to track ad impressions, minimize fraud, and improve ad effectiveness across the complex programmatic advertising supply chain. It uses sophisticated techniques to address the scalability in order to handle the thousands of transactions necessary in a digital ad campaign.

c. \textit{Gaming and trading}

\textsuperscript{79} Milan Sallaba, Mirko René Gramatke and Alexander Mogg, \textit{Blockchain @ Media, a new Game Changer for the Media Industry?}, Deloitte Blockchain Institute, p.3

\textsuperscript{80} Andre Dutra, Andranik Tumasjan, and Isabell M. Welpe, \textit{Blockchain Is Changing How Media and Entertainment Companies Compete}, MIT Sloan Management Review September 11, 2018

\textsuperscript{81} Nelson Granados, \textit{How Blockchain Is Making Waves In Media And Entertainment}, Dec 3, 2018
EverdreamSoft, a Swiss game developer, offers a game in which people buy cards that they use to play. What distinguishes it from other games where players buy assets is that the cards are registered in a public blockchain and can be sold or traded outside the game, through digital currency. A similar approach could be adopted by other gaming companies, with the benefits of making the game assets more valuable and potentially increasing the revenue generated by in-game asset purchases. This might also expand interest in the games themselves, creating a network effect that can lead to increases in game-related revenue streams such as subscriptions or licenses.\textsuperscript{82}

**TAKE-AWAYS**

A cryptocurrency is a tradable digital asset or digital form of money, built on blockchain technology that only exists online. They use cryptography to verify and secure transactions, allowing for a particular digital token to be generated, stored, and transacted securely and, typically, anonymously. There is also a common commitment to decentralization as cryptocurrencies are typically developed as code by teams who build in mechanisms for issuance. Bitcoin is the first successful attempt at implementing digital cash without the need for a central party like a government to oversee it.

Chiasso and Zug in Switzerland often referred to as ‘Crypto Valley’ on the Swiss-Italian border have recently allowed its residents to use cryptocurrency to make small tax payments.

The Delaware Blockchain Initiative in the United States aims to create appropriate legal infrastructure for distributed ledgers to increase efficiency and speed of incorporation services. This is important, given that half of all publicly traded companies in the US and 65% of the Fortune 500 companies are incorporated in Delaware.

There are a few reasons, both pre-existing and those that developed as a result of policy and legal intervention that make Switzerland a leading center for blockchain companies (most recently, Facebook’s Libra Association) in the world. It has been widely documented that start up’s find the infrastructure, legal certainty as well as socio-political optimism for a growing role of Blockchain as factors that draw them to set up businesses in this country. Similar reasons can be attributed to the attractiveness of Malta to Blockchain companies as well.

In general, governments that are supportive of innovation and demonstrate a willingness to create a playing field for suitable entities, tend to draw those entities in. In contrast, legal uncertainty or prohibitive reforms including penalties and criminal liability for actions associated with core functions of businesses or even high entry barriers whether financial or otherwise, tend not to make the ecosystem suitable for dynamic entities like crypto companies.

In the case of India, the government often takes a “better safe than experiment” approach which can be seen as both cautious and hostile because of the degree of restrictiveness. It is unsurprising that in this context, the government views “safety” as outlawing cryptocurrencies altogether.
1) Banking and Finance

The Institute for Development and Research in Banking Technology (IDRBT), an arm of Reserve Bank of India (RBI) and an institution exclusively focused on banking technology, has published a blueprint for the implementation of blockchain technology in the banking sector. The blueprint proposes a broad roadmap for the technology's adoption across industries and organizational functions. In addition, it has underscored the need for common protocols which will help ensure interoperability among different entities. It has recommended a “collaborative approach” among various stakeholders in a network and called for “a codified set of rules for smooth operations and collaboration.” It has also proposed the setting up of a “governance structure,” led by a steering committee, which will oversee the implementation of a blockchain-based platform.

Furthermore, the institute has also proposed creating industry-specific business value framework which will help analyze the suitability of business applications to migrate to the blockchain-based system. The document said that such a framework would enable prioritizing projects that have high business value and filter out those that are less impactful ones. It seems that at least with respect to Banking and financial services, regulators do see great potential for blockchain-based applications to contribute positively.

IDRBT released a report in January 2017 confirming the cost-savings, transparency, and efficiency advantages of blockchain technology. Significantly, it observed, “having had a good understanding of the various aspects around the blockchain technology ... we recommend that the time is ripe for its adoption in India.”

In April 2018, the RBI stated that it was exploring the possibility of a digitally issued fiat currency, and in February 2018, a Working Group on FinTech and Digital

---

Banking discussed the pros and cons of distributed ledger technology and digital currencies.84

a. ICICI Bank in partnership with Emirates NBD and Edgeverve is serving over 250 corporates with its custom made blockchain platform that simplifies paper-intensive trade finance process. The solution aims to enable cost-effective and secured cross-border remittance for salary and vendor payments in reduced time owing to the paperless trail.

b. Infosys is working with seven private Indian banks – ICICI, YesBank, Kotak, Axis, IndusInd, RBI Bank and South Indian Bank to build a blockchain based solution “India Trade Connect” for document tracking systems in trade finance. The blockchain solution aims to enable automation and simplify the paper intensive trade finance process.

c. Digiledge in partnership with FederalBank has built a cross border remittance solution on Corda for Federal bank of Kerala, which eliminates the processing fee involved with intermediary banks and enables real time transactions between banks. The solution enables cost efficient and secured transactions between transacting banks.85

a. BankChain is a community of banks exploring, building and implementing blockchain solutions(Permissioned Private Ledger). Formed in February 2017 with State Bank of India being the first member. BankChain now has 27 members from India and the Middle East. Bank-Chain has been formed in collaboration with Prime chain Technologies, a Pune-based startup with a core focus on Blockchain technologies. Signzy, a two-year-old startup, is using blockchain with artificial intelligence to enable banks to authenticate and identify a person in a few hours.86

Bankchain is reported to be working on setting up an integrated corporate e-KYC platform, a vendor rating system and a blockchain powered register, which records hypothecation, lien, mortgages and pledges on movable, immovable and tangible assets.

In November 2018, HSBC Bank in India settled an export transaction for Reliance Industries Limited using the blockchain. The customer in this transaction was based in the U.S. and the transaction involved using a blockchain-based Letter of Credit and an electronic bill of lading which allowed for a digital transfer in the title of goods.87

84 Id. at n.32, p.9
85 Id. at n.57 and pp 18,26 and 34
86 Sangeeta Devni, Block chain Business models & use cases in India, 13 November 2017
87 Id. at n.57
2) Cyber Security

Block Armour is a Mumbai-based startup focused on harnessing the potential of blockchain technology to counter growing cybersecurity challenges. The Block Armour solution ring-fences an organization’s critical resources, securely providing access to authorized users and devices. It leverages Blockchain-Defined Perimeter, using private permissioned blockchain to secure critical systems. It also leverages digital signature based identity and authentication for humans, devices, and data.

3) Healthcare

a. MedChain, Inc., is early stage company building globally compliant healthcare blockchain and decentralized applications for electronic medical records (EMRs) and is working with the IBM Business Partner Cognition Foundry to capitalize on the advanced data protection and high performance of IBM LinuxONE, the enterprise Linux server built on mainframe technology. The server, coupled with blockchain is designed to enhance MedChain solutions that address important challenges in healthcare. The MedChain Network is an extensible, layered architecture and protocol system governed and secured by multiple blockchains that utilizes a multi-crypto-token framework. This network is built upon the Hyperledger Fabric permissioned blockchain, an open source project hosted by the Linux Foundation and built to run on LinuxONE. The MedChain solution is a "common data-layer" that allows existing EMR companies to build compliant healthcare dApps, empowering clients with unprecedented levels of control and insight into their own information.

b. Kare4U has partnered with hospitals, insurance companies and patients to implement its Blockchain-enabled mobile platform “HealthPro” to connect hospitals, insurance companies and host medical records of patients. The Blockchain solution aims to reduce the delays in health insurance loan disbursement and help customers maintain and manage their medical records in a secure way.

---

88 Ibid
89 Ibid.
c. As per World Health Organization (WHO), 20% of medicines sold in India are counterfeit products and India is the source of 35% of all counterfeit drugs sold worldwide. Apollo Hospitals is collaborating with Oracle, Strides Pharma and NITI Aayog (An Indian Governmental think tank) to build a Blockchain solution that will store drug details such as drug serial number, labelling and scanning details about manufacturers’ supply chain which will track every hand change in the network.


d. Statwig has built a blockchain based solution which can be deployed across temperature controlled supply chain used for perishable products such as vaccines. The blockchain solution also helps in real time tracking of medicines.  ^{91}

4) Telecom

Tech Mahindra has partnered with Microsoft and their Blockchain Solution enables customer’s preference registration, consent acquisition, dynamic preference setting, stakeholder onboarding, header registration, template registration, scrubbing service, and complaint handling and tracking – which align with TRAI regulation. The goal would be to eliminate spam calls and financial fraud by unregistered telecom marketers and open up new revenue streams for the telecom companies, principal entities and telemarketers, to run focused and effective promotional campaigns, without encroaching into subscribers’ personal space.

5) Retail brand engagement

Nucleus Vision in partnership with Raymond suits and Arvind lifestyles has created a blockchain-powered system enabling retailers to obtain digital intelligence about walk-in customers to personalize their shopping experience. The technology aims to help retailers increase sales conversions, improve loyalty and basket size. The pilot studies have already shown 2.4 times increase in sales conversions.

Their blockchain based data exchange mechanism empowers consumers to have control over data sharing with retailers. The solution aims to reduce the sales and marketing cost for retailers by improving overall operational efficiency in the store. ^{92}

^{91} Ibid. p. 34
^{92} Ibid.
6) Government Adoption

One of the areas in which Indian governmental entities have adopted an enthusiastic approach to implementing blockchain has been in cases of creating land record repositories. This is a relatively simpler experiment (compared to say, developing a blockchain-based voting platform with potentially different applications for keeping track of registration/eligibility and the actual counting of votes) involving textbook applications of the technology with immediate perceivable benefits and not exposing the system to greater known risks than those already present. In any case, it seems that some governments do view Blockchain favorably at least in relation to its benefits in simplifying and streamlining provision of certain government public services.

a. Andhra Pradesh

This is the first Indian state to start testing blockchain for governance. It has piloted two key projects: (1) Managing land records to curb property-related disputes and (2) Streamlining vehicle registrations. The state plans to implement blockchain across its entire administration. The government is building a robust blockchain ecosystem and has partnered with a New York-based blockchain software technology company ConsenSys for its Fintech Valley Vizag initiative.

According to their official website “the Fintech Valley in Vizag is a self-sustaining global Fintech Ecosystem that focuses on converging finance and technology to create large avenues of growth through industry-enablers, world-class infrastructure, entrepreneurship and innovation.”

Global financial services companies, government and academia come together in this valley to build capacity, infrastructure, market access, connectivity, funding channels, and incentive mechanisms to achieve unmatched business goals and successes.” Start-ups, financial Institutions, technology vendors, incubators/accelerators/innovation labs, and investors simultaneously partner with each other on this common platform.

b. Maharashtra

The Government has begun to experiment with digitizing some of the processes involved in the land registration. For example, an online facility is

---

93 Federation of Indian Chambers of Commerce and Industry-Deloitte, *Blockchain in Public Sector Transforming government services through exponential technologies*, January 2018, p.11.
94 Anirban Ghoshal, Belfrics, Ethereum Co-founder’s ConsenSys boost Andhra Pradesh’s Blockchain Initiative, 7 March 2018
95 http://www.fintechvalleyvizag.com/use-case-repo/
96 NASCOMM-KPMG, *Fintech in India – powering a digital economy*, September 2018, p, 38
provided for registering a lease and license agreement instead of the physical registration in the office of the SubRegistrar. The Revenue Department of Maharashtra has also initiated a program for online Mutation in 73 talukas of 5 districts to ease the process of Mutation and reduce the need for physical documentation. A blockchain based solution could be a good fit to bring robustness and digitization to the entire process, bringing all stakeholders on a single platform.\textsuperscript{97}

c. IndiaChain

On 1st February, in his 2018 Union Budget speech, Finance Minister Arun Jaitley declared that the government of India would not recognize cryptocurrency as legal tender. However, he added that India will explore the potential of blockchain in governance. And so, Niti Aayog, the government’s think tank, was put to the task of studying the use-cases of blockchain technology and developing viable prototypes. It is currently working on what could be the world’s largest implementation of blockchain in governance - IndiaChain.\textsuperscript{98}

It has launched an interoperable platform for both the government and private entities to build scalable blockchain solutions. An aim of the project is to develop a system that minimises frauds, speeds up enforcement of contracts and increases transparency of transactions and boost the agriculture-based economy of the country. IndiaChain will be linked to IndiaStack and other government digital identification databases. IndiaStack, a set of API’s (Application Programming Interface) developed around India’s unique identity project Aadhaar, helping developers build products and services riding on the country’s digital infrastructure. When operationalised, India's will likely be the largest scale of blockchain implementation in governance anywhere in the world.

IndiaChain in its first phase will work on agriculture, land records, and electricity distribution (see used terms for ‘proof of concept’)or PoC cases. Eventually, it is said that it will be linked with Aadhaar to secure individual identity. The government has also begun working on generating soil health cards for agricultural land in India. This will allow every patch of land to be digitised in terms of quality of land, what crops are grown, how many times a year, and so on. The soil testing data will be tracked using blockchain and the system will also help in identifying

\textsuperscript{97} Federation of Indian Chambers of Commerce and Industry-Deloitte, *Blockchain in Public Sector Transforming government services through exponential technologies*, January 2018, p.12.

\textsuperscript{98} *IndiaChain – Reimagining India Through Blockchain*, January 4, 2019, recoverable at https://www.xpressmoney.com/blog/industry/indiachain-reimagining-india-through-blockchain/
fertilizer requirements for different patches of land and also keep track of crop or vegetable cycles on these farms lands.

---

**TAKE-AWAYS**

In April 2018, the RBI stated that it was exploring the possibility of a digitally issued fiat currency, and in February 2018, a Working Group on Fintech and Digital Banking discussed the pros and cons of distributed ledger technology and digital currencies.

An important use-case from the Indian context is Infosys working with seven private Indian banks – ICICI, YesBank, Kotak, Axis, IndusInd, RBI Bank and South Indian Bank to build a blockchain based solution “India Trade Connect” for document tracking systems in trade finance. The blockchain solution aims to enable automation and simplify the paper intensive trade finance process.

Another ambitious project is being carried out by Niti Aayog, the government’s think tank, which is studying use-cases of blockchain technology and developing viable prototypes. It is currently working on what could be the world’s largest implementation of blockchain in governance – IndiaChain. It has launched an interoperable platform for both the government and private entities to build scalable blockchain solutions. IndiaChain in its first phase will work on agriculture, land records, and electricity distribution ‘proof of concept’ or PoC cases. Eventually, it is said that it will be linked with Aadhaar to secure individual identity.

The Nasscom-Avasant report also found that about 50% of the states in India are involved in Blockchain-related initiatives, driving the public sector blockchain adoption in the country with the top use cases in land registry, farm insurance (Kerala, Maharashtra) and digital certificates.

Cross-cutting challenges across diverse jurisdictions and sectors include concerns over large energy consumption, ensuring interoperability between platforms, limitations in scalability and sustainability and privacy as it relates to storage of personal and sensitive data that may not be easily amendable.

---

99 Sunny Sen and Anand Murali, *IndiaChain: Niti Aayog starts on IndiaStack-linked, large-scale Blockchain projects*, November 13, 2017
ANALYSIS OF EXISTING REGULATORY AND LEGAL FRAMEWORK GOVERNING BLOCKCHAIN TECHNOLOGY

Blockchain technology and its applications – international responses

The Avasant-NASSCOM Blockchain report 2019 is an industry report highlighting developments in the global and Indian Blockchain market and ecosystem. The report intends to systematically understand these ecosystems holistically across market trends, enterprise demands, emerging applications, policy and regulations, tech startups and service provider offerings, investments and talent.

The report among other things suggests that investments in the Indian Blockchain ecosystem have been relatively low, at less than 0.2% of the global investments. A cautious regulatory environment in India is seen to be limiting the investment opportunities from both domestic and global investors into Indian start-ups and several India-based investors raising funds through VCs and Initial Coin Offerings (ICOs) in other jurisdictions such as Malta, Singapore, UK, Switzerland, etc. that have enabling regulatory environments.

The report was revealing in many aspects–

a) 5 Countries are participating or observing members in the development of Blockchain Standards with the International Standards Organization (ISO) with India as a participating member;

b) almost 50% of leading and enabling blockchain jurisdictions in the world are located in Europe;

c) 26 countries that have a Fintech and/or Blockchain regulatory sandbox that enables startups/ technology providers to test their products and services with a limited number of real consumers for a trial period without being subject to normal regulations.

d) While several countries apply existing regulations for blockchain, 7 countries have developed specialized Blockchain/DLT-specific regulations.
e) Japan recognizes Bitcoin and other digital currencies as legal tender, and digital currency exchanges are legal to operate if they are registered with the Japanese Financial Services Agency.

The report analyzed 120 countries across 10 key regulatory dimensions namely Digital Tokens/ Virtual Currencies, Crypto Exchanges, ICOs, Cryptocurrency Mining, DLT, Development of Blockchain Standards, Regulatory Sandbox, Crypto Exchange License Requirement, Taxation and KYC/AML and has classified countries into categories of “Leading”, “Enabling”, “Neutral”, “Cautious” and “Unfriendly” based on their Blockchain regulatory environment.

(Image reproduced from page 46 of the Nasscom-Avasant Report)

1. **Malta**
   In early 2018, Malta passed three new laws regulating the cryptocurrency and blockchain ecosystem. The first legislation provides for the establishment of a new authority, the MDIA, for the promotion and development of the innovative technology sector in Malta. It provides proper recognition and regulations for Distributed Ledger Technologies and smart contracts. Registration with the MDIA for developing anything in relation to blockchain technology is voluntary but it is recommended to have one's platform audited and certified by the MDIA. The

---

second legislation lays down the applicable regime for the registration of Technology Service Providers and the certification for Technology Arrangements. Currently, the ‘Innovative Technology Arrangements’ recognized under the Act relate only to DLTs and smart contracts. However, the MDIA has the power under the ITAS to notify additional Innovative Technology Arrangements. The third legislation provides a framework for issuance of DLT assets through ICOs and crypto exchanges and their operation. Malta has decided to remove the word ‘cryptocurrency’ and replace it with ‘Virtual Financial Asset’ where a VFA is defined as ‘any form of digital medium recordation that is used as a digital medium of exchange, unit of account, or store of value and that is not electronic money; a financial instrument or a virtual token’. Moreover, ‘ICO’ is replaced by ‘initial VFA offering’, ‘crypto-exchange’ is replaced by ‘VFA exchange’ and ‘crypto-services’ are replaced by ‘VFA services’. Furthermore, the issue of Virtual Tokens are excluded from the remit of the VFAA. The VFAA also lays down the financial instruments test to ensure that any cryptographic token that is issued during the ICO, or listed on a crypto-exchange, would either be within the existing regulation or not. The laws supplement other existing regulations such as the Malta Financial Services Authority, the Malta Gaming Authority and the Malta Communications Authority. 101

Special considerations
This three-pronged approach places Malta in a very favorable position when compared to its peers, mostly due to the creation of the MDIA, which is the first regulatory authority of its kind in the world.

The voluntary nature of any applications by those constructing DLT-based platforms ensures that any development taking place in Malta is not stifled, and only those who wish to obtain regulatory approval would be invited to tender their applications and submit themselves to regulatory and technical scrutiny. System auditors need not be based in Malta and can operate through resident agents, meaning that the doors are open for anyone with a legitimate interest in aiding the regulatory framework covering DLT-based projects.

The VFAA ensures that any cryptographic token issued during the ICO stage, or in relation to which a service is being offered, would either be within the confines of existing regulation or not. This is the cause of frustration for most entities seeking a jurisdiction within which to launch and run an ICO due to the regulatory uncertainty, which is what leads to an unstable environment for business. The Maltese VFA framework seems to consider the prevention of stifling of technological innovation as a key priority in drafting a fairly liberal regulatory framework for Blockchain technology and transactions concerning crypto-assets.

101 Id. at n.32, p 33
Gibraltar

Gibraltar is one of the few jurisdictions in the world to have a regulatory framework already in place specifically designed to regulate blockchain businesses. The regulation applies to cryptocurrency exchanges and wallet service providers, as well as any company that stores or transmits value belonging to others, using distributed ledger technology (DLT). When the government of Gibraltar decided that it wanted to regulate the blockchain industry in 2014, it started working closely with the private sector to identify what the most appropriate form of regulation should be. The aim was to create a principles-based regulatory framework that would be appropriate for blockchain and cryptocurrency businesses and also flexible enough to remain relevant as new technologies develop.

The Gibraltar DLT Regulations contain 9 principles and, as part of the application process, each applicant will have to demonstrate to the regulator how it addresses, and satisfactorily complies with, each of these principles. DLT firms in Gibraltar are regulated by the Gibraltar Financial Services Commission (GFSC), who have a team dealing exclusively with DLT applications. It is believed that having an approachable, business-friendly regulator with a profound understanding of cryptocurrencies and distributed ledger technology generally sets Gibraltar apart from the other jurisdictions.

Special Considerations

A small jurisdiction like Gibraltar can act quickly to changing environments and changing business needs. Being a close-knit community could mean close cooperation between government and business, and institutions which offer a greater understanding of business needs. It would likely be much harder to scale similar efforts in India given the complexities associated with population size, socio-economic and other heterogeneities as well as the sensibilities of parties involved.

While drafting the legislation in Gibraltar, the regulators decided to opt for a “light touch” approach; providing solid regulatory oversight while, at the same time, being ever-mindful of the need for continued innovation in the fast-moving

---

102 Jonathan Galea, Malta’s DLT Regulatory Framework, May 2019
crypto space. Underpinning this regulatory approach are the Nine Core Principle of Gibraltar’s DLT regulation:

**Principle One: Honesty and Integrity**
DLT providers must act with “honesty, integrity and professionalism”; they must always conduct their operations and communications in an honourable and forthright fashion and never “pose a risk to the public or to the reputation of Gibraltar”.

**Principle Two: Customer Care**
DLT providers must offer the utmost standards of customer care; they must always ensure all communications are clear-cut and transparent, with full disclosure of any conflicts of interest, and that all customer complaints or issues are dealt with swiftly.

**Principle Three: Resources**
DLT providers must ensure adequate resources are provided; they must ensure both financial and non-financial resources are available, including adequate insurance and capital.

**Principle Four: Risk Management**
DLT providers must take a common-sense approach to risk management; they must employ “forward-looking risk management practices” and always consider “risks to its customers and the reputation of Gibraltar in addition to risks to its own business.”

**Principle Five: Protection of Client Assets**
DLT providers must take significant steps to protect client assets; they must ensure adequate storage, data protection, proper record keeping and other appropriate measures to ensure the maximum wellbeing of all client assets.

**Principle Six: Corporate Governance**
DLT providers must “have effective corporate governance arrangements”; they must take careful consideration regarding structure, strategy, procedures and corporate culture.

**Principle Seven: Cyber Security**
DLT providers must demonstrate solid cyber security; they “must ensure that all systems and security access protocols are maintained to appropriate high standards” and all employees, including senior management and board members, must be fully aware of relevant cyber security threats.

**Principle Eight: Financial Crime**
DLT providers must take a proactive stance against financial crime; they must perform considerable due diligence and KYC vetting in full accordance with the Proceeds of Crime Act 2015 (POCA).

**Principle Nine: Resilience**
DLT providers must be resilient; they must be fully prepared for all possible contingencies to ensure minimal loss and disruption to clients, even in the event of the company winding down.104

2. Switzerland

In December 2018, alongside with the report on DLT regulation, the Swiss Federal Council, with the Swiss Financial Market Supervisory Authority FINMA, implemented a Fintech license, aiming to create an adequate, technology-neutral regulatory framework for any business that needs to accept deposits from the public without engaging in typical commercial banking activities.

The council released a report wherein it articulates Switzerland’s unique approach to regulation, distinguishing itself from competitive jurisdictions such as Malta and Lichtenstein. Switzerland does not foresee the need to create a new law dedicated to blockchain, but intends to “surgically” adjust the existing legal framework as much as necessary to support the development of the Swiss blockchain ecosystem.105

Firstly, the council has proposed an amendment to the country’s securities law to increase the legal certainty of crypto tokens. The council also wants to segregate crypto assets from the insolvent debtors’ total estate in bankruptcy proceedings. However, because under the country’s existing Debt Enforcement and Bankruptcy Act (DEBA) it is not clear whether these assets can be segregated, the council said there is a “great need for legal certainty for the parties involved and thus a corresponding change is proposed in the DEBA act.

Further, the government body has proposed the creation of a new “authorization category” for infrastructure providers in the blockchain sector, and will make amendments to its Financial Market Infrastructure Act accordingly. Currently, the council has not yet proposed any specific changes, as the central definitions of the terms “securities” and “derivatives” in financial market regulations are also relevant for blockchain-based business models.

Regarding the country’s Anti-Money Laundering Act, the council said the legislation is currently adequate enough to also cover activities related to cryptocurrencies and initial coin offerings.106

3. Japan

104 Gibraltar Financial Services Commission, Distributed Ledger Technology Regulatory Framework (DLT framework), retrievable at http://www.gfsc.gi/dlt
105 Mattia Rattaggi, Swiss on a roll to regulate crypto, blockchain space, 15 February 2019
106 Yogita Khatri, Switzerland to Regulate Blockchain Within Existing Financial Laws, 17 December 2018
Since the beginning of 2018, the Financial Services Agency in Japan (FSA) has been working on tightening regulations. A new five-point agenda has been introduced by the FSA focusing on: strict and robust security standards; KYC/AML — stringent customer ID protocols must be implemented when dealing with large value crypto transfers; management of customer assets must be separate from the company’s assets; prohibition of privacy coins such as Monero and ZCash; Corporate Governance — there must be a clear separation between the ownership and management of the business.

Also, nobody may provide services within the cryptocurrency industry without first being registered as a crypto (virtual) currency exchange service provider in Japan. These regulations will apply to anyone running an exchange from Japan but the regulations also imply that cryptocurrency exchanges being operated from outside of Japan will be prohibited from providing services to Japanese residents if such exchanges are not registered with the FSA.\(^\text{107}\)

4. United States

The U.S. Government has shown support for the development of Blockchain regulation and governance within the context of the technology’s growth and expansion. U.S. Congress has created the Congressional Blockchain Caucus to handle legislation pertaining to Digital Ledger Technology (DLT) and cryptocurrencies. In September 2018 co-chair of the Congressional Blockchain Caucus introduced the “Resolution Supporting Digital Currencies and Blockchain Technology” bill, the “Blockchain Regulatory Certainty Act” and the “Safe Harbor for Taxpayers with Forked Assets Act.” These bills encourage the federal government to monitor Blockchain entities and provide suggestions for taxation of digital assets via crypto taxation guidance. Also, under IRS Notice 2014-21, digital currency is treated as property rather than a foreign currency.

Another legislation has since been introduced as “The Virtual Currency Consumer Protection Act of 2018” and the “U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2018.” These bills provide recommendations to the U.S. Commodity Futures Trading Commission (CFTC) and focus on cryptocurrencies with regards to price manipulation, and examine U.S. Blockchain technology regulation in

\(^{107}\) Id at p.76
the global cryptocurrency universe. The U.S. Treasury Department’s Financial Crimes Enforcement Network (FinCEN) delineates virtual currency as “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency.”

Generally speaking, as a matter of U.S. federal law, Digital Assets are viewed as either “securities” (as appears to be the case with most ICO tokens), and thus subject to regulation by the Securities and Exchange Commission (“SEC”), or non-security “commodities” (as appears to be the case with Bitcoin and other cryptocurrencies), and thus subject to regulation by the Commodity Futures Trading Commission (“CFTC”). In addition, certain state laws may apply to Digital Asset custodial activities. A person acting as custodian for Digital Assets that are securities typically must register with the SEC as a broker-dealer. Among other regulations, registered broker-dealers are subject to extensive requirements related to the handling of customer funds and securities (which would include these Digital Assets), maintenance of minimum net capital, creation and maintenance of books and records, and anti-money laundering requirements.

At the State level, most regulatory activity is taking place in the legislative branch. There have been two approaches to regulation. Some states have tried to promote Blockchain technology by passing favourable laws, often by exempting cryptocurrencies from State securities and/or anti-money laundering statutes (e.g. Wyoming). These States hope to leverage investment in the sector to boost local economies and public services. On the other hand, states like California and New York are less favourable to the use of this technology with the latter adopting stringent and laborious regulations leading to the restriction of its use.

The National Conference of Commissioners on Uniform State Laws voted in July 2017 to approve a model act providing for the regulation of digital currency businesses at the state level. Arizona has passed a law recognizing "smart contracts" using blockchain technology, and has taken measures to ease the regulatory burdens on new financial technologies. A California law makes it illegal to buy or exchange a raffle ticket for any kind of cryptocurrency. Delaware has a pending initiative authorizing registration of shares of Delaware companies in blockchain form. New York currently uses a "Bitlicense" regulating digital currency within the state.

108 Astrid F. Kowlessar, Blockchain: U.S Regulation and Governance, 21 January, 2019
110 Global Legal Insights (Global Legal Group Ltd.), Blockchain and Cryptocurrency Regulation | USA, recoverable at https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa
Vermont recognized blockchain as evidence and Illinois has authorized the use of blockchain for real estate records.  

The foundation for much of American corporate finance is Delaware corporate law. In February 2018, the Delaware Blockchain Initiative (DBI) was launched, allowing for the application of distributed ledger technology to many of the private sector’s most basic and critical legal documents, which companies until then, filed with the Delaware Division of Corporations.

When then-Governor Markell launched the DBI, he committed the State government to use the technology and asked the Delaware State Bar Association’s Corporation Law Council to consider clarifying Delaware corporate law to expressly authorize tracking of share issuances and transfers on a distributed ledger. The first milestone on DBI’s roadmap has been reached. It is the rollout of distributed ledger technology at the Delaware Public Archives, which has been the “beta” test for the technology within State government. New “smart records” technology automates compliance with laws pertaining to retention and destruction of archival documents, among other features.

5. India

Two key observations regarding where India stands in terms of Blockchain regulation are -

a) the government’s approach has been radically different towards Bitcoin (unfavorable) and its underlying technology, blockchain (favourable) and;

b) Regulatory movement seems to concentrated in the Banking and financial services sector, for now, with the exception of the telecom sector. This is not to say that the government has not acknowledged the utility of Blockchain in other sectors, but that it seems to be prioritizing this initial phase of regulation in these sectors, perhaps because of the cross-border nature and high risks associated with high-value transactions.

The government is seeing Blockchain technology quite favourably but has prohibited the use of cryptocurrencies. RBI had issued three press releases dated December 24, 2013, February 01, 2017 and December 05, 2017 wherein the public was cautioned

---

111 Schnader Harrison Segal & Lewis LLP, United States: Taking A Trip Around The Regulatory Block: U.S. Regulation Of Blockchain And Digital Assets, 2 August 2018
112 Andrea Tinianow, Delaware Blockchain Initiative and Caitlin Long, Symbiont, Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance, Harvard Law School Forum on Corporate Governance and Financial Regulation, 16 March 2017
about the risks of VC’s including electronic wallets being prone to losses arising out of hacking, compromise of access credentials, malware attack etc. They also expressed concerns over the lack of established frameworks for recourse to customer disputes and the risk of great loss attributable to huge volatility in the speculative value of VCs. Lastly, RBI warned that the absence of information of counterparties in peer-to-peer anonymous/pseudonymous systems could subject the users to unintentional breaches of anti-money laundering and combating the financing of terrorism (AML/CFT) laws. 

The Reserve Bank of India circular dated April 6, 2018 banned all entities regulated by the RBI (i.e., banks, financing institutions, nonbanking financing institutions, payment system providers and the like) from dealing in, or facilitating any dealings in, cryptocurrencies. These entities were given a three-month period within which all accounts dealing with cryptocurrencies would have to be shut down. Following this, an Inter-Ministerial Committee that was constituted in 2017 under the Chairmanship of the Economic Affairs Secretary and comprising senior officials of the Ministry of Electronics and Information Technology, SEBI and the RBI, provided its recommendations on what the regulatory stance should be in relation to DLT’s and VC’s. The committee was set up to look into the legality of cryptocurrencies and blockchain and submitted its report to the Finance Ministry recommending that all private cryptocurrencies, except any cryptocurrency issued by the State, be banned in India. The Committee stated—“There is no underlying intrinsic value of (these) private cryptocurrencies...private cryptocurrencies lack all the attributes of a currency. There is no fixed nominal value of these private cryptocurrencies i.e. neither act as any store of value nor they are a medium of exchange. Since their inceptions, cryptocurrencies have demonstrated extreme fluctuations in their prices. Therefore, the Committee is of clear view that the private cryptocurrencies should not be allowed. These cryptocurrencies cannot serve the purpose of a currency. The private cryptocurrencies are inconsistent with the essential functions of money/currency, hence private cryptocurrencies cannot replace fiat currencies. A review of global best practises also shows that private cryptocurrencies have not been recognised as a LEGAL tender in any jurisdiction.”

The committee submitted its report along with a draft bill on digital currencies on February 28 2019 but was only made public on July 22 2019.

---

114 Department of economic affairs, Ministry of Finance (India). Report of the Committee to propose specific actions to be taken in relation to Virtual Currencies “IMC Report”), document dated 28 February 2019
115 IMC Report, p. 34
The IMC’s opinion that these crypto-assets are not backed by any intrinsic value, is not entirely true. Many cryptocurrencies, these days, are backed by petroleum, gold, as well as the US dollar in the case of Facebook’s Libra. The IMC does not make any differentiation among cryptocurrencies that are not backed by any central banks. Another criticism of the argument of lack of intrinsic value is that money is a social convention and as such people’s response to it is determined by what they collectively think will be other people’s response to it. Unlike wood (which can be used to make shelter) or grain (which can be eaten) gold does not have any intrinsic value but still has historically been one of the most widely used forms of money in the world over. Money’s own value is socially constructed since people attribute worth to a medium whose physical characteristics are essentially irrelevant to its monetary value. The report presents energy consumption as an issue in the context of Bitcoin mining, however, the report does not delve into the numerous solutions suggested world over to curb this consumption. Examples include Miners’ transition to eco-friendlier power sources like Vienna-based HydroMiner, that uses renewable hydroelectric power to mine Bitcoin and the case of a firm Soluna, which has teamed with the German wind-power developer ALTUS AG, aiming to build at least 36 megawatts of capacity by 2020 and complete the entire 900 megawatts in five years. The wind power will then supply cheap electricity to a high-density computing center for “mining” Bitcoin and other cryptocurrencies. Soluna will use the money it makes from mining to further develop the wind farm, says CEO John Belizaire, who adds that it will also be able to make money selling power to the Moroccan grid. He believes Soluna’s “vertically integrated” mining model represents not only a cleaner way to maintain Bitcoin’s and other blockchain networks, but also a new way to fund renewable-energy development. There is also no mention in the report of any comparative analysis showing that the resources expended (through cutting of trees, production of paper, printing, transport, etc.) on the circulation of paper currency are less than those that would be expended on mining cryptocurrencies on a large scale.

The IMC has also drafted a legislation entitled ‘Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019’, which mandates a fine and imprisonment of up to 10 years for specified offences. The provision appears excessive and applies to any person that “directly or indirectly mines, generates,

---

117 Suprita Anupam quoting Nischal Shetty (CEO and Founder of WazirX), The Aftermath Of India’s Cryptocurrency Ban: Startups, Investors Poke Holes In Govt’s Plan, 23 July 2019
118 Mark Fidelman, 5 Ways To Solve The Bitcoin Mining Energy Crisis, 11 December 2017
119 Mike Orcutt, This company thinks it can help solve Bitcoin’s energy problem, 23 August 2018
holds, sells, deals in, transfers, disposes of or issues Cryptocurrency or any combination thereof with an intent to use it for any of the purposes mentioned.”  

However, the Committee has expressed a more positive outlook towards the potential issuance of cryptocurrencies by RBI reiterating its previously mentioned stance that concerns raised in the Report relating to VC’s are restricted to private or non-sovereign-backed cryptocurrencies. It has stated that “it may be possible to visualise some models of future official digital currencies but as of date it is unclear whether there is clear advantage in the context of India to come up with a official digital currency. Hence, the Committee recommends that, if required, a Group may be constituted by the Department of Economic Affairs, with participation of the representatives of the RBI, MeitY and DFS for examination and development of an appropriate model of digital currency in India...(and in) due course, (if) it is decided to issue a digital currency in India having the status of a legal tender, the Reserve Bank of India should be the appropriate regulator of such digital currency by virtue of its powers under Section 22 of the RBI Act.” It is perhaps true that without the characteristic feature of decentralization, one of the premises of having cryptocurrencies is eroded and as such, a sovereign-backed, centralized version of these cryptocurrencies would not support similar advantages. So it is unclear whether or why the IMC has proposed a way forward in this regard.

Of particular interest are the stated concerns relating to the possible usage of non-official VC’s. The IMC has mentioned that their concerns include - consumer exploitation through various scams and the irreversibility in transactions, compromises in the ability of central banks to monitor and stabilise the economy and the added disadvantage of pseudonymity which could promote money-laundering, terrorism-financing and other cross-border criminal activity. In the Indian context, concerns such as unsophisticated consumers being lured into investing in ponzi schemes with the promise of Bitcoin returns could be quite valid, considering these persons do form a rather large majority, most of whom may not have meaningful access to sound legal and financial advice in the crypto space. This is separate from the fact that such frauds have actually been reported to have occurred. It must however be pointed out that frauds and scams are not unique to the cryptocurrency space and a large number of scams and frauds have been reported regarding regular banking and credit card operations as well.

120 Banning of cryptocurrency and regulation of official digital currency Bill, 2019, Chapter VI
121 IMC Report, p. 45.
122 IMC Report, p. 28 – 31, generally.
123 IMC Report, p.28
124 https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
In relation to the other stated concerns, the difficulties for law enforcement authorities to track down persons involved in cross-border financial crimes could be addressed to a large extent by enforcing rigid KYC/AML standards such as, for example, the ones in place in Japan. As mentioned previously, some of these steps could include customer ID protocols when dealing with large value crypto transfer and clear separation between the ownership and management of businesses. As regards the ambiguity in the legal status of virtual currencies creating problems for law enforcement authorities while framing charges, albeit valid, this particular challenge is similar to one that could occur in the cases of any civil or criminal offenses (cross-border) not legally recognized as such in all countries, and may not be a unique crypto-related challenge.

With respect to DLT’s more generally, the IMC has arrived at positive conclusions in their applicability and has gone so far as prescribing specific sectors for their adoption. The Committee recommended that the RBI examine the “utility of using DLT based systems for enabling faster and more secure payment infrastructure, especially for cross-border payments” and also recommended “that blockchain based systems be considered for building a low-cost KYC system that reduces the need for duplication of KYC requirements for individuals.” The committee also “saw value in the use of distributed ledgers in land deeds that could be beneficial for removing errors and frauds in land markets if the technology is implemented for maintaining land records.” 125 The RBI had also issued a White Paper on ‘Applications of Block Chain Technology to the Banking and Financial Sector in India’ in January 2017, which views the application of blockchain technology by banks favourably. The RBI has also indicated that it may create a domestic ledger platform involving National Payment Corporation of India in September 2017, it even announced that it had taken steps to create such a platform, and also filed three patent applications in this regard.

Along similar lines, the Indian Finance Minister, in his Budget Speech on February 1, 2018, stated that although the Indian government does not recognize Bitcoin as legal tender, it does encourage the use of blockchain technology in payment systems. 126

In view of the growing significance of fintech innovations, RBI set up an inter-regulatory ‘Working Group on FinTech and Digital Banking’ in July 2016 to study the regulatory responses to such innovations across the globe. The Group included representatives from the RBI, Securities Exchange Board of India (“SEBI”), Insurance

125 IMC Report, p. 53.
Regulatory and Development Authority of India (“IRDAI”), and Pension Fund Regulatory and Development Authority (“PFRDA”), select financial entities regulated by these agencies, rating agencies and fintech consultants and companies.

On February 08, 2018, this Working Group released its report, which, among other things, recommended the formulation of an appropriate framework for a regulatory sandbox. The Working Group noted that sandboxes offered benefits including limited testing which would answer questions, before the product is made available more broadly, on the product’s concerns as well as its potential for success. It was observed that the objective of a sandbox should be “to encourage more fintech experimentation within a well-defined space and duration where regulators will provide the requisite regulatory support, so as to increase efficiency, manage risks better and create new opportunities for consumers.”

The Proposed Framework was announced with the above objectives. The Framework describes a regulatory sandbox (“RS”) as the live testing of new products or services in a controlled regulatory environment, for which regulators may or may not permit certain regulatory relaxations for the duration of the testing.

The products, services, and technologies expressly stated to be eligible for the RS include blockchain technologies, and artificial intelligence and machine learning applications while crypto-currency/crypto-asset activities including Initial Coin Offerings (ICOs) have been expressly excluded from the scope of the RS. The Proposed Framework also states that financial services already being offered in India may not be suitable for the RS, unless the RS applicant demonstrates that either “a different technology is being gainfully applied or the same technology is being applied in a more efficient and effective manner”.

Since crypto-assets are essential to public blockchain technology, it remains to be seen how blockchain projects which are based on public blockchains such as Ethereum (or otherwise use tokens or crypto-assets) will be considered by the RBI. The Ethereum blockchain is used by a number of “Indian entities” including the Government of Andhra Pradesh, HP and Infosys.

**Regulatory relaxations**

Under the Proposed Framework, the RBI may relax specific regulatory requirements (which the RS entity will otherwise be subject to) for the duration of the RS.

While the Proposed Framework does not elucidate the types of regulatory relaxations that may be provided, possible regulatory relaxations that may be considered by the RBI, as contemplated by the Working Group’s report, include: i) quantitative...
prudential requirements, such as statutory or liquidity requirement, minimum paid-up capital, capital adequacy, license fees, and financial soundness; ii) corporate governance requirements such as board composition, management experience, and fit and proper criteria; and iii) risk management, which includes technology risk management and outsourcing guidelines.

However, compliance with certain regulatory requirements has been stated to be mandatory in all circumstances. These mandatory requirements include customer privacy and data protection measures, secure storage of and access to payment data of stakeholders, security of transactions, KYC/AML requirements, and statutory requirements (which presumably refers to legislative provisions which the RBI cannot relax).  

In the non-banking sectors, regulatory movement is seen with India’s telecom regulator, the Telecom Regulatory Authority of India's (TRAI), in July 2018 notifying the Telecom Commercial Communications Customer Preference Regulation, 2018. (“TCCPR Regulations”).

The TCCPR Regulations mandate the usage of Distributed Ledger Technology by telecom operators to solve the problem of unsolicited commercial communication. The TCCPR Regulations impose obligations on telecom ‘access providers’ to adopt DLT with permissioned and private DLT networks to ensure that all necessary regulatory checks are carried out for sending commercial communications, and to operate smart contracts among entities for effectively controlling the flow of commercial communications. The press release accompanying it further acknowledges that DLT is suitable for the adoption as Regulatory Technology (“RegTech”) for controlling and managing the Unsolicited Commercial Communication (“UCC”) ecosystem. While comparing the implementation of record keeping between traditional and DLT based systems, the TCCPR Regulations highlight that DLT has the potential to support the needs of telecom service providers, telemarketers, and mobile users for better control and management over UCC.

NITI Aayog, the government’s think tank, has announced that has been working on a national strategy for blockchain which will identify the areas where the country can implement the technology and also list out the means for doing so. An official has been reported to have said that Niti Aayog considers that blockchain can be useful if applied correctly, and that the technology which is primarily used for database management works best when multiple parties who do not trust each other have

---

128 Id. at n.32, pp. 10,11.
collaborated, in land records, for instance. Since the government can implement most of the projects involving blockchain, unlike in the case of artificial intelligence where it is acting just as a facilitator, it needs to identify where blockchain can be utilised and where it will not work. The official also spoke favourably about properly structured sandboxes and how they can align incentives between regulators and industry by giving regulators insights into blockchain technologies and industry the ability to test new technologies in a limited live environment without the litany of regulatory requirements. 129

Outside the realms of Executive and Legislative action, several stakeholders have also approached the judiciary by filing petitions before the Indian Supreme Court to compel the government to provide clarity on its position on cryptocurrencies, specifically.

The two primary petitions seeking to address the legality of cryptocurrencies were filed in 2017 by (i) Vijay Pal Dalmia and Siddharth Dalmia (“Dalmia Petition”), and (ii) Dwapayan Bhowmick (“Bhowmick Petition”).

The Dalmia Petition seeks an order to “restrain/ ban the sale/ purchase of or investment in, illegal cryptocurrencies and initiate investigation and prosecution against all parties which indulged in the sale/ purchase of cryptocurrency.”

The grounds for the stated petition was based on *inter alia* (i) the anonymous nature of cryptocurrency transactions which makes it well-suited for funding terrorism, corruption, money laundering, tax evasion, etc.; (ii) production and introduction of new cryptocurrency being generated by private parties, without the intervention of the government, and hence violating the Constitution; (iii) use of cryptocurrency being in contravention of several laws such as FEMA and Prevention of Money Laundering Act, 2002; and (iv) the fact that trading of cryptocurrencies permits players to bypass prescribed KYC norms.

The Bhowmick Petition seeks an “issuance of direction to regulate the flow of bitcoins as well as requiring the constitution of a committee of experts to consider prohibition/regulation of bitcoins and other cryptocurrencies.”

On the other hand, certain industry participants have filed writ petitions challenging the constitutionality of the RBI’s Circular banning cryptocurrencies and reiterated the need for clarity on regulation. Other stakeholders, such as the Internet and Mobile Association of India have filed intervention applications in the Bhowmick Petition in

---

129 Surabhi Agarwal, *NITI Aayog works on strategy to leverage blockchain technology*, 17 May 2018
order to draw attention to the impact that any restrictive regulation on cryptocurrencies may have to their businesses. Counsel for AMIMAI is also reported to have briefly stated that the RBI diktat of 6 April 2018 banning all entities regulated by the RBI from dealing in cryptocurrencies, directly affected businesses which are legal under the Article 19(1)(g) of Indian constitution thus implicating the constitutional guarantees that all citizens shall have the right to practice any profession, or to carry on occupation, trade or business.\(^{130}\)

The IAMAI moved the Supreme court to issue a stay application on RBI’s circular. Indian cryptocurrency exchanges like Koinex, Zebpay, Unocoin, Coindelta, coinsecure, throughbit and pocketbits came together to form the Blockchain and Cryptocurrency Committee (BACC) of the IAMAI. Counsel appearing for IAMAI is reported to have argued that blockchain technology adopted in these virtual currencies was not disputed and therefore a blanket ban was "arbitrary, unfair and unconstitutional". The counsel referred to a RTI reply given by the RBI in which it was said that no study had been undertaken by the top bank and not even any committee had been constituted to study the effect of cryptocurrency on the economy.\(^{131}\)

It is interesting to note that these Indian Cryptocurrency Exchanges are reported to be working together to create a central repository of transactions by traders in a bid to self regulate. The exchanges will pool trading data of users based on PAN and create a central repository for the government. Currently, transactions are recorded by each exchange but not shared with any other exchange, they are mutually exclusive.\(^{132}\)In relation to where the litigation now stands, IAMAI had filed representation or a detailed document on cryptocurrency, its uses and also how it can be regulated on May 29 2018 and the RBI was given one week to respond. The representation preferred regulations over a ban and was a point by point layout of recommendations for regulating Cryptocurrencies positively. When the RBI did respond, it was not specific to the representation but a generic response, of which the court took notice in its latest hearing. The judge then turned to RBI’s counsel and said that the RBI response to this representation is not appropriate as RBI simply flew their hands in the air and avoided responsibility by saying they had forwarded

---

\(^{130}\) Naimesh Sanghvi, IAMAI Counsel to Argue RBI’s Banking Ban violates “Right to practice any profession”, 19 August 2019, https://coincrunch.in/2019/08/19/iamai-counsel-how-rbi-banking-ban-violates-right-to-practice-any-profession


the representation to the IMC. The new date of hearing is set to September 25, 2019.

However, other reports state that the Supreme Court was informed in the first week of August 2019 that the contentious Bill may be introduced when parliament is reconvened, according to a court document, and that upon learning of the government’s intention to introduce the bill, the court has decided to postpone hearing the petitions concerning crypto regulation in India until the last week of January 2020.

POLICY CONSIDERATIONS AND RECOMMENDATIONS

1. Have multi-stakeholder consultations on the legality of cryptocurrencies

Till date, while the India Supreme Court has admitted all the petitions mentioned previously, the matters remain pending and the judiciary’s stance and therefore the legality of raised issues, unknown. Nevertheless, the arguments made indicate that there is both, an acknowledgment by civil society members of the various risks presented by cryptocurrencies as well as disapproval from those questioning the constitutionality of the RBI Circular imposing a blanket ban on their use. There is no single or overarching public sentiment about whether or not the use of cryptocurrencies should be permitted making it a worthwhile experiment to have multi-stakeholder consultation on the issue before arriving at a final framework. This could also start deliberations around whether and how the government should distinguish between regulating blockchain technology applications in the public and private sectors. Bitcoin and other cryptocurrencies are in an embryonic state as both a technology and a community of users. Therefore, the IMC Report will have a massive chilling effect on the community, deterring individuals and small businesses from using it to transact business. To avoid overly broad and strong regulation of the market, law-makers must ensure that they involve a variety of stakeholders in the regulatory process, so that their vision and needs can be fairly balanced with government interests. The government should work closely with owners of crypto-asset businesses, users, miners and advocates when creating and enforcing law. The Bitcoin Foundation is an example of an

133 Naimesh Sanghvi, You need to Respond to IAMAI Point by Point: Supreme Court Directs RBI, gives two weeks, 22 August, 2019
134 Kevin Helms, RBI’s Power Over Crypto Challenged at Length in Indian Supreme Court, 14 August 2019
American advocacy entity with a vested interest in the technology’s future and merits special attention from law-makers. A similar effort by Indian cryptocurrency entrepreneurs is the Digital Asset and Blockchain Foundation of India (DABFI), while the Blockchain Foundation of India is a community effort to promote the growth of blockchain-based initiatives in India. Bitcoin is open by nature and its survival is reliant on public contribution and support. Giving technology advocates “a seat at the table” when creating laws for a technology has historically been very successful. Organizations like W3C and ICANN played a vital role in creating sound regulation during the Internet’s early years and have maintained ownership of and advisory roles in many parts of the Internet. Similarly, users and advocates of Blockchain technology and its various applications including cryptocurrencies, should be empowered to take this kind of advisory role to law and policy makers, in promoting understanding of how the technology works, what problems it could solve and its applications. It is likely that such users and advocates are more nuanced in their understanding of country-specific and sector-specific challenges, as well the general risks and regulatory hurdles faced by counterparts in across the world. Given that most lawmakers are not programmers or technologists, technically qualified advisors inform and counsel them on the implications of potential legislation.  

As stated previously, in the case of India, the IMC did not comprise of diverse stakeholders and only represented the Central Government through Financial and other Regulatory Bodies. As such, the Report has been criticized by crypto-enthusiasts on various counts for inaccuracy and lack of reliable empirical data that formed the bases of their conclusions and recommendations.

2. Promote R&D and Legal Certainty for Blockchain Applications
To better understand blockchain and crypto-assets, regulators should set up specific committees or working groups that work to understand and classify emerging products and services as well as promote evidence-based adoption of the technology. Inherent to the mechanism of crypto-assets is the reality that many actors are involved with different roles, and, thus, different uses are made of them. Indeed, cryptocurrencies display certain features enabling it to function as a method of payment like any other currency, and alternatively as a speculative investment or even otherwise. Because the characterization will

---

135 See generally, Thomas Alcorn, Adam Eagle and Ethan Sherbondy (MIT), *Legitimizing Bitcoin: Policy Recommendations* p. 17
dictate the regulation, it is necessary to look at the various uses made and tie them to the appropriate regulations. In the case of India, as previously mentioned, where crypto-assets other than security tokens fall into a regulatory vacuum, classification would be an important step in arriving at a regulatory framework.

The committees or working groups mentioned above could have Members who are blockchain engineers, academics, government representatives and venture capitalists among others. Advisors could be representative of leading Universities that are publishing peer-reviewed content in the field as well as key managerial personnel from information technology and computer science enterprises e.g. IBM and Microsoft.

In the case of working groups specifically, a few examples of useful areas of focus are acquisition management, cybersecurity, economic analysis, education and training, energy and financial and regulatory groups.

The first Working Group could explore new methods, tools and techniques to use blockchain technology to establish secure and trusted processes for government contractors and acquisition authorities.

The second group could identify, study, and develop informative materials to improve the body of technologies, processes and practices to protect networks, computers, programs and data from hostile attacks, damage or unauthorized access.

The third group could evaluate the economic impacts of technologies involving blockchain and to offer impartial economic advice.

The fifth group could identify unique problem sets and challenges faced by public and private entities regarding energy supply, distribution and regulation while exploring innovative distributed ledger technologies to address these challenges to increase the efficiency, security, resilience and sustainability. Considering energy-related concerns were raised by the IMC in their Report, this could be of particular interest.

The last group could focus on the current day and emerging regulatory demands with Blockchain technology and the financial and payments sectors. This working group could encourage Blockchain companies, government regulators, law enforcement, and professionals in the financial regulatory and financial crimes space to contribute to ongoing debates surrounding dynamic and transient aspects of the technology.


137 See generally, Government Blockchain Association’s Working Groups. https://www.gbaglobal.org/working-groups/
An ad-hoc representative forum for experts that connects these stakeholders could be useful in not only promoting R&D in these areas but the Indian government may consider doing so even to inform the decision of the Government in regards to their regulatory responses to IMC Report going forward. However, unless the decision-making bodies are themselves representative of or at least comprise of these stakeholders, the responses of the Government may not be reflective of the needs of the persons most affected by the rules, even if they are informed by them (procedurally).

Efforts such as these should rely on interagency communication and coordination to ensure agencies do not arrive at conflicting decisions on the status and regulatory approval of these emerging technologies and their applications. Also, for everyday users to place trust in blockchains, they must be confident the information can be used in legal disputes. However, whether blockchain transactions and user signatures on blockchain-based accounts are legally binding is not settled law.  

3. **Equip ecosystems to support Blockchain through strategic partnerships**
   
   Regulatory approval can strongly impact the success of any distributed infrastructure implementation. For example, developing a distributed ledger to assist in the clearing and settlement of financial assets may involve custodial considerations, especially if assets are considered to be held on the network at any point. These custodial considerations may require a party to submit to regulatory requirements, which in turn could increase the compliance costs of such a system. On the other hand, a well-designed, standardized, automatically reconciled ledger could provide immediate real-time access to the relevant regulator for all partner institutions on the network. This could prove to save considerable costs and outweigh the additional compliance costs involved in establishing the system. Any solution will ultimately need to fit into an organization’s existing financial ecosystem. Considering this fit beforehand will improve the integration process later, should the concept prove successful.

   Additionally, many technological partners offer different applications of distributed infrastructure technology. Choosing the partner that fits a business need and desired configuration is vital to the technology’s individual success.  

4. **Consider diverse privacy issues during implementation**

Trading assets on an open blockchain may significantly cut costs, but it is not a practical solution if all transactions are observable by all parties in the system.

---


Consequently, the design of the technology itself will need to be reviewed depending on the application of choice. Furthermore, moving any product or service from a centralized to a decentralized mode of operation will have vast impacts on an entire organization. A business’ front office, operations, compliance, tax, accounting, legal and technology offices are likely to be involved. Any strategic identification of opportunities to improve a business using this technology will therefore need to consider the end-to-end operational impact of each solution.

Regarding an individual’s privacy rights, both the ICCPR and the ECHR prohibit intrusions upon the privacy of persons unless those intrusions are made in accordance with law that is sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. The imposition of financial surveillance upon every user of cryptocurrency, regardless of their particular circumstances, would probably fail to meet this international legal standard.  

One of the biggest issues with trying to build personal privacy protection with blockchain is the fact that privacy and protection are two very different things. Privacy is one’s ability to determine what type of information is collected about them. Protection is how well the data is secured once it is has already been gathered. The first part, privacy, is a right of the user. (A right that is often violated in today’s digital culture.) The second is the responsibility of the data gatherer. Both privacy and protection are important, but blockchain does one part far better than the other. Because blockchain is immutable, it means that a user will never have the option to go back and “erase” certain parts of their personal history if they wish to remove it from the blockchain itself i.e. the fact that X shopped for a certain book title on Amazon should not exist in the data ether forever. But with blockchain, it would. This single issue already defies the EU’s General Data Protection Regulation, which says that all users have the right to be “forgotten”. In this sense, blockchain is good for security but bad for privacy.

Blockchain participants can be identified using their public keys and IP addresses, among other identifiers, and transactions can be seen by all participants (this

---

140 Neeraj Agrawal, The world’s regulators are racing to develop blockchain policy, 1 August, 2016, recoverable at https://coincenter.org/link/the-world-s-regulators-are-racing-to-develop-blockchain-policy

141 Daniel Newman, Could Blockchain Solve Our Growing Privacy Issue?, 8 May 2019
is an essential feature of blockchain technology). Since blockchain is a new technology, most existing privacy laws around the world, including the Indian IT Act, would not contemplate privacy protections for blockchain participants in this sense.

Most Internet privacy laws deal with a situation where a website/app collects personal information from an end user. The IT Act, for instance, regulates the collection, use, and disclosure of sensitive personal data or information by a body corporate which owns, controls or operates a computer resource. So though participants would have these ordinary Internet privacy rights, such rights will likely not extend to the blockchain because there is no centralized organization collecting information.

If we look at the IT Act’s language (section 43A), privacy on the blockchain would likely not be available because there is no single “body corporate” collecting user information and “own[ing], control[ling] or operat[ing]” a computer resource (unlike a regular web service does, for instance). Rather, information is shared with all blockchain participants, and control is decentralized.

Lawmakers could look at mandating that blockchain operators (in situations where there are centralized operators) if technically feasible, maintain privacy to a certain degree without compromising accountability.

Under India’s draft personal data protection bill, all ‘data fiduciaries’, or parties who determine the purpose of processing personal data must protect the individuals’ digital privacy and grant them certain rights. The Bill also entails processing of personal data only for a specific and lawful purpose and such processing must be done with consent. It is pertinent to note that the Bill only governs the use of ‘personal data’, or data which is identifiable to an individual.

Data on a blockchain is likely going to be incompatible with some provisions of the Bill, if personal data is stored on the blockchain. The Bill has obligations requiring the deletion of data once the purpose of processing is achieved. However, this is not possible in an immutable ledger. The Bill also grants the data subject the right to modify and correct their personal data. However, the immutable nature of the blockchain may make this difficult. If data stored is not personal in nature, or the blockchain is permissioned in nature, these challenges maybe overcome.

5. Consider systemic inefficiencies and hidden costs arising from public ledgers as opposed to private ones

---

142 Supra, at n.32, pp.25-26
In a fully decentralized setup, access to the ledger is public. Anyone is allowed to access the entire history of data transactions, create new transactions and validate new blocks so, while activity recorded in a permissioned ledger is validated by participants on an equal basis, public ledgers require arbitrary parties to validate activity. Consequently, an incentive to validate transactions is required. This incentive is based on most public ledgers’ designs, which require tokens to perform functions on the network. Consequently, these tokens’ value is based on market demand. When tokens are provided as an economic incentive to participants who assist in the validation process, public ledgers can operate in a fully decentralized manner. This leads to three considerations. Firstly, to engage with the ledger, participants will need to purchase tokens at the market price. Consequently, basing a company's operations on a public infrastructure has monetary exchange risk implications that are not present in centralized infrastructures or permissioned ledgers. Secondly, the validation process itself for most public ledgers can be very inefficient. To prevent activity from being arbitrarily validated and to secure the ledger against attack, validating activity requires the solving of complex calculations. Because the token rewards are available for validating this activity, massive industrial mining operations in the bitcoin world are dedicated to computing the calculations. This has led to an issue of centralization of parties validating the activity and substantial amounts of energy expenditure. The challenge is also that more efficient and decentralized validation mechanisms that are being developed have not yet been broadly adopted and can be difficult to adopt, particularly as the large-scale miners have businesses to lose. Thirdly, when changes are required for the code that allows the ledger to run, public ledgers, if open to community development, cannot move as quickly or efficiently to upgrade or improve as development that is closely managed.

6. Combatting Illegal Markets

If businesses accept cryptocurrencies, the government could treat the currency as cash for all intents and purposes. Unlike credit or debit cards, when individuals make purchases using Bitcoin they are not required to disclose any personal information. As with the "cash model", the government should combat illegal markets by targeting unlawful businesses, rather than consumers. By working with Bitcoin experts and developing algorithms to analyze the ledger, the government could spot money laundering and illegal trade in Bitcoin more effectively than they can in cash.

---

143 Id. at n.94
144 Id. at n. 93, p.23
7. **Ensure regulatory neutrality**

Policymakers should adopt technology-neutral rules that create a level playing field for innovation. They should strongly support efforts to increase digitization and look to the unique benefits of a technology and the particular challenges of a project when deciding what technology to adopt. In addition, regulators should try to apply the same rules to different technologies used to offer similar products and services. Regulators do not necessarily need regulations simply because blockchain applications are different. When confronting a new technology or business model, regulators should first look to existing rules to see whether they apply to emerging applications, which would create a level playing field between the traditional and emerging technology or business model. Clearly, all technology applications are not the same. The concerns associated with money-laundering abuse from unregulated digital currencies may not be the same as from centralized-database-driven traditional banking. Wherever there are differences in technologies, policymakers should establish rules that recognize the risks that are distinct—or irrelevant—to particular applications. Unfortunately, with respect to virtual-currency businesses that often function similarly to mobile-payment businesses and international-transfer services, New York drafted its Virtual Currency (or VC) License, called BitLicense, subjected virtual-currency businesses to arduous anti-money laundering reporting requirements making an arbitrary distinction.

In the case of India, the IMC has outlawed private cryptocurrencies altogether when in fact, as suggested by Nishith Desai Associates’, a law firm that was invited by the Government of India to present their suggestions for a regulatory framework for digital currency, crypto-asset businesses could have been licensed by introducing a simple government notification bringing such crypto-asset business activity under the Prevention of Money Laundering Act. This would be the procedurally less complicated option among two options. Licensing businesses in the country may be done either by introducing new legislation or framing administrative regulations under existing legislations. With one fell swoop, that notification would have brought crypto asset activity within a well-established AML regime, operating on par with the financial sector.

As per the three authors of the paper, it would have been wise to divide the crypto assets into three types i.e. ‘payment tokens, security tokens, and utility tokens’. The paper explains - “For the purpose of legal analysis, all crypto...

---

145 Id. at n.94
assets are not alike, and the implications of each should be assessed on a case by case basis.

The proposal suggests that the second type of the crypto assets i.e. ‘security tokens’ should be taken care and regulated by the ‘Securities and Exchange Board of India (SEBI), as per the ‘Companies Act.’ The lawyer further elaborated-“The trading activity with regard to all other crypto assets falls in something of a regulatory vacuum, although existing laws like the Consumer Protection Act continue to apply to a significant extent.”

The ‘vacuum’ which the lawyer is referring to can be curbed with the help of ‘Know your customer’ and Anti-Money Laundering process. The final aspect of the paper was ‘Self Regulation’. Back in 2017, the authors of the paper submitted a paper about self-regulations to the previous government committee on crypto assets.

For the previous paper, the representative noted that the previous committee’s report was not made public and so they did not know how that committee responded to the suggestion for self-regulation.

If these approaches were to be considered, the IMC’s proposed ban can be thought of as needlessly excessive.

8. **Robust addressal of regulatory vacuum and clear segregation of crypto-assets**

For the purpose of legal analysis, all crypto-assets are not alike, and the implications of each should be assessed on a case-by-case basis. Broadly, crypto-assets can be considered to be of three types: payment tokens, security tokens, and utility tokens. Those security tokens which amount to ‘securities’ will be regulated by the Securities and Exchange Board of India and under the Companies Act. India presents somewhat traditional challenges when it comes to trading in crypto-assets because of a regulatory vacuum. This vacuum should be addressed by introducing: (a) a Know Your Customer / Anti-Money-Laundering (KYC/AML) regime, and (b) a licensing regime, for crypto-asset business activity. As regards KYC/AML, businesses dealing with crypto-assets, i.e., providing custody or trading services, can be included within the framework of the Prevention of Money Laundering Act by Central Government notification.

As regards licensing, a new licensing regime for crypto-asset business activity can be evolved by new legislative provisions. administrative regulation under various

---

laws such as the Consumer Protection Act, Payment and Settlement Systems Act, Non-Banking Financial Company (NBFC) regime, and/or Securities Contracts (Regulation) Act; and/or, statute-backed self-regulation. Administrative regulation under existing laws will be limited by the current scope of the parent statutes, while new legislative provisions may be able to better address the unique nature of crypto-asset activity. In either case, responsibility for such licensing or oversight should be clearly assigned to a given regulatory body to avoid jurisdictional ambiguity. Since SEBI has competence as regards investor protection, it is one option that can be considered in this connection.

Meanwhile, existing laws such as the Consumer Protection Act, Foreign Exchange Management Act, Indian Penal Code, Information Technology Act, Payment and Settlement Systems Act, Prevention of Money Laundering Act, Prize Chits and Money Circulation Schemes (Banning) Act, deposits-related laws, securities laws, and tax laws should be actively enforced with regard to crypto-asset business activity, since much of such activity is already covered by these laws. The applicability of some of these laws may also be further clarified or fine-tuned with respect to crypto-assets.

**CHALLENGES AHEAD**

The practical challenges associated with harnessing Blockchain technology are many and frequently cited. The more obvious issues that come up in envisaging widespread implementation of blockchain technology surround lack of adequate and widespread consumer awareness, teething issues and need for entire ecosystems with infrastructure and technically competent manpower to advance with, adapt to and support Blockchain. Without these, it would be difficult to fully realize any potential advantages but other particular challenges concern privacy, cybersecurity and large-scale short-term energy consumption until (if at all) blockchain is made more mainstream.

Bitcoin exchanges and participants have been subjected to security breaches numerous times, including a January 2018 hack of the exchange CoinCheck, resulting in losses amounting to over USD 500 million. The recent Ethereum DAO hack proves that vulnerabilities can exist outside of the Bitcoin implementation of blockchain technology too. Though the fundamental technology underlying the blockchain has rarely been questioned on security grounds, the implementation by participants, exchanges, etc has sometimes not been watertight. One security weakness at a fundamental level is the dependency on participants’ private keys and the total
absence of options if there is a permanent loss of it. The transparency that is essential to the blockchain, combined with the ability to trace participants' real identities, can lead to serious privacy implications and lastly, attention has also been drawn to the substantial energy consumption by blockchain networks, because of the computationally intensive process of mining/verification. However, newer (algorithms) are expected to improve energy efficiency over the long run.\footnote{Id. at n.32, p.33,34}

**CONCLUSION**

The duplication of data hosting and processing across every node in the blockchain network dramatically limits both capital efficiency and scalability to real-world data and transaction volumes. The consensus methods by which blockchain nodes agree upon the shared transaction ledger rely upon economic incentives for—and the rationality of—its participants, posing risks to settlement finality and the security of the network in the face of hostile actors. Perhaps most problematic, blockchain faces the opposing obligations of keeping mission-critical electrical and financial data confidential, while making it visible to its fleet of validator servers, which may operate outside of a corporate firewall. Moving this confidential data off-chain would eliminate the issue, but significantly reduce blockchain's role in primary transactive market functions. Cryptographic techniques to allow blockchain to meet these opposing obligations exist, but haven't been fully explored.\footnote{Ben Hertz-Shargel and David Livingston, *Assessing blockchain's future in transactive energy*, 23 September 2019}

However, the applications of blockchain technology have elicited excitement that has resulted in a diverse and interesting set of test cases that attempt to determine when a decentralized application is better than its centralized counterpart. While some of the case studies discussed may ultimately fail, many will succeed in showing blockchain’s strength in eliminating trusted intermediaries while maintaining trust in an official system of record.\footnote{Id. at n.96}

In this period of uncertainty regarding the scalability and sustainability of Blockchain, policymakers should adopt and demonstrate a pro-innovation stance in relation to blockchain applications.

In relation to a governance structure, while creation of a regulatory body similar to the MDIA could be both desirable and useful in the Indian context given how ripe the ecosystem is for innovative technologies, this process would be procedurally and substantively complex. It would require Legislative and Executive action, an analysis of the composition of such a body, their enumerated and unenumerated powers and

\footnote{Id. at n.32, p.33,34}
what conditions need to be met in order for the government to provide regulatory approval. This is separate from the inquiry as to the obligations and rights of the entity intending to be regulated. Ultimately, a stance needs to be arrived at that balances supporting and advancing technological innovation, public benefits that could accrue and the government’s interests in testing Blockchain technology to see if it can be implemented and scaled to produce long-term solutions in any sector where it can be applied. Also, in the Indian context, it is socio-politically challenging to conceive of successful implementation of Malta’s system of accepting applications for licensing on a voluntary basis.

Supporting Blockchain whilst simultaneously taking an anti-crypto stance could cause the blockchain as a system to be rendered either impotent or severely restricted (depending on the blockchain implementation). This has been recognized by several global experts including Ethereum co-founder Vitalik Buterin. Such tokens act as an incentive to the blockchain participants to verify transactions, and hence preserve decentralization, which is the very breakthrough of blockchain technology. As a result, it may not be the most useful to try and promote blockchain on the one hand, and severely restrict tokens on the other hand. In any case, it is imperative that the regulators adopt a nuanced framework after ensuring that they are well-informed about the technology and its benefits, and that public and private sectors collaborate to arrive at well-balanced policy outcomes.

In India, the RBI has taken an important pro-Blockchain step by announcing the Proposed Sandbox Framework. The expectation is that a ‘learning by doing’ approach adopted would allow it to take an empirical approach towards fintech innovation, while both the RBI and RS participants can learn from the sandbox testing to improve regulations and fintech solutions respectively. Additionally, the RS can potentially yield better outcomes for consumers through an increased range of products and services, reduced costs, and an improvement of financial inclusion. However, the Proposed Framework also presents some challenges such as a high net-worth requirement, ambiguous phrasing of eligibility conditions and other requirements, and the inclusion of crypto-asset activity, which is essential to blockchain technology, in its negative list.

---

150 Id. at n.32, p. 35.
151 Id. at n.88