Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BANGALORE SINGAPORE MUMBAI BKC NEW DELHI MUNICH NEW YORK

The Blockchain

Industry Applications and Legal Perspectives

November 2018

The Blockchain

Industry Applications and Legal Perspectives

November 2018

ndaconnect@nishithdesai.com

Contents

1. Introduction

Most people have heard of Bitcoin, the revolutionary decentralized, trustless payment system. But Bitcoin is just one application of a broader concept known as blockchain technology, or simply, 'the blockchain.' Blockchain technology made Bitcoin achieve a goal that many virtual currencies before it could not. In traditional payment systems, centralization is necessary to keep track of spending, and prevent 'double spending'of the same units. Users of the payment system must hence entirely trust these central authorities – usually, governments and banks. While there were virtual currencies before Bitcoin, including crypto-assets (i.e., instruments whose transactions are secured by cryptography), they remained centralized.

The genius of Bitcoin was to distribute the ledger containing all Bitcoin transactions among each user(or 'node') in the network. Hence, every single transaction is authenticated by every single user (this is called'proof of work'), and there is no centralized authority required for this. This is why the blockchain is often called a 'distributed ledger', and is a subset of distributed ledger technology. We have separately published a research paper on the legal and tax consequences surrounding Bitcoin and other crypto-assets.[1]

This research paper focuses on the aspects of blockchain technology other than the simple value transfer aspects (e.g., Bitcoin transactions) and the trading of crypto-assets on exchanges. Blockchain technology has attracted a lot of industry attention over the past few years. It has been proposed as a solution in areas ranging from finance to real estate to energy. Finance has probably been the sector which has given it the most attention. Nearly all the world's major financial institutions including Barclays, BNP Paribas, Goldman Sachs, J.P. Morgan, Morgan Stanley, NASDAQ, and Wells Fargo have explored the application of the blockchain to their businesses, independently and through consortiums such as the Enterprise Ethereum Alliance.[2] Big name technology and consulting firms heavily involved in blockchain projects include Deloitte, Google (DeepMind), IBM, KPMG, and Microsoft.

The Indian fintech space has seen considerable developments take place over the past few years. The Finance Minister post his Budget Speech earlier this year when he stated that "*the government will explore the use of blockchain technology proactively for ushering in digital economy*".[3] An inter-regulatory Working Group by the Reserve Bank of India (RBI) has been constituted to study regulatory issues relating to FinTech and Digital Banking in India.[4] Notable states that have launched a host of initiatives to implement blockchain include Andhra Pradesh, Karnataka, Maharashtra and Telangana. In a bid to 'strengthen cooperation in promoting FinTech innovation', the Maharashtra government and the Monetary Authority of Singapore (**"MAS"**) recently signed a Memorandum of Understanding.[5]

Indian banks that ran early blockchain pilots include ICICI Bank, Yes Bank, Kotak Mahindra Bank, and Axis Bank. In addition, Infosys, TCS, Wipro, and Cognizant were reported to have made significant investments in expanding their capabilities in the technology. Infosys and TCS were in fact the first two large companies globally to have rolled out the use of blockchain in core banking platforms.[6] The use of blockchain in a variety of other sectors continues to be explored in several industry verticals. Governments too

1. Latest draft available at http://www.nishithdesai.com/information/ research-and-articles/research-papers.html (last visited October 24, 2018)

2. E.g., http://www.r3cev.com/about/ (last visited October 24, 2018); http://entethalliance.org/ (last visited October 24, 2018)

3. https://www.indiabudget.gov.in/ub2018-19/bs/bs.pdf (last visited September 14, 2018)

4. https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=43097 (last visited September 14, 2018)

5. https://www.opengovasia.com/articles/mas-signs-mou-with-state-government-of-maharashtra-in-india-for-fintech-cooperation (last visited September 14, 2018)

6. http://www.livemint.com/Companies/bXjPtlHZRK46FQVb2hxhyN/TCS-throws-weight-behind-blockchain.html (last visited September 14, 2018)

have shown interest in the technology for their own operations, with the U.K. and Delaware governments being significant backers.

Significantly, the RBI's research arm, the Institute for Development and Research in Banking Technology (IDRBT) released a report in January 2017 confirming the cost-savings, transparency, and efficiency advantages of the technology and recommending that the time is ripe for its adoption in India. As part of its activities, the IDRBT is engaged in a research project entitled "Distributed Center of Excellence for Blockchain Technology", sponsored by the Ministry of Electronics and Information Technology (MeitY). Key objectives of the project include *inter alia* evolving a blockchain ecosystem around R&D organizations, Government departments and Academia; conducting research on issues and challenges related to blockchain usage in identified application domains and enhancing capacity building in blockchain technology.[7]

Businesses across verticals should therefore be actively assessing how the blockchain can help streamline tasks for them. At the same time, since the technology has various trade-offs, they should be tuned to look past the hype and only consider implementations of this technology when they present a true value addition. We hope this paper goes some way towards this.

The paper briefly describes the working of blockchain technology, discusses the current state of the art in industry, provides a legal and regulatory perspective, and concludes with a list of challenges and the way forward.

7. http://www.idrbt.ac.in/externalprojects.html October 24, 2018

2. How Blockchain Technology Works

To understand its industry applications and legal ramifications, it is important to grasp how blockchain technology works.

One can think about the blockchain as a ledger of transactions. A physical ledger is typically maintained by a centralized authority, not by market participants. The blockchain, however, is a distributed ledger which resides on each participant's device. Each individual copy is updated whenever a transaction or set of transactions is completed. The device of each participant or user is usually referred to as a 'node,' which forms part of a network of nodes.

not need to rely on a third party for transparency and authenticity. The blockchain ensures the transparency and integrity of transactions purely through mathematics, and not trust. The type of transaction varies depending on the application of blockchain technology. In Bitcoin, for instance, each transaction is a transfer of a certain value of Bitcoin between participants, and every transaction is recorded on the Bitcoin blockchain. However, the transactions could also be for other uses, like fiat money transactions or real estate title transfers, as discussed later in this paper.

Source: http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

The blockchain is unique because every node must authenticate every transaction in the network. This is why when a new node joins the network, the entire record of transactions is downloaded onto its system (e.g., for Bitcoin, this process takes over 24 hours). From then on, it will join the other nodes in updating the ledger as and when new transactions are authenticated. The process of authentication is based on advanced cryptography, and is widely considered to be secure in and of itself.[8] Hence, participants do

I. Technical Perspective[9]

To delve into some technical detail, when a node 'X' seeks to carry out a transaction (e.g., send 5 units from X to Y), it sends a transaction message,

8. *E.g.*, http://enigma.mit.edu/enigma_full.pdf. However, aspectsof the *implementation* of blockchain technology have been foundvulnerable on many occasions (e.g., http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millionsallegedly-stolen-2016-6?op=1) (last visited September 14, 2018), and this will be discussed inmore detail subsequently in this paper.

9. The technical explanation here is on the basis of the blog and video, "How Bitcoin Works Under the Hood" by Scott Driscoll, available at http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html (last visited September 14, 2018)

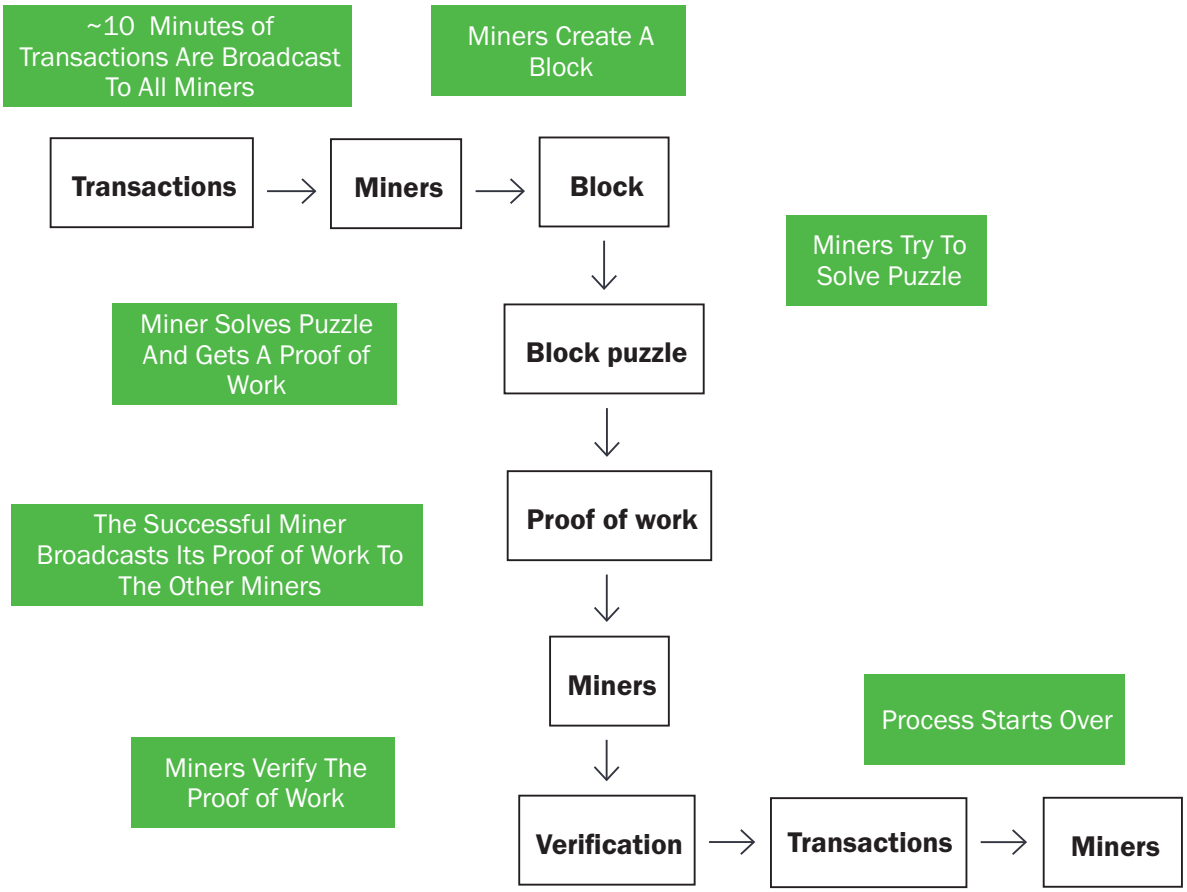
represented in computer code, to the network. To become an accepted transaction recorded on the blockchain (in this case, for 5 units to be considered transferred), this transaction message must be authenticated by every node in the network. The authentication is done on the basis of the digital signature accompanying the message.

Every node possesses a public and private cryptographic key. The public key is akin to a mailing address, to enable other nodes to communicate with it (send money, sign contracts etc.). The private key is akin to a secure password that only its holder knows. Whenever a node sends out a transaction message, a digital signature is generated using its private key and the message. The digital signature enables other nodes in the network to verify that the sender is really the holder of a given private key. Digital signatures hence enable the network to verify the authenticity of messages, preventing fraud by impersonation. Once the digital signature of a transaction is authenticated, it gets pooled with other authenticated transactions into a 'block.' After the first block, a series or 'chain' of blocks gets formed, hence leading to the term 'blockchain.'

This is where a second level of cryptography comes in. To prevent fraud and double spending, it is important that the order of transactions is authentic. This is because a transaction message reaches different nodes at different points in time (owing to varying network speeds). So, without a secure mechanism to order transactions, a buyer could send a payment, and before that message reaches the seller, the buyer could send the amount back to itself. Some nodes in the network may receive the second message before the first. The seller may have relied on the original payment message and shipped the goods, only to be left then without payment! This is because the buyer was able to capitalize on the varying times at which each node received the transaction messages, hence effectively manipulating the order of transactions. Several cryptocurrencies prior to bitcoin suffered from this problem. It was hence necessary for there to be a secure way of determining an order of transactions which could be accepted by all nodes as true. Blockchain technology achieves this.

It establishes a system through which the order cannot be manipulated unless the majority of the computing power in the network colludes to make it so (even then, manipulation is not guaranteed). Every block is encrypted using a cryptographic hash function. Transactions in the block can only be read and made sense of after the block is decrypted. But the text of each block relies on the previous block, so to decrypt a given block, the previous block must be known. This prevents the chain splitting into numerous parts,[10] and results in a mechanism to achieve consensus on the ordering of transactions. Because of the strength of the cryptographic hash function involved, a great deal of computing power is required for decryption. Every node in the network participates to work towards decrypting each block. This process is known as 'mining' and nodes doing this are called 'miners'. Incidentally, miners in the Bitcoin blockchain are rewarded for their work with Bitcoin value. This is what incentivizes them to keep authenticating transactions. When there are no more or too few Bitcoins to mine (the system is designed such that will be no more 'new' Bitcoins in 2140), nodes may be paid transaction fees.

10. In rare cases, there may be parallel chains for a short length of time, but since nodes follow the longest chain, this matter is resolved quickly.



Source: Business Insider, bullfax.com

The "work" involved in mining is not manual human work, and is performed by each node's device without human intervention. In simple terms, it is large-scale trial-and-error guesswork until the correct mathematical answer is reached. Therefore, like with digital signatures, the order of transactions is decided by mathematics and not trust or third party discretion. Once a block is authenticated, the ledger in all nodes is updated with the new transactions in that block, and so forth.

This discussion helps in revealing some features of the blockchain that are relevant to its industry applications and legal implications.

II. Public and Private Blockchains

Both public and private blockchains have similarities in that they are both distributed networks secured using cryptography and consensus protocols, and they are both usually immutable. However, as the words 'public' and 'private' suggest, there is a significant distinction in terms of who is allowed to participate in the network, execute the consensus protocol and maintain the shared ledger.[11]

The best example of a public blockchain is the Bitcoin blockchain, where anyone, anywhere in the world can read and write data on it.

In a private blockchain, only trusted and known participants are allowed to read or write on it. It could be used by a finite set of participants such as a consortium of financial institutions. Private blockchains are usually just a distributed ledger and may not have the decentralization benefits of blockchain as such. Some have criticized private blockchains as not being an innovation, but rather an implementation of long-existing technology.[12]

11. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/ (last visited September 14, 2018)

12. https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/ (last visited September 14, 2018)

Some blockchains follow a hybrid model; e.g., XinFin is built on both Ethereum, a public blockchain, and Quorum, a private blockchain.[13]

III. Looking Past the Hype[14]

While 'blockchain' is a buzzword today, the technology may not be suitable for all use-cases. Below we present some contrarian perspectives on the blockchain revolution. While we remain believers in the breakthroughs of blockchain technology, this article tries to convey that it is not suitable for all the scenarios it is often touted for.

First, it becomes necessary to understand the core characteristics of a blockchain. Blockchain is a decentralized ledger. It is essentially a system of distributed 'account books' which are continuously maintained at multiple locations and continuously synced. Transactions on the blockchain are reflected as secure changes in the ledger. This technology enables changes to the ledger to be made securely and transparently without the need to trust a single entity. Another attribute of how the blockchain works is potentially problematic, this is the character of 'immutability'. Once a transaction is processed on the blockchain, it cannot be reversed. While this ensures that the system is verifiable as transaction, it also results in the inherent difficulty in reversing fraudulent transactions.

Keeping the above in mind, the blockchain is meant for very specific types of transactions. By this nature – the blockchain is suited for transactions where (i) there are multiple parties and transactions, (ii) the transactions need to be recorded and verified in a permanent and transparent manner, (iii) where there is no central intermediary, and (iv) where the transactions need to be trustless i.e., not all parties trust each other.

An example where the blockchain is not very suitable would be for one-to-one transactions between trusted parties, who are protected by, for instance, a prior legally enforceable agreement or where the transaction occurs physically face to face, such as buying goods from a retail store.

Even if there is a multiplicity of parties, where there is a reliable, government-mandated/ trusted intermediary present in the transaction process, there is may be no need to tamper with an existing centralized system. An example of such a system is the retail payments system in India which is operated by the NPCI (National Payments Corporation of India) in co-ordination with the RBI. Systems such as Immediate Payment Service (IMPS) and Unified Payments Interface (UPI) settle payments among all the banks and financial institutions in India, with NPCI as the operator of the systems acting as a trusted intermediary. In examples such as this, and in the case of trusted, reputed intermediaries like large e-commerce marketplaces or payment networks, centralization can often serve the intended purpose effectively.

One example where blockchain could be particularly useful is in a situation where there are multiple counter-parties and there is a lack of trust. Imagine a global network of buyers and sellers, which don't have a trusted intermediary between them. This network of buyer and sellers can use the blockchain (either in a B2B or B2C context) to securely and transparently facilitate transactions among each other without the need for trust. Blockchain is also especially useful in circumstances where there is no regulatory protection for the transactions, such as the protection of a domestic banking regulator. An example of this is a cross-border transaction where the jurisdiction of a regulator may not extend to the entire transaction and, therefore, the parties need to trust a network which provides math-based security like the blockchain.

Another point worth remembering is that the security of blockchain transactions is dependent on the private key. The storage of the private key to secure such transactions hence becomes critical. While blockchain technology is inherently more secure due to public key cryptography, it cannot entirely cover the risks caused by human error.

13. https://bravenewcoin.com/insights/hybrid-blockchains-the-best-of-both-public-and-private

14. This portion has been adapted from an article first published by firm members Vaibhav Parikh, Jaideep Reddy, and Arvind Ravindranath in CEOInsights India Magazine (June 2018).

Improper storage of the private key can lead to its compromise and consequently the compromise of transactions on the blockchain as well.

Transaction settlement time can also be an issue with the blockchain. Bitcoin (the first blockchain), has seen average transaction confirmation times ranging from as little as 8 minutes to as much as 8 days in times of network congestion!. While different algorithms used to implement the blockchain operate differently, there is a case of repetition of activities and infrastructure costs across nodes and an increase in energy consumption for the maintenance of the systems compared to a centralized system. This is because efficiency is (often) compromised in the interest of de-regulation and transparency.

The transparency of the blockchain system is also an attribute that can function as a double-edged sword. In some public blockchains (like bitcoin), every transaction that is made on the network is publicly available. While these transactions are usually linked only to pseudonymous wallet addresses, from a consumer protection perspective there is a significant loss of financial privacy as most users may not be technologically savvy enough to use de-identification tools. From a commercial perspective, a business like an algorithmic trading firm may be unwilling to share proprietary information (even if encrypted) on the blockchain as it may lead to potential disclosure of its trading strategies.

To counter these concerns of efficiency and financial privacy arising out of public blockchains like Bitcoin, many have started to bat for 'private' or 'permissioned' blockchain systems. These continue to operate as blockchains but have a degree of centralization in the interests of efficiency, privacy, and intervening in limited situations (to reverse transactions, for instance). It is these private blockchain deployments that have garnered a lot of attention for their use in traditional commerce like clearing and settlement, supply chain management, insurance, etc.

However, some, like computer science researchers Arvind Narayanan and Jeremy Clark, have criticized private blockchains as being nothing more than 'shared databases'. They argue that once the decentralization element of public blockchains like Bitcoin is removed, the technology remaining (e.g., cryptographically securing transactions) actually dates as far back as 1991! They argue that where there are only a few trusted parties participating (like a consortium of banks), other long-standing solutions like linked timestamping would be sufficient. For a single entity to use a blockchain would be even less relevant, because even if it rolls out a blockchain ledger, other participants would still need to trust that entity (this is because just as it may manipulate a traditional ledger, it can manipulate the blockchain ledger since all nodes are within its control). The recent hype regarding the blockchain, may therefore be overdone by quite some margin!.

Therefore, while considering potential implementations of blockchain technology, decision-makers should consider whether they need a decentralized, trustless and disintermediated solution. If not, other existing technology can likely better serve the purpose and the costs of implementing the blockchain may outweigh the perceived benefits.

3. State of the Art in Industry

I. Applications

This section discusses some notable existing and proposedindustry applications of the blockchain.

A. Financial Services / Fintech

i. Banking

A report by Deloitte identifies 'trade clearing and settlement' as one among two use-cases of smart contracts that were most immediate to market.[15] This makes the banking industry a huge potential market for the blockchain. As mentioned in the Introduction, Infosys and TCS are the first large companies to roll out the use of blockchain technology in core banking platforms.[16] A recent report by the innovation fund of Santander Bank predicted cost-savings of USD 15 to 20 billion by 2022, as a result of blockchain technology reducing financial infrastructure costs.[17] Smart contracts add to the ledger functionality of blockchain technology, allowing many kinds of self-executing instructions to be programmed into the blockchain. With the blockchain as the single source of truth, requiring no manual verification, smart contracts can automate approval workflows and clearing calculations.[18] These processes are cost- and labor-intensive, and are subject to delay and human error.[19] This is exacerbated by each bank / financial institution having to independently process transactions.[20]

Several financial institutions, investment funds, and financial infrastructure bodies have taken notice of the potential impact of blockchain technology on clearing and settlement. The 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 Khosla Ventures, SV Angel, Citigroup, JP Morgan, and Santander. The Depository Trust & 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 (repo) transactions.[21] 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.[22]

Closer home, as mentioned above, Axis Bank, ICICI Bank, IDFC Bank, Kotak Mahindra Bank, and Yes Bank have carried out blockchain pilot runs for vendor financing and international trade finance.[23] In February 2017, India's largest bank, State Bank of India, announced a consortium "Bankchain" to implement blockchain technology, which now includes over 30 commercial banks, including most of India's largest banks.[24] Presently, Bankchain has 8 live projects with representation from 28

15. https://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html. The other use case is supply chain and tradefinance documentation, mentioned under the 'Legal Services'section subsequently. (last visited September 14, 2018)
16. "*A core banking system is the back-end data processing application for processing all transactions that have occurred during the day and posting updated data on account balances to the mainframe. Core systems typically include deposit account and CD account processing, loan and credit processing, interfaces to the general ledger and reporting tools.*" http://www.gartner.com/it-glossary/core-banking-systems/ (last visited September 14, 2018)
17. http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-aboutsmart-contracts/; http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf (last visited September 14, 2018)
18. http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-aboutsmart-contracts/ (last visited September 14, 2018)
19. Id
20. Id.
21. http://www.dtcc.com/news/2016/march/29/dtcc-and-digital-asset-to-develop-distributed-ledger-solution, http://www.dtcc.com/news/2017/february/27/dtcc-and-digital-asset-move-to-next-phase (last visited November 15, 2018)
22. https://www.euroclear.com/newsandinsights/en/press/2017/2017_mr-07-Liquidshare.html (last visited November 15, 2018)
23. https://qz.com/966629/blockchain-technology-is-the-coolest-thing-in-indian-finance-right-now-but-nobody-really-gets-it/ (last visited November 15, 2018)
24. http://www.bankchaintech.com/members.php (last visited November 15, 2018)

Indian banks including State Bank of India, ICICI Bank Ltd, Kotak Mahindra Bank Ltd, HDFC Bank Ltd and Yes Bank Ltd. 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.[25] The National Payments Corporation of India (NPCI) too had held an "ideathon," and set up a working group to help it understand the implications of blockchain technology.[26]

Interest has extended to the public sector too. Central bank and other government officials have been discussing the potential of blockchain technology at various international fora, such as the G20 and the IMF.[27]

In India, as mentioned previously, the 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."*[28] In April 2018, the RBI stated that it was exploring the possibility of a digitally issued fiat currency,[29] and in February 2018, a Working Group on FinTech and Digital Banking discussed the pros and cons of distributed ledger technology and digital currencies.[30] More detail on the Indian regulatory perspective is covered under Section 4 (**"Regulatory Reaction"**) below.

In November 2018, HSBC Bank in India settled an export transaction for Reliance Industries Limited using the blockchain.[31] 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.

Additionally, 'India Trade Connect' is a consortium led by Infosys which was joined by Axis Bank, ICICI Bank, IndusInd Bank, RBL Bank, Kotak Mahindra Bank, South Indian Bank, and Yes Bank, to address the trade finance process requirements of banks.[32] It is powered by Finacle Trade Connect, a blockchain-based solution for trade finance requirements that digitizes trade finance business processes and offers functionality including bill collection, letters of credit and invoice financing.

ii. Securities

In 2015, Nasdaq announced an enterprise-wide initiative to leverage blockchain technology.[33] Its first use was to *"offer efficient, fully-electronic services that facilitate the issuance, transfer, and management of private company securities."*[34] Significantly, in May 2016, it announced the 'Nasdaq Financial Framework,' which is an end-to-end solution for its financial infrastructure clients around the world, including traditional exchanges.[35] The Framework allows clients to leverage blockchain technology, as one of many other capabilities, including machine learning, for their individual needs. Nasdaq was one of the first multinational financial services companies to begin using the blockchain in a non-currency manner.[36] It stated that it sees

25. https://www.livemint.com/Industry/plB1lUobooCDVWyIkd8rOM/Banks-link-up-on-BankChain-to-exploit-blockchain-solutions.html (last visited October 16, 2018)
26. http://timesofindia.indiatimes.com/business/india-business/Next-Banking-Disruption-Lies-In-One-Open-Online-Ledger/articleshow/54318646.cms (last visited November 15, 2018)
27. https://cointelegraph.com/news/imf-vows-to-continue-devoting-attention-to-blockchain-cryptocurrency-in-fintech-drive, https://www.coindesk.com/g20-eyes-october-deadline-for-crypto-anti-money-laundering-standard (last visited November 15, 2018)
28. http://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf (lastvisited April 25, 2017)
29. https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574 (last visited November 15, 2018)
30. https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=43097 (last visited September 14, 2018)
31. https://timesofindia.indiatimes.com/business/india-business/hsbc-executes-indias-first-blockchain-pay/articleshow/66508206.cms
32. https://www.edgeverve.com/finacle/casestudy/india-trade-connect/ (last visited November 15, 2018)
33. http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196 (last visitedOctober 3, 2016)
34. Id.
35. http://www.coindesk.com/nasdaqs-blockchain-services-global-exchange/(last visited October 3, 2016)
36. http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196 (last visited October 3, 2016)

the blockchain as providing *"extensive integrity, audit ability, governance and transfer of ownership capabilities."*[37] Following in its lead, several other stock and commodity exchanges, including India's National Stock Exchange (NSE) and Bombay Stock Exchange (BSE), the New York Stock Exchange, the London Stock Exchange, the Japan Exchange Group, the Deutsche Börse, the Dubai Multi Commodities Centre, the Australian Securities Exchange, and the Sydney Stock Exchange have been investigating the potential of blockchain technology to varying extents.[38] In February 2017, the NSE, along with ICICI Bank, IDFC Bank, Kotak Mahindra Bank, IndusInd Bank, RBL Bank, HDFC Securities, and Blockchain startup Elemential, recently jointly conducted a Know Your Customer (KYC) data trial using the blockchain.[39] The NSE was also reported to be experimenting with the use of blockchain technology to ensure settlement guarantees.[40] Both the NSE and the BSE have in the past hosted blockchain events.

In August 2017, the Securities and Exchange Board of India (SEBI) announced the setting up of a Committee on Financial and Regulatory Technologies (CFRT) to explore the possibility of implementing blockchain in stock markets.[41] The terms of reference of the CFRT specifically envisage exploring DLT technologies.

In Japan, the Japan Exchange Group has reportedly already performed Proof of Concept testing for utilizing blockchain in its capital market infrastructure.[42] The Japan Exchange Group has published various white papers on the use of Blockchain and DLT in KYC processes and trade matching respectively.[43]

It should be noted that the existing legal system in most countries, including India, is set up with a securities regulator and regulated exchanges as the core parties. Hence, a new decentralized technology cannot by itself disrupt this legal model. At least in the near term, it seems likely that trust will continue to be placed in central parties viz. the securities regulator and stock exchanges, unless legal amendments are brought in.

iii. Derivatives

Derivatives are financial instruments that derive value from underlying assets, which could include stocks, bonds, commodities or even interest rates.[44] The White Paper which conceptualized Ethereum called financial derivatives *"the most common application of a 'smart contract'".*[45] 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."*[46] This engineering can be done using the various platforms, solutions, and frameworks discussed above, or through specialized blockchain derivatives players.

B. Telecom

India's telecom regulator, the Telecom Regulatory Authority of India's (TRAI), in July 2018 notified the Telecom Commercial Communications Customer Preference Regulation, 2018

37. Id.
38. http://www.coindesk.com/10-stock-exchanges-blockchain/;http://www.zdnet.com/article/sydney-stock-exchange-to-implement-instant-blockchain-based-settlements/; https://www.nasdaq.com/article/how-stock-exchanges-are-experimenting-with-blockchain-technology-cm801802 (last visited November 15, 2018)
39. http://www.coindesk.com/india-stock-exchange-blockchain-kyc/ (last visited April 25, 2017)
40. http://computer.financialexpress.com/news/nse-looking-at-blockchain-for-ensuring-settlement-guarantees/18956/
41. https://www.sebi.gov.in/media/press-releases/aug-2017/sebi-constitutes-committee-on-financial-and-regulatory-technologies-cfrt-_35526.html (last visited November 15, 2018)
42. https://www.jpx.co.jp/english/corporate/research-study/dlt/index.html (last visited November 15, 2018)
43. https://www.jpx.co.jp/english/corporate/research-study/working-paper/index.html (last visited November 15, 2018)
44. https://bitcoinmagazine.com/articles/blockchain-technology-will-profoundly-change-the-derivatives-industry-1464368431(last visited October 3, 2016)
45. https://github.com/ethereum/wiki/wiki/White-Paper#applications(last visited October 3, 2016)
46. https://bitcoinmagazine.com/articles/blockchain-technology-will-profoundly-change-the-derivatives-industry-1464368431(last visited October 3, 2016)

("TCCPR Regulations").[47] While blockchain cannot be always equated to Distributed Ledger Technology (DLT), 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 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.

C. Smart Contracts

While 'smart contracts' do not refer to contracts in the legal sense, legal contracts are an important application of them. As mentioned, contractual obligations like payment and delivery can be programmed to self-execute once given conditions are satisfied e.g., payment can be automatically made once a delivery event is proven (the delivery would also be automatically verified on the blockchain). This drastically reduces the resources that have to be spent on contract management i.e., ongoing monitoring and compliance with contractual obligations. Additionally, decentralization and math-based verification removes the need for trust-based execution of contractual obligations. A significant way this can be put to use is in supply chain and trade finance documentation, by automating processes "*previously spread across multiple parties and databases.*"[48] Barclays took an early lead by adopting 'Smart Contract Templates,' supported by R3. This has the capacity of automating the extensive legal documentation process involved in many banking and finance transactions. The impressive demo can be viewed at http://r3cev.com/projects/ (https://perma.cc/SKM5-EWFQ).

Similarly, startups like ChainThat offer blockchain-based solutions for use-cases such as allowing *"multi-parties to create, negotiate and manage a digital contract"* and having features including contract integrity and immutable history with time-stamping.[49]

However, some have argued that the inherent digital nature of smart contracts affects the technology's ability to enforce more subjective obligations in contracts such as ensuring 'commercially reasonable' efforts.[50]

D. Real Estate and Government Services

Real estate transactions around the world are usually time-consuming and bureaucratic. Because it is a trustless, decentralized system, the blockchain has the potential to remove the need for middlemen, disrupt existing identity verification processes (through digital IDs), reduce the risk of fraud (by creating incorruptible, digital ownership certificates for each property),[51] and track the regulatory compliance of the property. Transactions once completed would be immutably recorded in a distributed ledger (just as, for instance, Bitcoin transactions are currently done), with very little scope for doubt or manipulation.

47. https://www.trai.gov.in/notifications/press-release/trai-releases-telecom-commercial-communication-customer-preference (last visited November 15, 2018)

48. http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-aboutsmart-contracts/ (last visited October 3, 2016)

49. https://www.chainthat.com/solutions/, https://www.chainthat.com/technology/ (last visited November 15, 2018)

50. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ (last visited November 15, 2018)

51. https://techcrunch.com/2016/02/06/3-ways-that-blockchainwill-change-the-real-estate-market/; https://www.weforum.org/agenda/2016/08/how-disruptive-technology-could-solve-real-estate-s-transparency-problem/ (last visited October 3, 2016)

There is an International Blockchain Real Estate Association (IBREA) which notes that the "*[b]lockchain offers an open source, universal protocol for property buying, conveyancing, recording, escrow, crowdfunding, and more. It can reduce costs, stamp out fraud, speed up transactions, increase financial privacy, internationalize markets, and make real estate a liquid asset.*"[52] It is not surprising, therefore, that some governments are implementing or actively exploring the use of blockchain technology for their real estate record systems, including Sweden, some U.S. jurisdictions, Brazil, Georgia, Ukraine, and Ghana.[53]

'Ubitquity' offers a real estate blockchain platform that has already begun to be used for real-world property transfers.[54] 'REIDAO' offers a system for pooling and transacting in portions of real estate.[55]

But real estate is not the only government service that holds potential for the blockchain. The blockchain's features of decentralization and immutability have seen it garner interest by governments around the world for a range of services.[56] Besides the real estate initiatives already mentioned, the governments of Delaware, U.S.; Estonia; Malta; Russia; Singapore; South Korea; the U.K.; and Vermont, U.S., have been exploring the use of the blockchain for a variety of services ranging from banking and finance to healthcare.[57] The U.K. has been in particular very interested in the potential of the blockchain, both for its own services and as a catalyst for technology innovation in industry.[58] In April 2017, the Prime Minister of Malta expressed an ambition for Malta to be a leader in adopting bitcoin and blockchain technology, announcing a national strategy to promote these technologies and use them for purposes like land and healthcare registries.[59] This was eventually followed by a set of bills of 'Virtual Financial Assets'.[60]

In the context of land registration in India, land ownership records are often unclear and difficult to ascertain since many records are maintained on paper. These records and registration of land are susceptible to corruption, theft, simple loss (due to wear and tear or any natural forces), and is often manipulated by those in a position of power, particularly in rural areas. This was initially sought to be tackled somewhat by the Karnataka government in 2002, through the introduction of digitized property registration and record systems BHOOMI. However, BHOOMI has not been as successful as expected.[61] However, the low availability of digital kiosks for obtaining land record receipts, and the errant registrations which have now been solidified due to digitization of the records, have prevented digital land records from being the panacea they were envisioned to be.

Implementation of blockchain brings with it advantages of security and integrity to the land record system. These are improvements over the traditional, centralized digitalization only where the risk of tampering is high and transparency in transactions is essential. Proposed blockchain systems around the world (including certain states in India), have focused on the system's ability to eliminate corruption and enhance the integrity of property transactions.[62]

52. http://www.ibtcrea.org/ (last visited April 25, 2017)
53. https://www.weforum.org/agenda/2016/08/how-disruptive-technology-could-solve-real-estate-s-transparency-problem/; http://www.coindesk.com/blockchain-land-registry-solution-seeking-problem/ (last visitedApril 25, 2017)
54. http://www.ibtimes.co.uk/blockchain-powered-real-estate-platform-ubitquity-does-first-property-ownership-transfer-bitcoin-1569980; https://www.ubitquity.io/ (last visited October 3,2016) https://cointelegraph.com/news/us-based-startup-ubitquity-brings-blockchain-to-brazils-real-estate (last visited April 25,2017)
55. http://www.nasdaq.com/article/democratizing-real-estate-investing-with-blockchain-technology-cm768475 (last visited April 25, 2017
56. http://observer.com/2016/09/why-the-blockchain-is-perfect-for-government-services/ (last visited October 3, 2016)
57. Id.
58. https://bitcoinmagazine.com/articles/u-k-government-awardsframework-agreement-to-blockchain-as-a-service-company-credits-1470687028; www.coindesk.com/uk-blockchain-regulatory-approval (last visited October 3, 2016)
59. https://cointelegraph.com/news/suddenly-europe-is-starting-to-become-bitcoin-haven (last visited April 26, 2017)
60. https://www.mfsa.com.mt/pages/viewcontent.aspx?id=674 (last visited November 15, 2018)
61. https://www.commonfloor.com/guide/bhoomi-project-struggling-to-eliminate-land-disputes-in-karnataka-22617.html
62. https://www.cnbc.com/2017/10/10/this-indian-state-wants-to-use-blockchain-to-fight-land-ownership-fraud.html

However, most legal systems around the world place trust in the State to maintain land records. The legal system hence creates a central, trusted party and a mere technology may not be able to override this unless amendments are made (such drastic amendments would seem unlikely). However, some element of decentralization could still be used to ensure that no one party (e.g., an errant employee or department) within the government can manipulate records.

Ownership in the blockchain is determined by the possession of certain *private keys*. These private keys are not associated with the identity of their possessor and can be lost (or forcibly taken). With this in mind, there needs to be closer analysis done of the mechanism in which blockchain technology is implemented in the real estate context and the costs that accompany it. Only if the additional benefits of transparency and integrity (over and above traditional centralized online databases) exceed the costs of implementation (setting up the technological infrastructure, transferring data records to such a blockchain, ensuring sufficient nodes/verifiers exist to prevent brute-force consensus overrides, etc.), can such a system be effectively used.

E. Intellectual Property (IP), Media and Gaming

Like with real estate, the blockchain's properties make its application suitable to IP records and transactions. Works can be transferred and licensed with the accompanying terms, rights, and prices encoded on to them. Monegraph is an organization that facilitates this.[63] Its solutions help content owners and media businesses with rights management, revenue sharing, and distribution. Ampliative Art is a non-profit organization that uses blockchain technology to help artists get rewarded for their work through donations and grants.[64] The blockchain has also been used by some startups to facilitate the development of video games,[65] and the trading of digital game content.[66]

i. Media

The media value chain consists of artists, aggregators, content providers and royalty collectors. Blockchain and its disruptive, decentralized nature could very well result in a complete makeover of the existing media value chain. The deployment of blockchain could disintermediate the businesses of aggregation, provision and royalty collection. All these faculties could be aggregated into a single blockchain which would be owned and controlled by all stakeholders collectively, with transactions occurring by cryptographic consensus. The existing blockchains show that 'smart contracts' and payment verification if implemented correctly could increase efficiency of almost any task that can be automated.

Recent research has identified five use cases of blockchains that could change the way the media value chain works or potentially change the status quo.[67] The current subscription based model offers a lot of choice to the consumers but it also sometimes results in consumers not using as much as they pay for. The "per-use" payment model could be more in demand than a periodic subscription model and thus it can create a multitude of transactions which can result in rising transaction costs, in turn reducing profits.

According to Deloitte, *"[w]ith the help of a blockchain, individual articles or other pieces of content could be sold for cent prices without disproportionate transaction costs*".[68] This may enable the monetization of bite-sized content to be easier. The innate immutability trait of the blockchain along with its ability to store massive amounts of metadata could enable

63. https://monegraph.com/ (last visited November 15,2018)

64. http://www.ampliativeart.org/ (last visited November 15, 2018)

65. http://www.trustlessprivacy.com/ (last visited October 3, 2016)

66. http://ownage.io/ (last visited October 3, 2016)

67. https://www2.deloitte.com/nl/nl/pages/financial-services/articles/5-blockchain-use-cases-in-financial-services.html Last Accessed: 3/22/2018

68. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/ZA_PoV_Blockchain_Media_250817.pdf Last Accessed: 3/27/2018

copyright owners to also track how much their content is being used globally.

Furthermore, the ability of some blockchains to process micro-transactions makes it possible to have "ad-less" versions of online ad-based media services for a minor fee which would cover-up the loss in revenue that would occur by less ads playing.

The current media value chain allocates massive amounts to advertising and it remains the primary source of revenue in many models. The current model could completely shift with the implementation of blockchain, where content creators will be able to upload their media directly onto the blockchain and the users will be able to access the content through micro-payments, thus eliminating the need for aggregators and providers.

If aggregators focus their efforts on bettering the discovery of content for the user, it could result in a win-win-win for the artists, aggregators and users.

ii. Gaming

The idea of 'gaming' in a blockchain sense can be divided into two categories: first, gaming in the gambling sense with blockchain applications such as 'TrueFlip'[69] and 'Firelotto';[70]. and second, gaming in the video-gaming sense.

TrueFlip and Firelotto have tried to implement blockchain technology to the traditional lottery scenario. The manner in which it aims to improve on traditional systems is that it introduces a level of transparency that may be unprecedented in the sector. The workings of these blockchains are published on the internet and anyone can view the code of the lottery. This is to ensure that results are not manipulated. The format of the game is identical to the how lotteries work today, with incremental jackpots if nobody wins and higher prizes for more matching numbers.

Furthermore, unlike traditional lotteries which are run by individual institutions (a centralized model), this system would in essence be run by all the token holders of TrueFlip and Firelotto (a decentralized model). This is because as mentioned earlier, all decisions on blockchains are governed by the consensus protocol. The prizes are funded by an Initial Coin Offering (ICO) and then replenished via ticket sales. From the above, it is clearly seen how blockchains can revolutionize such online gaming, thus disrupting traditional models.

When it comes to video-games, the application of blockchain is slightly different from other applications. The game which started it all was known as 'Cryptokitties' – which saturated the Ethereum network with more than 15% of its capacity.[71] Other games which implement blockchain technology, 'CryptoCountries' and 'CryptoCities', allow buying and selling of virtual cities for a set amount of Ether. It is not a direct application of blockchain like TrueFlip or Firelotto but it uses the underlying principles of distributed ledger technology to record all the trades.

A more interactive application of blockchain technology in gaming can be seen in CryptoBots and Ethermons which are similar to Cryptokitties. All the data concerning the game is stored on the blockchain and the underlying transactions are recorded on the blockchain as well. Some of the use-cases for blockchain in gaming hit at the core of the value-add of blockchain i.e., decentralization and transparency.

F. Insurance

The blockchain's applications to insurance involve the streamlining of documentation, Anti-Money- Laundering / Know Your Customer (AML/KYC) processing, and claim processing.[72] This may be especially useful for wholesale

69. https://icobazaar.com static/89751ae54f10405d9a1951a4ea1c14cd/TrueFlip_Whitepaper(01.06).pdf Last Accessed: 3/27/2018

70. https://firelotto.io/whitepaper_en.pdf Last Accessed: 3/27/2018

71. https://techcrunch.com/2017/12/03/people-have-spent-over-1m-buying-virtual-cats-on-the-ethereum-blockchain/ Last Accessed: 3/22/2018

72. http://www.businessinsider.com/heres-how-blockchain-canhelp-the-wholesale-insurance-industry-2016-8?r=UK&IR=T(last visited October 3,2016)

insurance providers and consumers who may benefit from the reduced scope for fraudulent, double transactions and the ability to verify/prove accidents or other claims and reduce the scope for disputes.[73] Additionally, the use of blockchain may also enable greater interoperability of data across sectors, allowing insurance companies to potentially tap into mobile data and other public sensory devices that may be installed in a city's infrastructure. This would provide these companies with primary sources of accident and other mishap data, allowing them to act upon it with greater speed than would be possible where data is routed through multiple agencies and then sent to the insurance company. Payment service structures may undergo immense alteration with the introduction of blockchain-based smart contracts. For instance, smart contracts may be introduced, where, upon satisfaction of the system (via consensus), claims could potentially be automatically processed and benefits transferred to recipients without having to go through paperwork or other hurdles.

However, it needs to be assessed whether the decentralization aspect of blockchain is suitable for the above use-cases. In order to adopt a blockchain-based method, insurance companies would have to be comfortable with decentralization of various processes (e.g., by having every insured party as a validating node) and also with some possible efficiency losses due to the consensus processes. If there is no decentralization being implemented, the above potential use-cases would become issues of upgrading technology, but not of implementing blockchain as such.

Some consultants are of the view that smart contracts can help in insurance claim processing by automating error checking, routing and approval workflows, and calculating payout, based on the type of claim and the underlying policy.[74] Additionally, they could facilitate micro-insurance, such as pay-as-you-go automotive insurance, by processing micropayments based on usage data generated by connected devices (including Internet of Things devices).[75]

Startups like Dynamis, ChainThat, Aigang or InsurePal are "*working on blockchain-enabled P2P risk transfer protocols that aim at disrupting the core of the insurance industry's business model.*"[76]

G. Healthcare

The blockchain can be leveraged to streamline processes centered around healthcare data. It can store and control access to electronic medical records and health monitoring data generated by patients.[77] It can also link micropayments and rewards (set for patients under health plans) to this information, so that they are automatically disbursed when thresholds/milestones are met.[78]

i. Patient records

The healthcare industry, particularly the maintenance of patient records, has been plagued with the conflicting interests of patient privacy and the free interoperability of records. This is a field where the integrity and accuracy of the data stored is crucial, since errors can lead to misdiagnoses, threatening patient care. Further, issues of security also affect the full digitization of healthcare records, since an attack on the core trustee of such records can render a loss of patient privacy and lead to tampering of records. In such a field, the use of blockchain technology can be considered. It allows authorized individuals to access patient data and make use of the same, whilst ensuring security and integrity of input data. Such an approach may not only benefit patients, but also enable healthcare providers to ensure a higher quality of care, through accurate access to past patient records.

73. Id.

74. http://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html?top=4 (lastvisited October 3, 2016)

75. Id

76. https://www.willistowerswatson.com/en-IN/insights/2018/06/emphasis-blockchain-use-in-insurance-from-theory-to-reality (last visited November 16, 2018)

77. http://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html?top=4 (lastvisited October 3, 2016)

78. Id.

ii. Interoperability of data

There are multiple possible methods of value creation through the use of blockchain in healthcare. First, the security and integrity of vital health records and patient information could be ensured, with health care providers across the country having instantaneous access to a set of verified data about a given patient. Second, this data created can be securely shared (subject to patient consent) with government and insurance agencies, leading to greater transparency in ancillary industries associated with healthcare. For instance, a patient's health records could potentially be shared with a government driving licensing agency to validate his/her bodily fitness to drive, as has been implemented in Estonia. Sharing of data across borders would also become much more efficient (once and if such technology is adopted globally). Further, the democratizing effect that the blockchain has on health records is notable. Patients may have access to a fully transparent set of records that is immune to tampering. This could build trust in patients and enables them to take charge of their own health in a way that was not previously possible. This is supplemented by the existence of multiple health monitoring devices in status quo, which presents patient data in an easy to understand format so that patients can begin taking steps right from home.

iii. Outage Avoidance

The implementation of a blockchain system is not always smooth, however. What incentives do "verifiers" of data have to devote their resources to such a system? If the number of verifiers are low (due to a lack of incentive or otherwise), it becomes simple for a malicious entity to tamper with records in the system, as it could potentially manipulate a majority of the nodes to effect changes to patient data. Although this tampering would be visible, when spread across millions of patients, rectification of errors becomes immensely difficult. A healthcare blockchain would have to have checks in place for these circumstances in order to achieve any sort of added security over a simple centralized digital repository of records.

There need to be incentives for not only individual patients to act as verifiers, but also each and every healthcare provider in the country. On-boarding of patient data can be done via individual healthcare providers, with each acting as a verifier of the other provider's data.

One thing that should be noted is that a blockchain ledger of this range and depth may not have the actual data itself stored on the ledger. Rather, it may work as has been implemented in Estonia, where citizens have in their possession a unique identifier which links them to their personal medical record. *"The system files and signs the data, with new signatures generated whenever the information is altered. The data itself is not stored on the blockchain, just the hash values that indicate when files have been updated."*[79] This prevents a slowing down of the system when multiple records are being accessed, and establishes a functional yet secure system for patient data. This also has the added benefit of being going towards compliance with the EU GDPR (which provides for the right to be forgotten) or any other applicable data protection laws, since at no point is the actual data record placed on the blockchain for examination by third parties.

iv. Supply Chain Management

Outside of patient records, blockchain may be effectively utilized to track and optimize pharmaceutical supply chain management. Pharma products are often uniquely "stamped" with a registration number and verified at the point of origin. By feeding this data into a blockchain network, it could be possible to have a transparent tracking mechanism which cuts down on costs and eliminates data-based errors. The total risk in the supply chain is minimized, as each point of additional verification is simply appended to the individual pharma product's block, leading to transparent serialization.

There have been various real-world implementations of blockchain technology in healthcare. iSolve is a company that has been

79. https://www.finextra.com/blogs/fullblog.aspx?blogid=13801 (last visited March 27, 2018)

working with various pharma companies in the U.S. to implement blockchain networks to enable drug supply chain integrity.[80] The Estonian government has further signed a deal with a blockchain services company, Guardtime, to secure the health records of its citizens.[81]

Gem Health is an enterprise solution offering blockchain infrastructure for wellness apps, electronic medical records, global patient ID software, medical inventory management, and rehabilitation incentive programs.[82] In 2016, it announced a partnership with Philips.[83]

H. Asset and Wealth Management

A major segment of the financial industry that could benefit greatly from the implementation of blockchain is the wealth and asset management industry. A report by E&Y[84] discusses various applications of blockchain in the wealth and asset management which includes reduction in friction of client onboarding process, streamlined management of the model portfolios, speedy clearing and settlement of trades, and ease of compliance burden associated with AML and KYC procedures.

I. Energy

There are ventures aiming at creating an energy data exchange platform,[85] and a platform for distributed solar power.[86] Energy distribution has long been centralized through a grid system. Electricity companies, often managed by the government, maintain a monopoly over distribution infrastructure, and hence, the system of distribution as well. With the introduction of a decentralized ledger system such as blockchain, it may be possible for communities to reclaim power over electricity distribution while still making use of the infrastructure provided by electricity companies. Peer to peer trading of energy may reach new heights through the use of blockchain. By 'tokenizing' energy assets and trading them on a dedicated platform, energy can be exchanged in much smaller quantities, through self-generated energy projects, such as solar panels. For instance, ElectriCChain has created SolarCoin,[87] which is a reward-based crypto-asset for a network of affiliated solar power generators. For every MWh of electricity produced, one gets one SolarCoin, which is roughly worth USD 0.050.[88]

Such peer-to-peer based energy transactions reduce dependence on centralized grids, which may fail in the event of natural calamities or due to maintenance/servicing. This can lead to the rise of 'microgrids', with localized energy production and distribution. For instance, a block of buildings fitted with solar panels may generate more electricity than required for their consumption. With the use of a microgrid, this excess electricity can be purchased by other buildings on the grid, at prices set by the community. The use of blockchain comes in for accounting purposes, and to share information about electricity usage/purchase with the other members of the grid. This can prove especially useful when implemented in rural areas, which have little to no access to traditional power grids.

80. https://isolve.io/our-solutions/adlt/ (last visited November 16, 2018)

81. https://guardtime.com/blog/estonian-ehealth-partners-guardtime-blockchain-based-transparency (last visited November 16, 2018)

82. https://gem.co/health (last visited November 16, 2018)

83. https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gem-launches-gem-health-network-with-philips-blockchain-lab-1461674938 (last visited October 3, 2016)

84. https://webforms.ey.com/Publication/vwLUAssets/Blockchain_in_wealth_and_asset_management/$File/ey-blockchain-innovation-wealth-asset-management.pdf (last visited October 16th, 2018)

85. http://gridsingularity.com/ (last visited October 3, 2016)

86. https://idcubed.org/chapter-10-green-coins-using-digital-currency-build-new-power-platform/ (last visited October 3, 2016)

87. https://solarcoin.org/ (last visited November 16, 2018)

88. https://coinmarketcap.com/currencies/solarcoin/ (last visited November 16, 2018)

Further, energy commodities trading can possibly be made more efficient with the use of blockchain. BP and Shell, two leading energy companies, have initiated plans for a global consortium to set up a tool for energy trading via blockchain.[89] They intend to use a distributed ledger to enable greater clarity in ownership over commodities and create greater efficiency in trade through the provision of accurate information as to payments and shipping dates.

However, the problem that is faced by emerging markets such as India is that there may not exist capable infrastructure to implement a microgrid for energy distribution. Further, in welfare states such as India, where electricity is a public utility, there is not much demand for privately generated electricity, which will invariably cost more than a public grid system. Hence a decentralized system as described above may work only if this changes. Also, in order to access a microgrid on a blockchain, the internet infrastructure needs to be strong and have widespread penetration. Currently, only 20.26% of rural India has access to the Internet.

J. Other Fields

The blockchain has been called "the big breakthrough," the "Internet of Finance," the "Internet of Trust," and the "Internet of Value."[90] It is a wide-ranging innovation, so there is no end to the types of applications that it is being extrapolated to.[91] To illustrate, below are some additional fields in which it is being explored:

i. Accounting: The blockchain could save time and effort in accounting by obviating existing auditing processes. [92]

ii. Education and Employment: Some educational institutions have begun recording students' academic credentials and achievements on the blockchain, so that prospective employers can be confident that the credentials they receive are authentic.[93]

iii. Extension to the Physical Realm: Slock. it is a startup that enables machines (e.g., Internet of Things devices) to operate autonomously.[94] There are also proposals for decentralized ridesharing services,[95] and a way to automatically prove one's physical address.[96] iii. Social networks: Ventures like Project Groundhog[97] and Akasha[98] seek to use the blockchain to divest power from centralized operators of social networks. Steemit has emerged as a leading blockchain based social network. Users on Steemit are paid in the platform's cryptocurrency 'Steem' to interact with the platform like posting/sharing content etc.[99]

iv. Social impact and political participation: Our founder, Nishith M. Desai, has been predicting direct democracy facilitated by technology for a quite a while. D-CENT is a Europe-wide project that uses the blockchain to facilitate direct democracy and economic empowerment by citizens,

89. https://in.reuters.com/article/energy-blockchain/bp-shell-lead-plan-for-blockchain-based-platform-for-energy-trading-idINKBN1D612W (last visited November 16, 2018)

90. http://fortune.com/2016/05/08/why-blockchains-will-changethe-world/; http://www.forbes.com/sites/joeharpaz/2016/05/31will-blockchain-become-the-internet-of-finance/#5dcc55a12712;http://bravenewcoin.com/news/imf-report-calls-bitcoins-blockchain-the-internet-of-trust/ (last visited October 3, 2016)

91. *See* https://medium.com/the-intrepid-review/the-top-10-blockchain-startups-to-watch-in-2016-the-leaders-who-are-changingthe-game-6195606bod70#.mi8zrmpuq; https://github.com/ethereum/wiki/wiki/White-Paper#further-applications (lastvisited October 3, 2016)

92. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf (last visited October 3, 2016)

93. http://www.cnbc.com/2016/05/09/schools-are-recording-students-results-on-the-blockchain.html; http://chainthat.com/education/ (last visited October 3, 2016)

94. https://slock.it/solutions.html (last visited October 3, 2016)

95. . https://github.com/jorisbontje/moveth (last visited October 3,2016)

96. https://proofofphysicaladdress.com/ (last visited October 3,2016)

97. . https://www.youtube.com/watch?v=WFeJYv3PSaI (last visitedOctober 3, 2016)

98. http://akasha.world/ (last visited October 3, 2016)

99. https://www.wired.com/story/the-social-network-doling-out-millions-in-ephemeral-money/

so they can "*be informed and get real-time notifications about issues that matter to them; propose and draft solutions and policy collaboratively; decide and vote on solutions and collective municipal budgeting*" and be rewarded under blockchain reward schemes.[100] This application of the blockchain was also suggested in the Ethereum white paper.[101]

v. Miscellaneous: Some other proposed applications are: decentralized organizations / "future of work" (Ethereum is already a sophisticated user of these);[102] over-the-air television streaming;[103] a notary service;[104] crowdsourcing;[105] an emergency reporting system;[106] a file storage system;[107] and a domain name registry.[108]

100. http://dcentproject.eu/ (last visited October 3, 2016)

101. https://github.com/ethereum/wiki/wiki/White-Paper#applications(last visited October 3, 2016)

102. https://colony.io (last visited October 3, 2016)

103. http://dereo.io/ (last visited October 3, 2016)

104. https://github.com/maran/notareth (last visited October 3 2016)

105. http://getcrystal.net/ (last visited October 3, 2016)

106. https://github.com/mizutaka/DAERS (last visited October 3, 2016)

107. https://github.com/ethereum/wiki/wiki/White-Paper#decentralized-file-storage (last visited October 3, 2016)

108. https://github.com/ethereum/wiki/wiki/White-Paper#identity-and-reputation-systems (last visited October 3, 2016)

4. Regulatory Reaction

Since blockchain technology only creates an *infrastructure* or medium enabling a variety of applications, it is yet to stir up much regulatory controversy in and of itself. This is as opposed to, say, crypto-assets, which may disrupt traditional value-transfer systems and have governments around the world scrambling to understand their legal consequences.

As opposed to crypto-assets, most regulators' statements on blockchain technology have been positive. Led by the U.K., many countries including Australia, the U.S., Hong Kong, Malaysia, Singapore, Switzerland, Thailand, and United Arab Emirates have implemented or are exploring the idea of 'regulatory sandboxes' for blockchain (and other types of) innovation.[109] Regulatory sandboxes allow organizations to experiment with innovative business models without fear of regulatory consequences, as long as they meet certain consumer protection norms. In India, the RBI's Report of the Working Group of FinTech and Digital Banking also seems to indicate that the RBI will consider regulatory sandboxes for India.[110] The draft Payment and Settlement Systems Bill, 2018 also has the concept of a regulatory sandbox.[111]

On a separate note, as mentioned previously, the governments of Canada, China, Japan, India, Netherlands, the U.K., and Sweden have all been reported to be exploring the issuance of digital versions of fiat currency on the blockchain.[112] Such government authorization will pave the way for the adoption of blockchain technology in mainstream financial transactions.

In India, at the moment, there is no law or policy specifically addressing blockchain technology.

In April 2017, an inter-disciplinary committee was set up by the Ministry of Finance, to be chaired by the Special Secretary (Economic Affairs) and representatives from various Central government departments, including the Department of Revenue (CBDT), Ministry of Electronics and Information Technology, the RBI, NITI Aayog, and State Bank of India, to examine the regulation of virtual currencies.[113] However, there may be a dichotomy in the government's approach to virtual currencies (which the government appears concerned about in light of the consumer protection risks) and blockchain technology as such (on which the government has expressed no negative view).

The Committee on Digital Payments, chaired by Mr. Ratan P. Watal, and constituted by the Ministry of Finance, in its December 2016 report cited an earlier version of this paper and noted the benefits of blockchain technology.[114] In addition, as mentioned previously, the IDRBT has recommended that the "time is ripe" for the adoption of blockchain technology in India. The Government of Andhra Pradesh in October 2016 signed a FinTech Cooperation Agreement with the Monetary Authority of Singapore to "*promote innovation in financial services in their respective markets[,]explore joint innovation projects on technologies such as digital payments and blockchain[,]collaborate on the development of education programmes/curricula on FinTech[, and] discuss emerging FinTech trends and exchange views on regulatory issues related to innovations in financial services.*"[115]

In addition, some regulatory officials have made press comments about blockchain technology, which have varied in tone.

109. https://www.americanexpress.com/uk/content/foreign-exchange/articles/regulatory-sandboxes-for-innovative-payment-solutions/ (last visited April 25, 2017)

110. https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=892 (last visited November 16, 2018)

111. https://dea.gov.in/sites/default/files/Payment%20and%20settlement.pdf (last visited November 16, 2018)

112. E.g., https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=43574 (last visited November 16, 2018)

113. http://pib.nic.in/newsite/PrintRelease.aspx?relid=160923 (last visited April 25, 2017)

114. http://finmin.nic.in/reports/watal_report271216.pdf (last visited April 25, 2017)

115. http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/Singapore-and-the-Government-of-Andhra-Pradesh-ink-FinTech-cooperation-agreement.aspx (last visited April 25, 2017)

In 2016, former Deputy Governor H. R. Khan had told reporters, "*Blockchain is one thing that has come out of Bitcoin which provides a lot of flexibility in terms of financial transactions. So, we need to study... how this blockchain technology can be used in financial transactions where the entire data systems move to some more levels.*"[116]

The then RBI Deputy Governor R.S. Gandhi in March 2017 said, "*Blockchain, the foundation for bitcoins-like innovations, is touted to be the death knell of currency. I believe its potential is being overstated. We can see that in these types of solutions for virtual currency, there is no central bank or monetary authority. They pose potential financial, operational, legal, customer protection and security related risks.*"[117] However, he added he was glad about the IDRBT's blockchain research project, and said, "*There is a movement to make use of blockchain technology for virtual currency by the central banks themselves. Of course, this calls for lot of research.*"[118]

As mentioned above, the RBI had recently come out with its Report of the Working Group of FinTech and Digital Banking. The Report has identified Blockchain as one of the 'Three Pillars' which will drive digital transformation and innovation in the Banking, Financial Services and Insurance (BFSI) sector, including Artificial Intelligence and Internet of Things. [119]

In the February 2018 Budget Speech, the Finance Minister stated,

> "*Distributed ledger system or the block chain technology allows organization of any chain of records or transactions without the need of intermediaries. The Government does not consider crypto-currencies legal tender or coin and will take all measures to eliminate use of these crypto-assets in financing illegitimate activities or as part of the payment system. The Government will explore use of block chain technology proactively for ushering in digital economy.*"[120]

However, in April 2018, the RBI issued a circular which dealt a body blow to the crypto-asset and blockchain ecosystem in India.[121] This circular prohibited entities regulated by the Reserve Bank such as banks and financial institutions from dealing with 'Virtual Currencies' (VCs) or providing services for facilitating any person or entity from dealing or settling 'VCs'. The services which were deemed to facilitate the 'dealing or settling of VCs' included maintaining accounts, registering, trading, settling, clearing, giving loans against virtual tokens, accepting them as collateral, opening accounts of exchanges dealing with them and transfer/ receipt of money in accounts relating to purchase/ sale of 'VCs'. The circular is currently being challenged in the Supreme Court of India on its constitutional validity (*Disclosure:* Nishith Desai Associates acts for the Internet and Mobile Association of India in its petition against the said RBI circular).

While it appears that the intention of the RBI was to cut off the traders of crypto-assets and various crypto-asset exchanges from the financial system, it has had side effects on the blockchain ecosystem. For instance, in the absence of any clear definition of the term 'Virtual Currency' from the RBI, the circular could impact any blockchain-based platform which is dependent on tokenization of some sort. The operators of a blockchain platform which uses tokens either for incentivization or to maintain stability of the network may potentially be cut off from the financial system as Indian banks and financial institution may not be allowed to support them.

Since there is little legal authority on how blockchain technology will be treated, there is uncertainty in industry on this question. The thinking is that though the blockchain itself has not caused a regulatory stir, this does not guarantee that particular *applications* will not.

116. http://m.moneycontrol.com/news/economy/rbi-to-study-blockchain-technology-to-curtail-paper-currency_6927981.html (lastvisited October 3, 2016)

117. http://www.coindesk.com/indian-central-banker-potential-blockchain-currencies-overstated/ (last visited April 25, 2017)

118. *Id.*

119. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF (last visited November 15, 2018)

120. https://www.indiabudget.gov.in/ub2018-19/bs/bs.pdf (last visited November 15, 2018)

121. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=11243 (last visited October 26, 2018)

On this note, the President of the Chamber of Digital Commerce, the world's largest trade association representing the blockchain industry, and the World Federation of Exchanges, the global trade body for exchanges, have called for regulatory clarity over the use of blockchain technology for different purposes.[122] In October 2016, the Digital Currency and Ledger Defense Coalition (DCLDC), a coalition of prominent U.S. lawyers and academics, was announced.[123] The DCLDC seeks to protect the right of innovators experimenting with blockchain technology, through pro bono attorney referrals and the filing of amicus briefs. Where regulatory sandboxes are not forthcoming, therefore, staying involved with industry bodies can be a powerful fallback for blockchain innovators.

I. Global Developments

A. U.K. Government Authorization of Blockchain E-Money Startup

In February 2017, the U.K. government granted the blockchain-based finance startup Tramonex a small Electronic Money Institution (EMI) registration.[124] The EMI registration is for persons who "issue e-money", and "e-money" includes *"monetary value represented by a claim on the issuer that is stored electronically, including magnetically"*.[125] Tramonex's website does not provide any description of how blockchain technology is involved in its offerings, but its website suggests that the solutions are related to traditional fiat currencies and not cryptocurrencies.[126] Tramonex offers to provide a *"single centralised payment hub [that] can reduce the cost of your banking infrastructure and increase efficiencies"* with the following solutions: working capital management, FX risk management, and operational management.[127]

B. French Government Regulations

In December 2017, France became one of the first countries in the world, and possibly the first country in Europe, to *"regulate the recording and transfer of securities on a shared electronic recording device, such as blockchain"*.[128] In April 2016, the French government passed an order legislating rules surrounding 'mini-bonds,' a type of corporate debt instrument facilitating crowdfunding.[129] The order explicitly permitted the issuance and transfer of mini-bonds using the blockchain, given certain adapted procedures and safeguards. The order stated that the registration of the sale transaction in the blockchain will operate as the transfer of title ownership. A working group was to determine detailed safeguards to ensure reliability, security, and the capacity to be audited. The order also contained the first known regulatory definition of the blockchain: a "shared electronic storage device" or *"a shared electronic recording system allowing for authentication."* As a result of this move, BNP Paribas announced in September 2016 that it would expand its blockchain platform to allow private companies to issue minibonds via crowdfunding platforms.[130]

122. https://www.forbes.com/sites/perianneboring/2016/06/28/the-blockchain-brain-drain-how-the-states-are-driving-blockchain-companies-abroad/#29b047e783fc (last visited April 25, 2017); http://www.reuters.com/article/us-exchange-regulations-blockchain-idUSKCN11017Q (last visited October 3, 2016)

123. http://www.the-blockchain.com/2016/10/03/40-us-law-firms-joinup-to-form-blockchain-legal-defense-coalition/ (last visited October3, 2016)

124. https://cointelegraph.com/news/uk-government-grants-permission-to-issue-blockchain-based-currency (last visited April 26, 2017)

125. https://www.fca.org.uk/publication/archive/emoney-approach.pdf (last visited April 26, 2017)

126. https://tramonex.com/#/home (last visited April 26, 2017)

127. *Id*

128. https://www.lexology.com/library/detail.aspx?g=abbf3f48-0933-497c-8a11-580a79341266 (last visited November 16, 2018)

129. https://translate.google.com/translate?hl=en&sl=fr&u=https://www.legifrance.gouv.fr/eli/rapport/2016/4/29/FCPT1608300P/jo&prev=-search (translated report explaining the order); https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032465520&-categorieLien=id (original text of order).

130. https://group.bnpparibas/en/press-release/bnp-paribas-securities-services-expands-blockchain-platform-private-stocks (lastvisited October 3, 2016)

C. Malta Regulatory Framework

Earlier this year, Malta passed three new laws namely, The Malta Innovation Authority Act, The Innovative Technology Arrangements and Services and The Virtual Financial Assets Act for regulating the cryptocurrency and blockchain ecosystem.[131]

The Malta Digital Innovation Authority Act (the 'MDIA'): It 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 innovative technology arrangements and related services, especially Distributed Ledger Technologies and smart contracts. It is important to note that 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 Innovative Technology Arrangements and Services Act (the 'ITAS Act'): It 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 ITAS Act relate only to DLTs and smart contracts. However, the MDIA has the power under the ITAS to notify additional Innovative Technology Arrangements.

The Virtual Financial Assets Act (the 'VFAA'): It provides a framework for issuance of DLT assets through ICOs and crypto exchanges and their operation. It also lays down specific requirements for the drafting of a whitepaper for an ICO. Malta has evidently decided to remove the word 'cryptocurrency' and replace it with 'Virtual Financial Asset' (**"VFA"**). Wherein, 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, to name a few. Malta, with the passing of these legislations is attempting to become a safe place for the blockchain industry to grow, and enables the government to implement safeguards to ensure consumer protection, market integrity and financial stability.

D. Thailand's Law on Digital Asset Business

On May 13, 2018, the Thailand Ministry of Finance and The Securities and Exchange Commission, Thailand (**"SEC Thailand"**) published two Decrees in the Royal Gazette to enact specific regulations relating to:

1. Operations of digital asset business (Royal Decree on the Digital Asset Businesses B.E. 2561)[132]
2. Tax implications on income earned from digital assets (Royal Decree of the Amendment to the Revenue Code).[133]

The Royal Decree came into effect on 14 May 2018 and in the words of the Secretary General of the SEC Thailand, *"aims regulate and supervise offering of digital tokens and undertaking of digital*

131. https://www.financemalta.org/publications/articles-interviews/articles-and-interviews-detail/second-reading-in-parliament-for-blockchain-bills-the-innovative-technology-arrangements-and-services-act/, https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF (last visited November 16, 2018)

132. https://www.sec.or.th/TH/SECInfo/LawsRegulation/Documents/Act_Royal_Enactment/enactment_digital_2561_summary_en.pdf

133. *Ibid*

asset businesses, including exchange, brokerage and dealing."[134] The legislation has also brought digital assets within the purview of the Thai Anti Money Laundering Act and also aims to protect investors from risks of fraud and deception by imposing requirements which consist of inter alia registering a prospectus, continuous disclosure requirements, measures against insider trading, false dissemination of information, front running etc. Issuance of 'Digital Tokens' to the public can only take place after approval from the SEC Thailand, which requires the filing of a draft prospectus and a registration statement.

The new law also recognizes three distinct businesses within the Digital Asset space. These are 'Digital Asset Exchange'[135], 'Digital Asset Broker'[136] and Digital Asset Dealer.[137] The recognition of brokers and dealers may be somewhat unique, and is seems to be an attempt to bring Digital Assets within the realm of conventional financial instruments such as securities. Another interesting aspect is that the new law requires that: "*issuers of Digital Tokens who are willing to accept Cryptocurrencies in the offering process or the operators of digital asset businesses who are willing to accept Cryptocurrencies from the counterparties in any transaction shall only accept Cryptocurrencies obtained from or deposited with operators of digital asset businesses regulated under the Royal Decree*". This seems to indicate that in order to pay for any issue of Digital Tokens in Thailand with cryptocurrency, the cryptocurrency will have to be purchased from registered digital asset entities. It is however unclear at this moment as to how Thai regulators will enforce such a requirement as major cryptocurrencies like Bitcoin are often traded on a peer-to-peer basis. However, blockchain analysis tools like Elliptic could be one such option.

The Amendment to the Thai Revenue Code has also brought Digital Assets within the tax net, thus recognizing Digital Assets and related businesses.

134. https://www.sec.or.th/en/Pages/News/Detail_News.aspx?tg=NEWS&lg=en&news_no=50&news_yy=2018

135. Under the Royal Decree, "Digital Asset Exchange" means a center or a network established for the purposes of purchasing, selling or exchanging of digital assets, operates by matching or arranging the counterparty or providing the system or facilitating a person who is willing to purchase, sell or exchange of digital assets to be able to enter into an agreement or match the order, in the normal course of business, excluding the system or network in the manner as specified in the notification of the SEC

136. Under the Royal Decree, "Digital Asset Broker" means a person who services or holds himself out to the public as available to be a broker or an agent for any person in the purchase, sale or exchange of digital assets to other person in the normal course of business, in consideration of a commission, fee or other remuneration, excluding the brokers or agents in the manner as specified in the notification of the SEC.

137. Under the Royal Decree, "Digital Asset Dealer" means a person who services or holds himself out to the public as available to purchase, sale or exchange of digital assets for his own account in the normal course of business outside the digital asset exchange, excluding the dealer in the manner as specified in the notification of the SEC.

5. Forecasting Legal Issues

Despite the lack of legal authority on blockchain technology to date, there are several interesting legal questions which it raises and should be considered. In general, however, analyzing the legal implications of the blockchain outside of a particular use case is less straightforward than the same analysis of Bitcoin. This is because Bitcoin is only one specific use case of blockchain technology, whereas blockchain technology can be applied in almost any context.

I. Pseudonymity and Legal Enforcement

A lot of people still associate Bitcoin with nefarious activities on the 'dark web,' like illegal purchases of banned substances and guns, and financing terrorism.[138] This is because network participants could be anonymous or pseudonymous i.e., not fully anonymous – because of various identifying information like network (IP) addresses and public keys – but not obviously linked to a real identity.[139] In this aspect, the blockchain operates with the same properties as Bitcoin. Therefore the question arises about how regulators and counterparties will hold participants accountable, and enforce legal, tax, and contractual obligations.[140] Albeit a tangential example, the enormous amount of resources it took for the U.S. Federal Bureau of Investigation (FBI) to trace the mastermind behind 'Silk Road' (the infamous 'dark web' exchange) bears testimony to this.[141] Further, when the blockchain is deployed in regulated industries, KYC requirements and various reporting obligations like anti-money-laundering and anti-terrorist-financing (depending on the jurisdiction) are triggered. These will be hard to meet when transactions are on blockchains, at least in the form that blockchains are commonly used today.[142] The likely solution to this is the requirement that participants must shed their anonymity/pseudonymity on the blockchain for commercial transactions. This is something that lawmakers could address. The Indian Information Technology Act, 2000 ("**IT Act**") could, for instance, be amended to this effect. There are already technical solutions that facilitate this.[143] In addition, 'private' or 'permissioned' blockchains, which, as opposed to 'public' or 'permissionless' blockchains (like Bitcoin), regulate who can access the blockchain network and how they can participate in it. This is usually an important feature of the various enterprise blockchain solutions on the market. The Chain Protocol, the blockchain protocol targeted at financial institutions and discussed previously, is an example of a permissioned blockchain.[144]

II. Privacy and Cybersecurity

A. Privacy

The counterpoint to the pseudonymity-based legal issues is that because blockchain participants cannot be fully anonymous and the distributed ledger is publicly viewable, there are privacy implications.[145] As mentioned, blockchain participants can be identified using their public keys and IP addresses, among

138. *E.g.*, http://www.coindesk.com/google-search-study-hints-shady-truth-bitcoin-users/ (last visited October 3, 2016)

139.. http://gizmodo.com/a-friendly-reminder-bitcoin-is-not-anonymous-1682885318 (last visited October 3, 2016)

140. http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f; http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited October 3, 2016)

141. http://www.usatoday.com/story/news/nation/2013/10/21/fbicracks-silk-road/2984921/ (last visited October 3, 2016)

142. http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f (last visited October 3, 2016)

143. *E.g.*, http://www.blockchainme.com/index.html (last visited October3, 2016)

144. https://news.bitcoin.com/chain-open-standard-1-goes-public/ (lastvisited October 3, 2016)

145. http://www.lexology.com/library/detail.aspx?g=ee10aaof-3447-4088-81dd-7521244fecb3; http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited October 3, 2016)Provided upon request only

other identifiers, and every transaction can be seen by every participant (this is an essential feature of blockchain technology). Since the 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.[146] 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.[147] 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. Enterprise deployments of commercial blockchain technology might therefore look to address these privacy concerns,[148] incorporating privacy by design. While doing so, however, they should also look to preserve accountability, for reasons discussed in the previous section. Lawmakers could look at mandating that blockchain operators (in situations where there are centralized operators) incorporate such a dual-edged feature, if technically feasible.

India is currently on the cusp of a sea change in regulating the manner in which personal data is processed. The Committee of Experts under the Chairmanship of Justice Srikrishna released the draft Personal Data Protection Bill, 2018[149] . Under this Bill, a duty has been cast on all 'data fiduciaries', or parties who determine the purpose of processing personal data to protect the individuals' (data principals) 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 the consent of the data principal. It is pertinent to note that the Bill only governs the use of 'personal data', or data which is identifiable to an individual. A close analysis of the Bill and the unique nature of the blockchain may result in the position that blockchain is likely going to be incompatible with some provisions of the Bill, if personal data is stored on the blockchain. Some of these provisions have been explained below.

- 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.
- In some instances, where the data being processed is classified as 'critical personal data', then the Bill requires the processing of the data to happen only within India. However, the blockchain by itself is global and de-centralized. It lives on the internet. Designing a blockchain system in compliance with this requirement and to ensure that the 'nodes' of the blockchain are Indian IP addresses could lead to loss of efficiency and transparency.
- The Bill mandates that the personal data of a data subject be made 'portable' or transferable from one service to another. It is unclear however, how this can be implemented in a blockchain.
- The Bill grants the data subject the right to modify and correct their personal data. However, the immutable nature of the blockchain may make this difficult.

146. http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3 (last visited October 3, 2016)

147. Section 43A, IT Act, read with the Information Technology (Reasonablesecurity practices and procedures and sensitive personal data orinformation) Rules, 2011. (last visited October 3, 2016)

148. http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited October 3, 2016)

149. http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last visited October 30, 2018)

B. Cybersecurity

If high value transactions and records are going to be moved to the blockchain – which seems likely, as the earlier discussion of industry applications showed – cybersecurity becomes essential.[150] Data breaches are being announced every day, and several hacks, including the recent CoinCheck hack of over USD 500 million worth of cryptoassets,[151] show that the implementation of blockchain technology is not infallible (even though the underlying technology is widely acknowledged to be robust and secure). For instance, participants' private keys (stored on their devices and/or on the cloud) can unlock their entire holdings, making private keys a definite target,[152] and often a 'single point of failure.'[153] This risk has already materialized several times with Bitcoin. Existing laws, including the requirements under the IT Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, will govern blockchain activity since the blockchain is an Internet-based system. But these requirements do not easily fit with the nature of the blockchain. As mentioned above, with the blockchain, there is usually no controlling "body corporate" to pin accountability for cybersecurity to. Where there are blockchain operators, they will be held to the cybersecurity requirements of the Rules. But because the system is decentralized, and because there are not always any centralized 'operators' (as with Bitcoin), this is not enough to ensure cybersecurity. Further, existing standards on data protection, such as the IS/ISO/IEC 27001 standard that the Rules mention, may not suffice for the blockchain, because they were not designed keeping in mind its decentralized nature. As we speak, however, new cybersecurity standards tailored to the blockchain are being conceived, [154] and such standards will have to be referenced into existing law. .

III. Complications Associated with Decentralized Autonomous Organizations (DAOs)

"*A DAO is a virtual autonomous organization, in which the functions of the organization exist in software, and the laws governing the organization's functions are set into smart contracts that become automatically enforceable if a set of defined conditions are met. As a result, the DAO becomes a company that runs by itself, without a centralized governing body.*"[155]

The most well-known example of a DAO was 'The DAO' (mentioned earlier), an organization functioning on the Ethereum blockchain, and which had collected a pool of cryptocurrency worth several million U.S. dollars as crowdfunding for venture capital investment purposes. [156] Being of such a decentralized, pseudonymous nature, DAOs do not fit within existing definitions of legal entities like companies and partnerships. [157] This is because stakeholders in DAOs may not necessarily agree with the distribution of decision-making power, and the responsibilities of directors, shareholders, partners, and employees, dictated by these traditional structures. In a DAO, as the name suggests, authority is thoroughly decentralized, with decision-making often

150. http://www.lexology.com/library/detail.aspx?g=ee10aaof-3447-4088-81dd-7521244fecb3 (last visited October 3, 2016)

151. https://www.forbes.com/sites/forbestechcouncil/2018/09/17/why-are-crypto-exchanges-are-hacked-so-often/ (last visited November 16, 2018)

152. Id.

153. See e.g., this explanation by Vitalik Buterin, a co-founder of Ethereum:https://www.youtube.com/watch?v=UFDAtStVXbc. (last visitedOctober 3, 2016)

154. https://www.w3.org/2016/04/blockchain-workshop/report.html(last visited October 3, 2016)

155. https://www.tractica.com/automation-robotics/blockchain-daosand-the-future-of-government/ (last visited October 3, 2016)

156. http://fortune.com/2016/05/15/leaderless-blockchain-vc-fund/ (lastvisited October 3, 2016)

157. http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF; but see http://bollier.org/sites/default/files/misc-file-upload/files/DistributedNetworksandtheLaw%20report,%20Swarm-Coin%20Center-Berkman.pdfsuggesting possible legal organizational structures within whichDAOs could fall. (last visited October 3, 2016)

driven purely by consensus.[158] Further, they are not 'located' within any particular jurisdiction (they are considered 'stateless'),[159] so the applicable law is itself a question.[160] The nature of their members' 'interest' in is also unclear (as opposed to a company share or partnership stake).[161] These make it hard to answer how a DAO's or its members' legal rights and duties would be considered. It is not easy to simply create an artificial regulatory definition for a DAO, because they are governed and operated by software code, and the organizational rules can be written in a limitless number of ways. Another question worth considering is to what extent the programmers of the code underlying the DAO be accountable for its actions and for security breaches of its architecture.[162] These theoretical difficulties become clearer to visualize when one thinks of the multimillion dollar hack of the Ethereum DAO, discussed previously.[163] The applicable law, the legal recourse for the DAO's investors, the development of a suitable insurance regime for such situations, the liability of the DAO's programmers, and the regulation of DAOs as investment vehicles make for difficult questions in such a situation.[164] This is in addition to the difficulty of pinning down responsibility due to anonymity/ pseudonymity and decentralization. At the time of writing, [165] the persons responsible for the hack of the Ethereum DAO were still unknown. No member or software developer within that DAO could be faulted either, because the code was open-source, hence making everyone (and no one) responsible for its robustness. The legal concept of an 'association of persons' may be a useful starting point for the legal analysis of DAOs. Under Indian law, an association of persons is a body of individuals or legal entities which associate themselves to further a common purpose.[166] Other than interpretation of the broad concept by courts, there are no legal strictures – as there are for companies and partnerships – surrounding this concept. This provides DAOs with a significant degree of legal flexibility to be governed as their members decide. At the same time, laws such as the Income Tax Act, 1961 and the Competition Act, 2002, recognize the concept of an 'association of persons,' hence preventing DAOs from 'slipping under the radar' and being considered nefarious.

In July 2017, the U.S. Securities and Exchange Commission (SEC) issued an investigative report concluding that the Ethereum DAO tokens were 'securities'.[167]

IV. Complications Due to Immutability and Irreversability

Blockchains cannot be 'edited' like conventional ledgers. Once transactions are recorded, they remain in the universal ledger unless every participant agrees otherwise.[168] In one sense, the only editors are cryptography and the 'wisdom of the crowd'. This has led some to point out that immutability is "*[t]he most obvious risk inherent in blockchain technology.*"[169] This is because while immutability preserves the integrity of transactions, it may become problematic when untrustworthy users have managed to conceal

158. https://medium.com/@BlockChannel/what-is-a-dao-how-do-theybenefit-consumers-f7a0a862f3dc#.g8brl9tgq (last visited October 3,2016)

159. http://www.economist.com/news/finance-and-economics/21699159-new-automated-investment-fund-has-attracted-stacks-digital-money-dao (last visited October 3, 2016)

160. http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brothem

161. *Id.*

162. http://www.clydeco.com/insight/article/ethereums-dao-attacksmart-contracts-and-blockchain-face-their-first-big-te (last visitedOctober 3, 2016)

163. http://fortune.com/2016/06/18/blockchain-vc-fund-hacked/ (lastvisited October 3, 2016)

164. http://www.clydeco.com/insight/article/ethereums-dao-attacksmart-contracts-and-blockchain-face-their-first-big-te (last visitedOctober 3, 2016)

165. October, 2016.

166. http://www.financialexpress.com/archive/legal-concept-of-association-of-persons/372324/ ; C.I.T. v. Indira Balkrishna, 39 ITR 546. (lastvisited October 3, 2016)

167. https://www.sec.gov/news/press-release/2017-131 (last visited November 16, 2018)

168. http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited October 3, 2016)

169. *Id.*

fraud.[170] In an ordinary situation, the defrauded parties could approach courts, regulatory bodies (in India, one could approach the RBI under the Banking Ombudsman Scheme), or third party gatekeepers (like banks) to either (a) reverse the fraud, or (b) receive compensation.[171] In blockchain transactions, however, (a) fraudulent transactions cannot be reversed by any central party, and (b) it is difficult for courts to trace the wrongdoer, and even if they do, to enforce a judgment, for reasons discussed under sub-section I. above (**"Pseudonymity and Legal Enforcement"**).[172] It is likely that enterprise deployments of blockchain technology will, through private/permissioned systems, look to tackle these problems. Otherwise, banks and payment system operators using the blockchain may find themselves (in some cases) in violation of the detailed regulatory requirements governing them – such as, in India, those under the Banking Regulation Act, 1949, and the Payment and Settlement Systems Act, 2007. So that innovation is not unnecessarily impeded, regulators may consider mandating a workaround that does not compromise the decentralization and permanence that is unique to the blockchain, but holds some possibility for 'corrections' to the ledger if certain conditions are met.

V. Jurisdictional Questions

The Internet itself has raised several questions on how to decide when a given jurisdiction's law would govern a given situation. For example, Indian courts will look at whether a website was made available in the country "*with an intention to conclude a commercial transaction*" with Indian users.[173] In the case of an ultra-decentralized technology like the blockchain, the difficulty of these questions is amplified.[174] This is because there are no identifiable 'hosts' or 'operators' as there are for ordinary websites and apps (even if there is an identifiable blockchain operator, its role would likely be very different from a website/app operator's). This makes identifying legal responsibility difficult, as discussed above. In addition, servers for each blockchain network are decentralized and likely spread throughout the world, making it difficult to pinpoint where a breach or failure occurred.[175] In the case of the Internet generally, several jurisdictions have mandated some form of data localization or border controls, where servers are required to be kept in that jurisdiction (e.g., Russia) or there are restrictions on how data can flow out of the jurisdiction (e.g., the EU and India). For the blockchain, lawmakers will have to consider how their jurisdictions' technology laws apply. A multi-stakeholder, global approach appears to be best, to ensure the harmony of international rules. In this vein, associations like the Chamber of Digital Commerce and the Digital Currency and Ledger Defense Coalition have garnered wide participation and are likely to play an important role.

VI. Contract Law Grey Areas

As discussed previously, a key feature of the blockchain is the "*formation and execution of digital contracts.*"[176] In other words, instead of ordinary human language, software code dictates parties' rights and responsibilities, and automatically executes when specified conditions are met. This could be for the entirety of the contract or only in certain provisions. Contract law around the world is based on human decisions and judgment (e.g., the treatment of offer and acceptance, meeting of the minds, and consideration).[177] Therefore, automatic execution and machine language create new legal questions:

170. *Id*

171. *Id.*

172. *Id.*

173. Banyan Tree Holding Pvt. Ltd. v. A. Murali Krishna Reddy & Anr., 2008(38) PTC 288 (Del) (last visited October 3, 2016)

174. http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF (last visited October 3, 2016)

175. *Id.*

176. http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f (last visited October 3, 2016)

177. http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF (last visited October 3, 2016)

- Are these digital contracts "contracts" as seen by the law?
- Can they be enforced and parties be held responsible in the same way as traditional contracts?
- What if the code underlying these digital contracts is hacked?

Commentators have given the example of parties not being able to plead duress or mistake of fact in a real estate transaction because all changes in ownership and the status of the property would have already been verified and recorded in a universally accessible blockchain.[178] They have also noted that the 'volition' element in law, where parties' choice of action gains importance, may not suit blockchain transactions, since actions – such as the filing of a lawsuit upon default – automatically execute.[179] (One could argue, however, that volition occurred at the time the digital contract was drafted.) Also, due to immutability and irreversibility, as mentioned above, remedies for smart contracts 'gone wrong' (e.g., mistaken rainfall data in the context of a drought insurance contract)[180] may be difficult to pursue, since traditional contract law options like rescission will not be viable.[181] Because of immutability and irreversibility, arguments for unenforceability that fall outside those situations contemplated by the written code (e.g., fraud, force majeure, and frustration) may become harder to resolve than usual.[182]

To help resolve such contractual ambiguities, some have suggested that there should be natural language contracts signed, complementing the digital contracts (e.g., a Master Supply Agreement that governs all the smart contract purchase orders), that enable the parties to resolve such situations under traditional contract law mechanisms.[183]

Whether through this way or another, the practical solution appears to be to retain a natural language contractual element at least until the legal system, parties, and lawyers are familiar with smart contracts. It is also essential that, because of the murky legal issues discussed in this section, blockchain contracts have detailed dispute resolution clauses in which the parties legislate for various outcomes specifically taking into account the technology,[184] hence avoiding confusion later. Digital/smart contracts raise the question of the role of lawyers in transactional practice going forward. This is of course even more relevant in the light of the rapid strides in artificial intelligence. The reasonable view is that lawyers will still be required to draft non-obvious contractual terms or terms that cannot fit into technical language; interact with programmers on the correspondence between the natural language and software code;[185] and counsel parties on legal risks.

Many have pointed out that a working understanding of software programming will be very useful for the next generation of lawyers.[186] While regulation should not be imposed hastily, it is likely that as smart contracts come into use, new contract law rules are necessary to govern code-based and blockchain-driven contracts.[187]

178. http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f; http://www.lexology.com/library/detail.aspx?g=ee10aaof-3447-4088-81dd-7521244fecb3 (last visited October3, 2016)

179. http://www.lexology.com/library/detail.aspx?g=ee10aaof-3447-4088-81dd-7521244fecb3 (last visited October 3, 2016)

180. http://www.clydeco.com/insight/article/arbitrating-blockchain-disputes-will-smart-contracts-require-smart-dispute (last visitedOctober 3, 2016)

181.. http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited October 3, 2016)

182. http://www.clydeco.com/insight/article/smart-contracts-where-lawmeets-technology (last visited October 3, 2016)

183. Id.

184. http://www.clydeco.com/insight/article/arbitrating-blockchain-disputes-will-smart-contracts-require-smart-dispute (last visitedOctober 3, 2016

185. http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited October 3, 2016)

186. Richard Susskind, Tomorrow's Lawyers: An Introduction to YourFuture (Oxford University Press, 2013); http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf; http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bfb-8e13-1826e9d2733f (last visited October 3, 2016)

187. http://www.clydeco.com/insight/article/smart-contracts-where-lawmeets-technology (last visited October 3, 2016)

VII. Whether Blockchain Tokens are 'Securities'

Transactions occur on the blockchain through the exchange of tokens. In the case of the Bitcoin blockchain, the tokens stand for Bitcoin value, but tokens can be configured to represent anything that can be transacted (e.g., real estate or company shares.) As we discussed in Section 3(III) (**"Applications"**), securities and derivatives are a major potential application of blockchain technology. The question of how blockchain tokens fall within existing definitions of 'securities' and 'derivatives' therefore becomes relevant. In our 2015 paper on Bitcoins,[188] we have concluded that Bitcoins could not be classified either as 'securities' or 'derivatives' under the Securities Contracts (Regulation) Act, 1956 (**"SCRA"**). This is because Bitcoins do not have an underlying asset, and are not "issued" by any particular entity. When analyzing blockchain tokens in general, the analysis is more context-specific. This is because while Bitcoins only represent virtual value, nearly anything can be represented on the blockchain.

A publication by the Coinbase, Coin Center, Union Square Ventures, and Consensys, in partnership with the U.S. law firm Debevoise & Plimpton, aimed to establish a securities law framework for blockchain tokens under U.S. law.[189] It established a mechanism for entities to "estimate how likely a particular token is to be a security" under U.S law. This mechanism is a step-by-step process leading to a score, which is meant to act as a risk assessment. The publication also sets out best practices for 'crowdsales' of tokens. Finally, it contains an analysis by Debevoise & Plimpton which concludes, "*an appropriately designed Blockchain Token that consists of rights and does not include any investment interests should not be deemed to be a security, subject to the specific facts, circumstances and characteristics of the Blockchain Token itself. Rather, given our analysis in the above, it should be characterized as a simple contract, akin to a franchise or license agreement.*" An earlier publication by several well-known thinkers on blockchain technology (some of whom also participated in the previously mentioned publication) also undertook a detailed analysis of how blockchain tokens would fall within the 'securities' definition under U.S. law.[190]

Its conclusion was that the answer would change depending on what the token represented. Analyzing different hypothetical tokens, the working paper concluded that tokens representing: access to a software product which may appreciate in value; voting rights with a financial concern; and ownership of digital assets without an expectation of profit, may generally be considered securities. Tokens representing non-transferable software access rights; voting rights without a financial concern; digital goods without an expectation of profit; and 'shares' in DAOs were not likely to be considered securities.

As mentioned above, in July 2017, the U.S. Securities and Exchange Commission (SEC) issued an investigative report concluding that the Ethereum DAO tokens were 'securities'.[191]

In the Indian context, the analysis will have to be made primarily with regard to the 'underlying asset' and 'issuance' requirements.

VIII. Adaptations of Older Requirements

Existing law has a swathe of procedural requirements governing commercial transactions and political processes, including (in India):

- The requirement of physical signatures, notarization, stamping, and registration for specified classes of documents (e.g., real

188. Latest draft available at http://www.nishithdesai.com/information/research-and-articles/research-papers.html. (last visited October 3,2016)

189. https://blog.coinbase.com/2016-12-07-blockchain-token-securities-law-a66ef03c383f; see also https://www.debevoise.com/~/media/files/insights/publications/2017/10/20171017a%20bright%20lines%20dont%20work%20for%20blockchain%20tokens.pdf (last visited November 26, 2018)

190. http://bollier.org/sites/default/files/misc-file-upload/files/DistributedNetworksandtheLaw%20report%2C%20Swarm-Coin%20Center-Berkman.pdf (last visited April 26, 2017)

191. https://www.sec.gov/news/press-release/2017-131 (last visited November 16, 2018)

property conveyances) under various laws;

- Formalities for assignment under intellectual property laws;
- The IT Act's stipulations on electronic signatures;
- The process for voting under the Representation of the People Act, 1951, and the Companies Act, 2013;
- Share issuance and transfer procedures under the Companies Act, 2013, and the Foreign ExchangeManagement Act, 1999;
- Maintenance of records and registers under various laws including the Companies Act, 2013, the Limited
- Liability Partnership Act, 2008, and the Partnership Act, 1932;
- Securities transactions regulations under the SCRA;
- Payment and settlement system requirements under the Payment and Settlement Systems Act, 2007; and
- Detailed banking and finance regulations under the Banking Regulation Act, 1949, the Recovery of Debts Due to Banks and Financial Institutions Act, 1993 (commonly known as the 'Debt Recovery Act'), and the Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002 (commonly known as 'SARFAESI').

In addition to the broader principle of trust placed in centralized regulators and regulated entities, many of these requirements will struggle to be satisfied by the blockchain because of its electronic, trustless, and decentralized nature. As blockchain technology gains ground in India, lawmakers can consider a legislation relaxing procedural requirements that impede its progress (hence impeding innovation). These requirements may have been suitable for an older way of doing things but will likely be obviated by the unique features of the blockchain. The French government's regulations on securities, discussed earlier, are a good example of regulations expressly enabling the use of the blockchain.

6. Practical Challenges

The blockchain is fascinating in theory, but some consider it overhyped.[192] They believe that the numbers on its funding, manpower, and adoption do not live up to the many ambitious estimates of its potential.[193] The following are some challenges that it will have to face if it is to reach its predicted success:

I. Cybersecurity

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.[194] 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, and DAOs has sometimes not been watertight. One security weakness at a more fundamental level is the importance attached to participants' private keys: some have stated, "*[p]ermanent loss of a private encryption key would be a lot like loss of life.*"[195] Organizations may thus face a security v. cost tradeoff that *"either means your blockchain is cheap but risky or expensive and secure."*[196]

II. Widespread Adoption

Mr. A. P. Hota, the erstwhile CEO and Managing Director of India's NPCI, remarked after a blockchain event, *"[w]hile it was clear that the technology is radical, unless the entire ecosystem moves toward it, it is hardly of any significance."*[197] This can be easily understood when we consider that the value of Bitcoins is only existent because people are willing to trade currency/goods/services for them. A Bitcoin network of a few people would be of little consequence. Credit Suisse has also pointed out that "critical mass" is essential for the blockchain's success, and that players like R3 (through the initiatives and partnerships discussed previously) are making positive steps towards this.[198] However, the inertia of established systems (and the integration of the blockchain with them); skepticism towards Bitcoin and the blockchain as 'rebel' systems; and the high cost of a sophisticated blockchain deployment may be challenges to widespread adoption.[199]

III. Necessity

The question arises why established industries and processes should break a working status quo and use the blockchain.[200] This is the case when as in banking services, the blockchain's features do not easily support some processes taken for granted today, such as chargebacks/refunds by banks after fraudulent transactions. According

192. https://www.bloomberg.com/gadfly/articles/2016-09-08/blockchain-s-ambitions-thwarted-by-funding-resources; http://www.coindesk.com/reached-peak-blockchain-hype/ (last visitedOctober 3, 2016)

193. Id.

194. https://www.forbes.com/sites/forbestechcouncil/2018/09/17/why-are-crypto-exchanges-are-hacked-so-often/ (last visited November 16, 2018)

195. http://www.lexology.com/library/detail.aspx?g=ee10aaof-3447-4088-81dd-7521244fecb3 (last visited October 3, 2016)

196. http://www.businessinsider.com/credit-suisse-on-the-challenges-for-blockchain-going-mainstream-2016-8 (last visited October3, 2016)

197. http://timesofindia.indiatimes.com/business/india-business/Next-Banking-Disruption-Lies-In-One-Open-Online-Ledger/articleshow/54318646.cms (last visited October 3, 2016)

198. http://www.businessinsider.com/credit-suisse-on-the-challenges-for-blockchain-going-mainstream-2016-8 (last visited October3, 2016)

199. http://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html; http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF (last visited October 3, 2016)

200. http://www.businessinsider.com/credit-suisse-on-the-challenges-for-blockchain-going-mainstream-2016-8 (last visited October 3, 2016)

to Credit Suisse, blockchain technology will only be useful in a particular application if parties *"(1) require a database, (2) need shared write access, (3) have unknown writers whose interests are not unified, and (4) not trust a third party to maintain the integrity of the data."*[201] Organizations should therefore look beyond the excitement and carefully assess whether the blockchain is suitable and can adapt to their needs.

IV. Teething Problems

Many have acknowledged that the blockchain is a nascent technology, and its real-world applications outside Bitcoin, and to some extent Ethereum, are still largely untested.[202] Some experts, while positive about the technology, give it 10 to 20 years to become mainstream.[203] Aspects such as the speed of transactions, the process of verification, and data limits therefore still have to find their 'sweet spot' in non-Bitcoin applications.[204]

V. Privacy

The transparency that is essential to the blockchain, combined with the ability to trace participants' real identities, can lead to serious privacy implications (see the previous section's discussion of this issue).[205]

VI. Energy Consumption

Some have also drawn attention to the substantial energy consumption by blockchain networks, because of the computationally intensive process of mining/verification.[206] However, newer technologies, such as the more widespread use of the 'proof of stake' algorithm are expected to improve energy efficiency over the long run.[207]

201. Id.

202. http://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html; http://www.businessinsider.com/credit-suisse-on-the-challenges-forblockchain-going-mainstream-2016-8; http://www.clydeco.com/uploads/Files/CC010565_Blockchain_brochure_10-06-16_LOWRES.PDF (last visited October 3, 2016)

203. http://www.coindesk.com/blockchain-decade-away-mainstream/(last visited October 3, 2016)

204. http://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html (last visited October 3, 2016)

205. Also see id.; http://www.businessinsider.com/credit-suisse-onthe-challenges-for-blockchain-going-mainstream-2016-8. (lastvisited October 3, 2016

206. http://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html (last visited April 25, 2017)

207. https://www.cnbc.com/2018/02/23/bitcoin-blockchain-consumes-a-lot-of-energy-engineers-changing-that.html

7. Conclusion

Blockchain is no doubt a revolutionary technology, replacing trust with math-based security to a large extent. However, many oft-touted blockchain use-cases need to be critically examined to see if they actually utilize blockchain's key innovation i.e., decentralization. Centralization can often bring with it efficiency and accountability benefits, and decentralization may result in certain trade-offs in this regard. However, decentralization is useful in cases where there are multiple parties who wish to transact with each other and do not have a system of trust or regulation on which to fall back. This makes cross-border transactions between multiple untrusted parties (e.g., a global B2B distribution network) particularly suitable. This would appear to be the reason why the Bitcoin network has gained such traction.

Like any new technology or business model, the blockchain brings along with its benefits a host of legal, strategic, and operational challenges. As lawyers, we foresee several legal grey areas that could arise as a result of the blockchain being deployed in the various industries that it has applications in. While it is heartening to see that some jurisdictions like Malta have taken the lead in creating regulations around blockchain, in the Indian context, we would not recommend hasty or technology-specific regulation of this technology, since it is complex and calls for time and effort to be put into understanding its implications. Further, principle-based regulation tends to be more time-proof than technology-specific regulation. A rushed job is likely to impede innovation. At the same time, left unregulated, courts, adjudicators, and commercial parties will be left trying to fit square pegs into round holes to understand how the technology fits within existing legal rules. A measured approach to regulation, that clarifies ambiguities where necessary, would hence be ideal.

Certain blockchain use-cases would also would need legal amendments in light of their decentralized nature, since existing regulation usually places trust in centralized parties i.e., licensed entities and regulators. This is a public policy that needs to be taken, since some amendments e.g., decentralization of land records, may be considered radical by many.

Further, the law in India on virtual currencies is currently in flux. There is a pending Supreme Court case against the RBI's circular on the subject, as well as a multi-stakeholder government committee that is due to submit its report on the legal treatment of virtual currencies. The government has made several pro-blockchain statements in various reports and press statements, but has continually cautioned against the risks associated with virtual currencies.

In our view, the blockchain as a system would be rendered either impotent or severely restricted (depending on the blockchain implementation) without any virtual currency / crypto-token. This has been recognized by several global experts including Ethereum co-founder Vitalik Buterin and author Andreas Antonopoulos. 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 a wise policy move to try to promote blockchain on the one hand, and severely restrict tokens on the other hand. It is our hope that any impending policy or judicial decision recognizes this fact, and adopts a nuanced framework taking this into account.

Finally, it is essential to ensure that regulators are well-informed about the technology and its benefits, and that the public and private sectors collaborate to arrive at well-balanced policy outcomes. Such outcomes, along with education and awareness initiatives, should aid in the successful adoption of the technology in India, and in India becoming a leading player in the field, just as it has been with other information technologies over the years.

About NDA

At Nishith Desai Associates, we have earned the reputation of being Asia's most Innovative Law Firm – and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium *Aligunjan*, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international firm with offices in Mumbai, Palo Alto (Silicon Valley), Bangalore, Singapore, New Delhi, Munich, and New York. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly – the VISION – to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of Things (IOT), Aviation, Artificial Intelligence, Privatization of Outer Space, Drones, Robotics, Virtual Reality, Ed-Tech, Med-Tech & Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

The firm has been consistently ranked as one of the Most Innovative Law Firms, across the globe. In fact, NDA has been the proud recipient of the Financial Times – RSG award 4 times in a row, (2014-2017) as the **Most Innovative Indian Law Firm.**

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global case study, aptly titled 'Management by Trust in a Democratic Enterprise,' published by John Wiley & Sons, USA.

A brief chronicle our firm's global acclaim for its achievements and prowess through the years -

- **IFLR1000 2019:** Tier 1 for Private Equity and Project Development: Telecommunications Networks.
- **AsiaLaw 2019:** Ranked 'Outstanding' for Technology, Labour & Employment, Private Equity, Regulatory and Tax
- **RSG-Financial Times:** India's Most Innovative Law Firm (2014-2017)
- **Merger Market 2018:** Fastest growing M&A Law Firm
- **IFLR:** Indian Firm of the Year (2010-2013)
- **Legal 500 2018:** Tier 1 for Disputes, International Taxation, Investment Funds, Labour & Employment, TMT
- **Legal 500 (2011, 2012, 2013, 2014):** No. 1 for International Tax, Investment Funds and TMT

- **Chambers and Partners Asia Pacific (2017 – 2018):** Tier 1 for Labour & Employment, Tax, TMT
- **IDEX Legal Awards 2015:** Nishith Desai Associates won the "M&A Deal of the year", "Best Dispute Management lawyer", "Best Use of Innovation and Technology in a law firm" and "Best Dispute Management Firm"

Please see the last page of this paper for the most recent research papers by our experts.

Disclaimer

Contact

For any help or assistance please email us on ndaconnect@nishithdesai.com
or visit us at www.nishithdesai.com

The following research papers and much more are available on our Knowledge Site: **www.nishithdesai.com**

Fund Formation: Attracting Global Investors

March 2018

Social Impact Investing in India

July 2018

The Curious Case of the Indian Gaming Laws

February 2018

Corporate Social Responsibility & Social Business Models in India

March 2018

Incorporation of Company LLP in India

April 2017

Outbound Acquisitions by India-Inc

September 2014

Internet of Things

January 2017

Doing Business in India

September 2018

Private Equity and Private Debt Investments in India

March 2018

NDA Insights

TITLE	TYPE	DATE
Blackstone's Boldest Bet in India	M&A Lab	January 2017
Foreign Investment Into Indian Special Situation Assets	M&A Lab	November 2016
Recent Learnings from Deal Making in India	M&A Lab	June 2016
ING Vysya - Kotak Bank : Rising M&As in Banking Sector	M&A Lab	January 2016
Cairn – Vedanta : 'Fair' or Socializing Vedanta's Debt?	M&A Lab	January 2016
Reliance – Pipavav : Anil Ambani scoops Pipavav Defence	M&A Lab	January 2016
Sun Pharma – Ranbaxy: A Panacea for Ranbaxy's ills?	M&A Lab	January 2015
Reliance – Network18: Reliance tunes into Network18!	M&A Lab	January 2015
Thomas Cook – Sterling Holiday: Let's Holiday Together!	M&A Lab	January 2015
Jet Etihad Jet Gets a Co-Pilot	M&A Lab	May 2014
Apollo's Bumpy Ride in Pursuit of Cooper	M&A Lab	May 2014
Diageo-USL- 'King of Good Times; Hands over Crown Jewel to Diageo	M&A Lab	May 2014
Copyright Amendment Bill 2012 receives Indian Parliament's assent	IP Lab	September 2013
Public M&A's in India: Takeover Code Dissected	M&A Lab	August 2013
File Foreign Application Prosecution History With Indian Patent Office	IP Lab	April 2013
Warburg - Future Capital - Deal Dissected	M&A Lab	January 2013
Real Financing - Onshore and Offshore Debt Funding Realty in India	Realty Check	May 2012

Research @ NDA

Research is the DNA of NDA. In early 1980s, our firm emerged from an extensive, and then pioneering, research by Nishith M. Desai on the taxation of cross-border transactions. The research book written by him provided the foundation for our international tax practice. Since then, we have relied upon research to be the cornerstone of our practice development. Today, research is fully ingrained in the firm's culture.

Our dedication to research has been instrumental in creating thought leadership in various areas of law and public policy. Through research, we develop intellectual capital and leverage it actively for both our clients and the development of our associates. We use research to discover new thinking, approaches, skills and reflections on jurisprudence, and ultimately deliver superior value to our clients. Over time, we have embedded a culture and built processes of learning through research that give us a robust edge in providing best quality advices and services to our clients, to our fraternity and to the community at large.

Every member of the firm is required to participate in research activities. The seeds of research are typically sown in hour-long continuing education sessions conducted every day as the first thing in the morning. Free interactions in these sessions help associates identify new legal, regulatory, technological and business trends that require intellectual investigation from the legal and tax perspectives. Then, one or few associates take up an emerging trend or issue under the guidance of seniors and put it through our "Anticipate-Prepare-Deliver" research model.

As the first step, they would conduct a capsule research, which involves a quick analysis of readily available secondary data. Often such basic research provides valuable insights and creates broader understanding of the issue for the involved associates, who in turn would disseminate it to other associates through tacit and explicit knowledge exchange processes. For us, knowledge sharing is as important an attribute as knowledge acquisition.

When the issue requires further investigation, we develop an extensive research paper. Often we collect our own primary data when we feel the issue demands going deep to the root or when we find gaps in secondary data. In some cases, we have even taken up multi-year research projects to investigate every aspect of the topic and build unparallel mastery. Our TMT practice, IP practice, Pharma & Healthcare/Med-Tech and Medical Device, practice and energy sector practice have emerged from such projects. Research in essence graduates to Knowledge, and finally to *Intellectual Property*.

Over the years, we have produced some outstanding research papers, articles, webinars and talks. Almost on daily basis, we analyze and offer our perspective on latest legal developments through our regular "Hotlines", which go out to our clients and fraternity. These Hotlines provide immediate awareness and quick reference, and have been eagerly received. We also provide expanded commentary on issues through detailed articles for publication in newspapers and periodicals for dissemination to wider audience. Our Lab Reports dissect and analyze a published, distinctive legal transaction using multiple lenses and offer various perspectives, including some even overlooked by the executors of the transaction. We regularly write extensive research articles and disseminate them through our website. Our research has also contributed to public policy discourse, helped state and central governments in drafting statutes, and provided regulators with much needed comparative research for rule making. Our discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged. Although we invest heavily in terms of time and expenses in our research activities, we are happy to provide unlimited access to our research to our clients and the community for greater good.

As we continue to grow through our research-based approach, we now have established an exclusive four-acre, state-of-the-art research center, just a 45-minute ferry ride from Mumbai but in the middle of verdant hills of reclusive Alibaug-Raigadh district. **Imaginarium AliGunjan** is a platform for creative thinking; an apolitical eco-system that connects multi-disciplinary threads of ideas, innovation and imagination. Designed to inspire 'blue sky' thinking, research, exploration and synthesis, reflections and communication, it aims to bring in wholeness – that leads to answers to the biggest challenges of our time and beyond. It seeks to be a bridge that connects the futuristic advancements of diverse disciplines. It offers a space, both virtually and literally, for integration and synthesis of knowhow and innovation from various streams and serves as a dais to internationally renowned professionals to share their expertise and experience with our associates and select clients.

We would love to hear your suggestions on our research reports. Please feel free to contact us at

research@nishithdesai.com

Nishith Desai Associates

LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI

93 B, Mittal Court, Nariman Point
Mumbai 400 021, India

tel +91 22 6669 5000
fax +91 22 6669 5001

SILICON VALLEY

220 California Avenue, Suite 201
Palo Alto, CA 94306-1636, USA

tel +1 650 325 7100
fax +1 650 325 7300

BANGALORE

Prestige Loka, G01, 7/1 Brunton Rd
Bangalore 560 025, India

tel +91 80 6693 5000
fax +91 80 6693 5001

SINGAPORE

Level 30, Six Battery Road
Singapore 049 909

tel + 65 65509855

MUMBAI BKC

3, North Avenue, Maker Maxity
Bandra–Kurla Complex
Mumbai 400 051, India

tel +91 22 6159 5000
fax +91 22 6159 5001

NEW DELHI

C–5, Defence Colony
New Delhi 110 024, India

tel +91 11 4906 5000
fax +91 11 4906 5001

MUNICH

Maximilianstraße 13
80539 Munich, Germany

tel +49 89 203 006 268
fax +49 89 203 006 450

NEW YORK

375 Park Ave Suite 2607
New York, NY 10152

tel +1 212 763 0080