

Beyond Bitcoin: Exploring the Blockchain

Industry Applications and Legal
Perspectives

October 2016

Beyond Bitcoin: Exploring the Blockchain

Industry Applications and Legal Perspectives

October 2016

Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

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

ndaconnect@nishithdesai.com

Contents

1. INTRODUCTION	01
2. HOW BLOCKCHAIN TECHNOLOGY WORKS	02
3. STATE OF THE ART IN INDUSTRY	05
I. Platforms	05
II. Blockchain Solutions	06
III. Applications	07
4. REGULATORY REACTION	13
I. Early Days	13
II. Positive Indications; 'Regulatory Sandboxes'	13
III. Indian Response	13
IV. Uncertainty	14
V. French Government Order on Mini-bonds	14
5. FORECASTING LEGAL ISSUES	15
I. Pseudonymity and Legal Enforcement	15
II. Privacy and Cybersecurity	15
III. Complications Associated with Decentralized Autonomous Organizations (DAOs)	17
IV. Complications due to Immutability and Irreversibility	18
V. Jurisdictional Questions	18
VI. Contract Law Grey Areas	19
VII. Whether Blockchain Tokens are 'Securities'	20
VIII. Adaptations of Older Requirements	20
6. PRACTICAL CHALLENGES	22
I. Cybersecurity	22
II. Widespread Adoption	22
III. Necessity	22
IV. Teething Problems	23
V. Privacy	23
VI. Uncertain Regulatory Status	23
VII. Energy Consumption	23
7. CONCLUSION	24

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, to prevent ‘double spending’ of the same units. Users of the payment system must hence entirely trust and rely on these central authorities – usually, governments and banks. While there were virtual currencies before Bitcoin, including cryptocurrencies (i.e., currencies 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 blockchain technology is often referred to as ‘distributed ledger’ technology, and the blockchain is called a ‘distributed ledger.’

We have separately published a research paper on the legal and tax consequences surrounding Bitcoin.¹ This research paper focuses on the broader concept of the blockchain itself.

Blockchain technology has attracted a lot of industry attention over the past year. 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. Over the past year, over 50 major financial institutions including Barclays, Goldman Sachs, J.P. Morgan, Morgan Stanley, BNP Paribas, and Wells Fargo, have formed a consortium in partnership with R3, a prominent financial technology (“**fintech**”) firm, to explore the application of the blockchain to their businesses.²

Homegrown firms Infosys, TCS, Wipro, and Cognizant have made significant investments in expanding their capabilities in the technology.³ Infosys and TCS are in fact the first two large companies globally to have rolled out the use of blockchain in core banking platforms.⁴ The use of blockchain in a variety of other sectors is being explored and is widely predicted.⁵ Governments too have shown interest in the technology, with the U.K. government in particular being a big backer.⁶

Businesses across industries should therefore be actively assessing how the blockchain can help streamline tasks for them. 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.

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

2. <https://r3cev.com/press/2016/8/31/press-release-metlife-joins-r3-distributed-ledger-consortium> (last visited October 3, 2016)

3. <http://www.livemint.com/Companies/bXjPtIHZRK46FQVb2hxyN/TCS-throws-weight-behind-blockchain.html>, <http://www.livemint.com/Companies/9bfMN9evtiDSsJZaq16w8M/Indian-IT-firms-eye-technology-behind-Bitcoin-for-disruptive.html>; <http://www.livemint.com/Companies/05UolSzi9taRIdc5tDi5M/Wipro-steps-up-blockchain-focus.html> (last visited October 3, 2016)

4. <http://www.livemint.com/Companies/bXjPtIHZRK46FQVb2hxyN/TCS-throws-weight-behind-blockchain.html> (last visited October 3, 2016)

5. *E.g.*, <http://www.businessinsider.com/goldman-blockchain-beyond-the-hype-practical-uses-2016-5?r=UK&IR=T>; <http://www.bloomberg.com/news/articles/2016-05-19/built-for-bitcoin-blockchain-goes-beyond-crypto-currency>; <http://www.cio.com/article/3115776/internet/how-blockchain-will-disrupt-your-business.html>; <http://www.healthcareitnews.com/news/one-unveils-winners-blockchain-health-it-challenge> (last visited October 3, 2016)

6. <http://www.zdnet.com/article/blockchain-as-a-service-approved-for-use-across-uk-government/>; *see also* <http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hermano-de-soto-bitfury/#3016dcbd6550>, <http://www.coindesk.com/bitfury-working-with-georgian-government-on-blockchain-land-registry/> (last visited October 3, 2016)

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 in real time⁷ whenever a transaction is completed. The device of each participant or user is usually referred to as a 'node,' which forms part of a network of nodes.

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.⁹ Hence, participants do 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



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 (for Bitcoin, this process now takes over 24 hours).⁸ From then on, it will join the other nodes in

transaction is recorded on the Bitcoin blockchain. However, the transactions could also be something like real estate title transfers, as discussed later in this paper.

7. As a practical matter, transactions are usually processed in batches, or 'blocks', at intervals of, in most cases, a few minutes.

8. <http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html> (last visited October 3, 2016)

9. *E.g.*, http://enigma.mit.edu/enigma_full.pdf. However, aspects of the *implementation* of blockchain technology have been found vulnerable on many occasions (e.g., <http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6?op=1>), and this will be discussed in more detail subsequently in this paper. (last visited October 3, 2016)

Technical Perspective

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

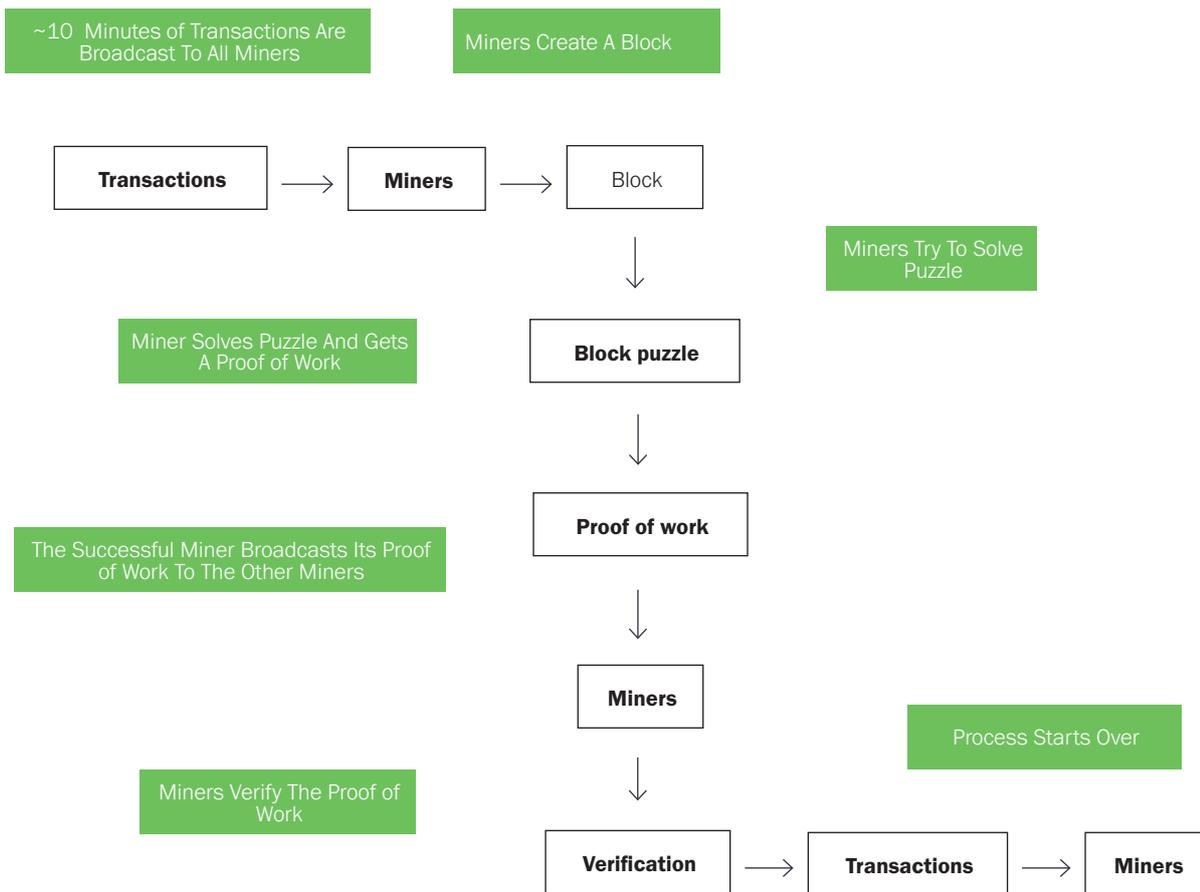
Once the digital signature of a transaction is authenticated, it gets pooled with other authenticated transactions into a 'block.' After the first block, a series or 'chain' of blocks gets formed, hence leading to the term 'blockchain.' This is where a second level of cryptography comes in.

To prevent fraud and double spending, it is important that the order of transactions is authentic. This is not automatically ensured because a transaction message reaches different nodes at different points in time (owing to varying network speeds). 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. Else, for example, a buyer could send a payment, and before that message reached the seller, the buyer could send the payment back to itself.¹⁰ 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.

The blockchain 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. A block can only be read and made sense of after it is decrypted. 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.

10. <http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html> (last visited October 3, 2016)



BI Intelligence

Source: Business Insider,¹¹ bullfax.com¹²

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.

The blockchain is likely best used when:

1. There are a series of transactions / events.
2. They need to be recorded.

3. They need to be verified.

Verification occurs with respect to:

- a. The integrity of the information, and
- b. The integrity of the order of events.

4. There are several participants in the system.
5. Transparency is important.
6. Decentralization is important.
7. Permanence is important.

Based on these features, it is easy to see why some of the leading use cases being proposed for the blockchain are financial clearing and settlement and many record-keeping functions, like the maintenance of real estate records.

3. State of the Art in Industry

The discussion on the current industry state of the art is best divided by speaking of:

1. Platforms – These are targeted at developers who can use the platform to build blockchain-based applications that can then be used by end-users (enterprises or consumers). A well-known example is the ‘Ethereum’ platform.
2. Blockchain Solutions – These are targeted at organizations who wish to deploy blockchain technology for custom use in their organization, but need professional assistance to do so. This assistance may be through product or service offerings. Microsoft’s ‘Azure Blockchain as a Service’ is a significant example.
3. Applications – These are the fruits of the underlying technology, and are designed to accomplish specific tasks for end-users that lead to tangible results (e.g., payment and settlement, record-keeping, and voting).

This is because Ethereum is written in a scripting language that is fully-functional, or ‘Turing-complete,’ as opposed to Bitcoin which was designed only to facilitate exchanges of Bitcoin value.¹³ Ethereum is based on ‘smart contracts,’ which are computer protocols that allow transactions between users to be programmed and then executed automatically (as opposed to then existing blockchain technology which only kept a record of transactions).¹⁴ For example, a smart contract can allow a buyer to make payment only after goods or services are actually delivered. If the parties have agreed what the delivery event is, this can be programmed into the smart contract, which will automatically debit the buyer’s account once delivery has occurred. It is easy to see how this system can support complex commercial transactions, eliminating manual labour and human error.

Buterin envisaged three types of applications for Ethereum:¹⁵

- i. Financial: These refer to purely financial uses and include financial derivatives, hedging contracts, savings wallets, and wills.
- ii. Semi-financial: These refer to uses where there is both a monetary and a non-monetary side to the transaction. Buterin’s example is of self-executing rewards to programmers for solutions to computational problems.
- iii. Non-financial: These refer to applications such as online voting.

I. Platforms

A. Ethereum

After Bitcoin, Ethereum is probably the most well-known deployment of blockchain technology, and is in fact the second largest cryptocurrency in the world after Bitcoin.¹¹ It was conceived in 2013 by Vitalik Buterin, a young programmer (just 19 years old at the time) who was heavily involved in research and writing on Bitcoin, cryptocurrencies, and their underlying technology i.e., the blockchain. He released a white paper, “*A Next-Generation Smart Contract and Decentralized Application Platform*”¹² which proposed a system through which blockchain technology could be used in applications beyond Bitcoin and cryptocurrencies.

11. <http://fortune.com/2016/09/04/ethereum-fall-out/> (last visited October 3, 2016)

12. <https://github.com/ethereum/wiki/wiki/White-Paper> (last visited October 3, 2016)

13. <https://techcrunch.com/2015/08/01/vapor-no-more-ethereum-has-launched/> (last visited October 3, 2016)

14. “*They are pieces of software, not contracts in the legal sense, that extend blockchains’ utility from simply keeping a record of financial transaction entries to automatically implementing terms of multiparty agreements.*” http://d27n20517r0okf.cloudfront.net/wp-content/uploads/2016/06/DUP_2833_Smart-contracts_vFINAL.pdf, p. 2; <http://www.ethnews.com/smart-contracts>. (last visited October 3, 2016)

15. <https://github.com/ethereum/wiki/wiki/White-Paper> (last visited October 3, 2016)

Ethereum's initial release was in July 2015, and it quickly became a buzzword in technology circles. Numerous startups began and continue to construct applications based on its platform. Microsoft's offering of Ethereum as part of its cloud platform 'Azure,'¹⁶ is likely to lead mainstream use of the Ethereum platform.

Recently, a massive user of Ethereum, 'The DAO,' a decentralized autonomous organization which pooled money from investors (as a kind of decentralized investment fund), was involved in a cybersecurity breach. Its underlying code was exploited, enabling unidentified hackers to siphon off cryptocurrency (Ethereum units called 'ether') worth tens of millions of U.S. dollars (some estimates say USD 60 million).¹⁷ After much debate, the Ethereum community reached a technical solution (a 'hard fork') that enabled much, but not all, of the stolen cryptocurrency to be rolled back.¹⁸ Though blockchain technology as such is widely acknowledged to be secure, the breach shows that its implementation, especially in high-value contexts, can be risk-ridden unless done with extreme care. The breach has led to some skepticism as to the extent to which blockchain technology can replace laws and financial institutions as securers of commercial transactions.¹⁹

B. Bitcoin and Colored Coins

Though a discussion of Bitcoin as a currency is outside the scope of this paper, the Bitcoin blockchain can be used for applications other than the exchange of Bitcoin value. 'Colored Coins' is an open source protocol that allows developers to use the Bitcoin blockchain for applications beyond currency, for nearly any exchange of value that can occur online.²⁰ Also, Blockstack Labs has developed 'Blockstack,' which uses the Bitcoin

blockchain and supports applications for uses such as payment and settlement, recording and transfer of digital assets, and smart contracts.²¹

C. Chain Open Standard

Chain is a leading blockchain-focused organization which is partnering with several well-known financial organizations to "*build blockchain networks that transform markets.*"²² The impressive list of its partners includes Capital One, Citigroup, Fidelity, Nasdaq, State Street, and Visa, among others.²³ It recently announced the release of 'Chain Open Standard 1,' an open source blockchain protocol tailored to the development of financial applications.²⁴ The Open Standard is meant to ensure transaction finality as well as protect privacy.²⁵ Applications that facilitate simple payment, asset issuance, bilateral trade, transaction ordering, collateralized loans, and auctions, among other functions, can be built using the Open Standard.²⁶ Chain also provides blockchain solutions to enterprises, and this is discussed in the next section.

II. Blockchain Solutions

A. Azure Blockchain as a Service

Microsoft Azure, which is a leading cloud service provider (Amazon Web Services is the other notable name in the industry), now offers Blockchain as a Service (BaaS) as part of its cloud offering. Microsoft describes the service, 'Azure Blockchain as a Service,' as a "*single click cloud based blockchain developer environment.*"²⁷ It is meant to allow enterprises, business networks, and developers to experiment and collaborate on blockchain deployment.²⁸

16. Details follow in the next section.

17. <http://fortune.com/2016/06/18/blockchain-vc-fund-hacked/>; <http://www.coindesk.com/author-daos-original-code-minimize-regulatory-backlash/> (last visited October 3, 2016)

18. <http://fortune.com/2016/09/04/ethereum-fall-out/> (last visited October 3, 2016)

19. *Id.*

20. <http://coloredcoins.org/> (last visited October 3, 2016)

21. <http://coloredcoins.org/>; <https://www.dxmarkets.com/>; <https://mycelium.com/> (last visited October 3, 2016)

22. <https://chain.com/> (last visited October 3, 2016)

23. *Id.*

24. <https://chain.com/os> (last visited October 3, 2016)

25. <http://www.prnewswire.com/news-releases/chain-and-global-financial-firms-unveil-open-standard-for-blockchain-300260512.html> (last visited October 3, 2016)

26. <https://chain.com/showcase> (last visited October 3, 2016)

27. <https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/> (last visited October 3, 2016)

28. <https://azure.microsoft.com/en-us/solutions/blockchain/>

It was first announced in 2015, and integrates various existing distributed ledger technologies including the Ethereum blockchain and Eris (discussed below).

B.Chain

Chain, mentioned earlier, is building blockchain networks targeted at the financial industry.²⁹ It offers ‘Chain Core,’ which enterprises can use to initiate, operate, or connect to a blockchain network, and ‘Chain Sandbox,’ which development teams can use to build upon Chain Core.³⁰

C.Eris

Eris is a blockchain platform developed by Eris Industries, targeted at “information age organizations,”³¹ ranging from businesses to governments. It uses aspects of Ethereum, along with changes, to customize blockchain technology for industry adoption.³² It offers products like pre-written smart contract libraries, services like smart contract drafting, and ongoing support to help organizations easily adopt blockchain for use in their particular activities.³³ According to Microsoft, “[t]he Eris platform greatly reduces the complexity of creating blockchain-based applications. ... Eris also makes it simple and easy for your organization to get started using permissionable [i.e., access-controlled], smart-contract capable blockchains.”³⁴ PricewaterhouseCoopers (PwC) recently announced a strategic partnership with Eris Industries.³⁵

29. <https://chain.com/> (last visited October 3, 2016)

30. <https://chain.com/core/>, <https://chain.com/sandbox/> (last visited October 3, 2016)

31. <https://erisindustries.com/components/erisdb/> (last visited October 3, 2016)

32. *Id.*

33. <https://erisindustries.com/products/> (last visited October 3, 2016)

34. <https://azure.microsoft.com/en-in/blog/azure-blockchain-as-a-service-update-4/> (last visited October 3, 2016)

35. <https://bitcoinmagazine.com/articles/pwc-partners-with-blockstream-and-eris-industries-to-create-blockchain-solution-portfolio-1454359482> (last visited October 3, 2016)

III. Applications

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

A.Financial Services / Fintech

i. Banking

In a recent report, Deloitte identified ‘trade clearing and settlement’ as one among two use cases of smart contracts that were most immediate to market.³⁶ 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.³⁷

A recent report by the innovation fund of Santander Bank predicts cost-savings of USD 15 to 20 billion by 2022, as a result of blockchain technology reducing financial infrastructure costs.³⁸ 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.³⁹ These processes are cost- and labor-intensive, and are subject to delay and human error.⁴⁰ This is exacerbated by each bank / financial institution having to independently process transactions.⁴¹

36. <http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-about-smart-contracts/>. The other use case is supply chain and trade finance documentation, mentioned under the ‘Legal Services’ section subsequently. (last visited October 3, 2016)

37. “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 October 3, 2016)

38. <http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-about-smart-contracts/>; <http://santanderinnovations.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf> (last visited October 3, 2016)

39. <http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-about-smart-contracts/> (last visited October 3, 2016)

40. *Id.*

41. *Id.*

Several financial institutions, investment funds, and financial infrastructure bodies have taken notice of the potential impact of blockchain technology on clearing and settlement. As mentioned earlier, R3 leads a consortium of over 50 large financial institutions exploring the use of blockchain technology. Investors in blockchain startups in the clearing and settlement space include Khosla Ventures, SV Angel, Citigroup, JP Morgan, and Santander.⁴² Recently, 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.⁴³ Also recently, seven major European financial institutions, including BNP Paribas Securities, announced a Memorandum of Understanding to explore the development of a post-trade blockchain-based infrastructure for small and medium enterprises in Europe.⁴⁴

Closer home, Kotak Mahindra Bank, Axis Bank, and ICICI Bank have announced their interest in blockchain technology.⁴⁵ Yes Bank and IDFC Bank recently partnered with a blockchain-driven fintech startup, 'Uphold,' to enable cross-border payments into India.⁴⁶ The National Payments Corporation of India (NPCI) recently held an "ideathon," and has set up a working group, to help it understand the implications of blockchain technology.⁴⁷

Interest has extended to the public sector too. Central bank officials from over 90 countries, including the Chair of the U.S. Federal Reserve, and officials from the International Monetary Fund, World Bank and the Bank for International Settlements recently attended a

keynote talk on the blockchain by the CEO of Chain.⁴⁸ He explained how blockchain technology can help them "*operate the digital networks themselves, issue digital assets, hold those assets, create products and services to run on those networks or just observe them.*"⁴⁹ The talk was received with interest.⁵⁰

In India, a multi-stakeholder panel comprising members from the Reserve Bank of India (RBI), Institute for Development & Research in Banking Technology (IDRBT), and industry is to look into the implications of blockchain technology.⁵¹ More detail on the RBI's perspective is covered under Section 4 ("Regulatory Reaction") below.

ii. Securities

In 2015, Nasdaq announced an enterprise-wide initiative to leverage blockchain technology.⁵² Its first use was to "*offer efficient, fully-electronic services that facilitate the issuance, transfer, and management of private company securities.*"⁵³ It is also using the technology to enable some public companies' shareholders exercise their corporate voting rights.⁵⁴

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.⁵⁵ The Framework allows clients to leverage blockchain technology, as one of many other capabilities, including machine learning, for their individual needs.⁵⁶

Nasdaq was one of the first multinational financial services companies to begin using the blockchain in

42. *Id.*

43. <http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-about-smart-contracts/>; <http://www.dtcc.com/news/2016/march/29/dtcc-and-digital-asset-to-develop-distributed-ledger-solution> (last visited October 3, 2016)

44. <http://www.businesswire.com/news/home/20160621006306/en/Euronext%20%20Major-Financial-Institutions-Join-Forces-Develop> (last visited October 3, 2016)

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

46. *Id.*; <https://uphold.com/en/blog/posts/uphold/uphold-opens-cross-border-payments-to-india> (last visited October 3, 2016)

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

48. <http://www.bloomberg.com/news/articles/2016-06-06/central-bankers-told-they-should-be-sprinting-toward-blockchain> (last visited October 3, 2016)

49. *Id.*

50. *Id.*

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

52. <http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196> (last visited October 3, 2016)

53. *Id.*

54. <http://www.bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain>; <http://www.coindesk.com/nasdaq-shareholder-voting-estonia-blockchain/> (last visited October 3, 2016)

55. <http://www.coindesk.com/nasdaq-blockchain-services-global-exchange/> (last visited October 3, 2016)

56. <http://business.nasdaq.com/market-tech/nasdaq-financial-framework> (last visited October 3, 2016)

a non-currency manner.⁵⁷ It sees the blockchain as providing “*extensive integrity, audit ability, governance and transfer of ownership capabilities.*”⁵⁸

Following in its lead, several other stock and commodity exchanges, including India’s National Stock Exchange (NSE), 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.⁵⁹ The NSE is exploring the use of blockchain technology to ensure settlement guarantees.⁶⁰ It recently held a widely-attended conference on blockchain technology, comprising speakers from R3, Nasdaq, JP Morgan Chase, IBM, TCS, and the NSE itself, among others.⁶¹

iii. Derivatives

Derivatives are financial instruments that derive value from underlying assets, which could include stocks, bonds, commodities or even interest rates.⁶² The White Paper which conceptualized Ethereum called financial derivatives “*the most common application of a ‘smart contract’*”.⁶³ 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.*”⁶⁴ This engineering can be done using the various platforms, solutions, and frameworks discussed above, or through specialized blockchain derivatives players like

HitFin. HitFin facilitates the direct trading of custom derivatives between parties, without intermediaries, “within seconds.”⁶⁵

B. Legal Services

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.*”⁶⁶

Barclays has taken the lead in 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>).

57. <http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196> (last visited October 3, 2016)

58. *Id.*

59. <http://www.coindesk.com/10-stock-exchanges-blockchain/>; <http://www.zdnet.com/article/sydney-stock-exchange-to-implement-instant-blockchain-based-settlements/> (last visited October 3, 2016)

60. <http://computer.financialexpress.com/news/nse-looking-at-blockchain-for-ensuring-settlement-guarantees/18956/> (last visited October 3, 2016)

61. <http://futuretech2016.com/conference.html#about1> (last visited October 3, 2016)

62. <https://bitcoinmagazine.com/articles/blockchain-technology-will-profoundly-change-the-derivatives-industry-1464368431> (last visited October 3, 2016)

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

64. <https://bitcoinmagazine.com/articles/blockchain-technology-will-profoundly-change-the-derivatives-industry-1464368431> (last visited October 3, 2016)

65. <http://www.hitfin.com/> (last visited October 3, 2016)

66. <http://deloitte.wsj.com/cfo/2016/06/23/getting-smart-about-smart-contracts/> (last visited October 3, 2016)

Template Editor Agreement Editor Trade Entry Trade Affirmation Trade Viewer 

Credit Support Annex 1995 - England and Wales

Close Edit Delete 

determined for each relevant currency and calculated for each day in that Interest Period on the principal amount of the portion of the Credit Support Balance comprised of cash in such currency, determined by the Valuation Agent for each such day as follows:

(x) the amount of cash in such currency on that day; multiplied by
 (y) the relevant Interest Rate in effect for that day; divided by
 (z) 360 (or, in the case of pounds sterling, 365)

"Interest Period" means the period from (and including) the date on which the Local Business Amount has yet been transferred, the Local Business Amount is transferred to or received by the Transferee) to (but excluding) the Local Business Day on which the current interest amount is transferred.

```
{
  "id": "DailyInterestAmount",
  "type": "Expression",
  "value": "(CashAmount * InterestRate) / (if Currency == 'GBP' then 365 else 360)"
}
```

"Interest Rate" means, with respect to an Eligible Currency, the rate specified in Paragraph 11(f)(i) for that currency.

A still from Barclays' demo of smart contract templates, where legal prose is shown converted to computer code.

Credit: Barclays, R3. Source: <https://vimeo.com/168844103>

Similarly, ChainThat, a startup, is offering a blockchain-based legal contract management system to enterprises.⁶⁷ The solution uses the blockchain for the creation, negotiation, and signing of contracts, along with the automated execution of the contractual obligations within.⁶⁸

C. 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 can 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), and track the regulatory compliance of the property.⁶⁹ 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.

It is not surprising, therefore, that some governments are already exploring the use of blockchain technology for their real estate record systems. The governments of Sweden, Ghana, and Georgia – and according to some sources, the U.S. – have announced proposals to pilot blockchain technology in this context.⁷⁰ 'Ubitquity' offers a real estate blockchain platform that has already begun to be used for real-world property transfers.⁷¹

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.⁷² Besides the real estate initiatives already mentioned, the governments of Delaware, U.S.; Estonia; Russia; Singapore; South Korea; and the U.K. are exploring the use of the blockchain for a variety of services ranging from banking and finance to healthcare.⁷³ The U.K. is in particular very interested

67. <http://chainthat.com/legal/> (last visited October 3, 2016)

68. *Id.*

69. <https://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-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)

70. <https://www.weforum.org/agenda/2016/08/how-disruptive-technology-could-solve-real-estate-s-transparency-problem/>; <http://www.africapropertynews.com/investing/3246-blockchain-and-bitcoin-technology-could-alter-real-estate-deals.html> (last visited October 3, 2016)

71. <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)

72. <http://observer.com/2016/09/why-the-blockchain-is-perfect-for-government-services/> (last visited October 3, 2016)

73. *Id.*

in the potential of the blockchain, both for its own services and as a catalyst for technology innovation in industry.⁷⁴

D. Intellectual Property (IP)

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.⁷⁵ Its solutions help content owners and media businesses with rights management, revenue sharing, and distribution.⁷⁶ Ampliative Art is a non-profit organization that uses blockchain technology to help artists get rewarded for their work through donations and grants.⁷⁷

The blockchain is also being used by some startups to facilitate the development of video games,⁷⁸ and the trading of digital game content.⁷⁹

E. Insurance

The blockchain's applications to insurance involve the streamlining of documentation, Anti-Money-Laundering / Know Your Customer (AML/KYC) processing, and claim processing.⁸⁰ This would be especially useful for wholesale insurance providers.⁸¹ According to Deloitte, 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.⁸² They can also 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).⁸³

ChainThat, mentioned earlier, has adapted blockchain technology to develop a decentralized commercial and specialty insurance placing platform.⁸⁴ A startup called Dynamis is using smart contracts to build a "*peer to peer supplemental unemployment insurance protocol which uses policy holders' social capital to replace underwriters.*"⁸⁵

F. 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.⁸⁶ 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.⁸⁷

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.⁸⁸ It recently announced a partnership with Philips.⁸⁹

74. <https://bitcoinmagazine.com/articles/u-k-government-awards-framework-agreement-to-blockchain-as-a-service-company-credits-1470687028>; www.coindesk.com/uk-blockchain-regulatory-approval (last visited October 3, 2016)

75. <https://monegraph.com/> (last visited October 3, 2016)

76. <https://monegraph.com/everywhere> (last visited October 3, 2016)

77. <http://www.ampliativeart.org/en/faq/>; <http://www.ampliativeart.org/en/example>; <http://www.ampliativeart.org/en/development/> (last visited October 3, 2016)

78. <http://www.trustlessprivacy.com/> (last visited October 3, 2016)

79. <http://ownage.io/> (last visited October 3, 2016)

80. <http://www.businessinsider.com/heres-how-blockchain-can-help-the-wholesale-insurance-industry-2016-8?r=UK&IR=T>; see also <https://proofofphysicaladdress.com/>. (last visited October 3, 2016)

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

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

83. *Id.*

84. <http://chainthat.com/insurance/> (last visited October 3, 2016)

85. <http://www.dynamisapp.com/vision.html> (last visited October 3, 2016)

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

87. *Id.*

88. <https://gem.co/health> (last visited October 3, 2016)

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

G. 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. Energy: There are ventures aiming at creating an energy data exchange platform,⁹⁴ and a platform for distributed solar power.⁹⁵
- iv. Extension to the Physical Realm: Slock.it is a startup that enables machines (e.g., Internet of Things devices) to operate autonomously.⁹⁶ There are also proposals for decentralized ridesharing services,⁹⁷ and a way to automatically prove one’s physical address.⁹⁸

- v. Social networks: Ventures like Project Groundhog⁹⁹ and Akasha¹⁰⁰ seek to use the blockchain to divest power from centralized operators of social networks.
- vi. 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, 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.¹⁰¹ This application of the blockchain was also suggested in the Ethereum white paper.¹⁰²
- vii. Miscellaneous: Some other proposed applications are: decentralized organizations / “future of work” (Ethereum is already a sophisticated user of these);¹⁰³ over-the-air television streaming;¹⁰⁴ a notary service;¹⁰⁵ crowdsourcing;¹⁰⁶ an emergency reporting system;¹⁰⁷ a file storage system;¹⁰⁸ and a domain name registry.¹⁰⁹

90. <http://fortune.com/2016/05/08/why-blockchains-will-change-the-world/>; <http://www.forbes.com/sites/joeharpaz/2016/05/31/will-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-changing-the-game-6195606bod70#.mi8zrmpuq>; <https://github.com/ethereum/wiki/wiki/White-Paper#further-applications> (last visited 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. <http://gridsingularity.com/> (last visited October 3, 2016)

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

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

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

98. <https://proofofphysicaladdress.com/> (last visited October 3, 2016)

99. <https://www.youtube.com/watch?v=WFeJYv3PSaI> (last visited October 3, 2016)

100. <http://akasha.world/> (last visited October 3, 2016)

101. <http://dcentproject.eu/> (last visited October 3, 2016)

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

103. <https://colony.io> (last visited October 3, 2016)

104. <http://dereio.io/> (last visited October 3, 2016)

105. <https://github.com/maran/notareth> (last visited October 3, 2016)

106. <http://getcrystal.net/> (last visited October 3, 2016)

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

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

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

4. Regulatory Reaction

I. Early Days

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, Bitcoin, which was a specific application that disrupted traditional currency systems and had governments around the world scrambling to understand its legal consequences.¹¹⁰ As a response to Bitcoin, some governments instituted licensing requirements for dealing in virtual currencies, such as the New York State Department of Financial Services' 'BitLicense' regime,¹¹¹ and some even went so far as to ban them.¹¹²

II. Positive Indications; 'Regulatory Sandboxes'

As opposed to Bitcoin, most regulators' statements on blockchain technology have been positive.¹¹³ As discussed in the previous section, the blockchain is receiving a lot of interest from governments for innovation in their own services. Further, led by the U.K., many countries including Hong Kong, Australia, Singapore, and Abu Dhabi are exploring the idea of 'regulatory sandboxes' for blockchain (and other types of) innovation.¹¹⁴ Regulatory

sandboxes allow organizations to experiment with innovative business models without fear of regulatory consequences, as long as they meet certain consumer protection norms.¹¹⁵



Source: <https://www.fca.org.uk>

The U.K.'s Financial Conduct Authority is considered by the fintech industry as one of the most forward-thinking regulators worldwide.¹¹⁸

III. Indian Response

In India, as mentioned previously, officials from the RBI are part of a multi-stakeholder group involving the IDRBT and industry representatives to explore the implications of blockchain technology.¹¹⁷ At a recent event, RBI Deputy Governor H. R. Khan 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.*"¹¹⁸ He also said the RBI may set up a committee to study how blockchain technology can reduce the use of paper currency.¹¹⁹

110. See sections 4-6 of our research paper on Bitcoin, available at <http://www.nishithdesai.com/information/research-and-articles/research-papers.html>. (last visited October 3, 2016)

111. <http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf>; <http://www.coindesk.com/regulation/bitlicense/> (last visited October 3, 2016)

112. <http://www.coindesk.com/bolivias-central-bank-bans-bitcoin-digital-currencies/> (last visited October 3, 2016)

113. *E.g.*, <https://www.finextra.com/blogposting/13055/blockchain-playing-in-the-regulatory-sandbox>; <http://www.coindesk.com/south-africas-central-bank-says-open-cryptocurrencies/> (last visited October 3, 2016)

114. <https://www.finextra.com/blogposting/13055/blockchain-playing-in-the-regulatory-sandbox> (last visited October 3, 2016)

115. *Id.*

116. <https://www.ft.com/content/8ab3c696-6634-11e6-8310-ecfobddad227#axzz4IovJIM45> (last visited October 3, 2016)

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

118. *Id.*

119. <http://www.livemint.com/Politics/oIe2NO4WLeJUT8sL3FctUN/RBI-to-study-Blockchain-technology-to-curtail-paper-currency.html> (last visited October 3, 2016)

IV. Uncertainty

However, 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. On this note, the World Federation of Exchanges, the global trade body for exchanges, recently called for regulatory clarity over the use of blockchain to reduce costs in share trading, stating that the lack of clarity was holding back the development of blockchain technology for this purpose.¹²⁰

In October 2016, the Digital Currency and Ledger Defense Coalition (DCLDC), a coalition of nearly 50 prominent U.S. lawyers and academics, was announced.¹²¹ The DCLDC seeks to protect the right of innovators experimenting with blockchain technology, through *pro bono* attorney referrals and the filing of amicus briefs.¹²² Where regulatory sandboxes are not forthcoming, therefore, this can be a powerful fallback for blockchain innovators.

V. French Government Order on Mini-bonds

At the time of writing,¹²³ the only non-virtual-currency-related regulatory move concerning blockchain technology that we came across was a French government order legislating rules surrounding ‘mini-bonds,’ a type of corporate debt instrument facilitating crowdfunding.¹²⁴ The order explicitly permits the issuance and transfer of mini-bonds using the blockchain, given certain adapted procedures and safeguards.¹²⁵ The order states that the registration of the sale transaction in the blockchain will operate as the transfer of title ownership.¹²⁶ A working group is to determine detailed safeguards to ensure reliability, security, and the capacity to be audited.¹²⁷ The order also contains the first known regulatory definition of the blockchain, namely a “shared electronic storage device” or “*a shared electronic recording system allowing for authentication.*”¹²⁸

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 mini-bonds via crowdfunding platforms¹²⁹.

120. <http://www.reuters.com/article/us-exchange-regulations-blockchain-idUSKCN11017Q> (last visited October 3, 2016)

121. <http://www.the-blockchain.com/2016/10/03/40-us-law-firms-join-up-to-form-blockchain-legal-defense-coalition/> (last visited October 3, 2016)

122. <http://www.dcldc.org/> (last visited October 3, 2016)

123. October, 2016.

124. <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).

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.* <https://webcache.googleusercontent.com/search?q=cache:VR-W2iHh822kj:https://btcmanager.com/news/finance/france-issues-new-ruling-for-mini-bonds-trading-on-blockchain-platforms/+&cd=1&hl=en&ct=clnk&gl=us> (last visited October 3, 2016)

129. <https://group.bnpparibas/en/press-release/bnp-paribas-securities-services-expands-blockchain-platform-private-stocks> (last visited October 3, 2016)

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 associated Bitcoin with nefarious activities on the ‘dark web,’ like illegal purchases of banned substances and guns, and financing terrorism.¹³⁰ This was 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.¹³¹ 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.¹³² 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.¹³³ 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.¹³⁴

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.¹³⁵ In addition, ‘private’ or ‘permissioned’ blockchains, which, as opposed to ‘public’ or ‘permissionless’ blockchains (like Bitcoin or Ethereum, which are more commonly used today), 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. Chain’s Open Standard 1, the blockchain protocol targeted at financial institutions and discussed previously, is an example of a permissioned blockchain.¹³⁶

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.¹³⁷ As mentioned, blockchain participants can be identified using their public keys and IP addresses, among other identifiers, and every transaction can be seen by every participant (this is an essential feature of blockchain technology). Since the blockchain is a

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

131. <http://gjzmodo.com/a-friendly-reminder-bitcoin-is-not-anonymous-1682885318> (last visited October 3, 2016)

132. <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)

133. <http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/> (last visited October 3, 2016)

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

135. *E.g.*, <http://www.blockchainme.com/index.html> (last visited October 3, 2016)

136. <https://news.bitcoin.com/chain-open-standard-1-goes-public/> (last visited October 3, 2016)

137. <http://www.lexology.com/library/detail.aspx?g=e1e0a0af-3447-4088-81dd-7521244fecb3>; http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf (last visited October 3, 2016)

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.¹³⁸ 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.¹³⁹ 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,¹⁴⁰ 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.

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.¹⁴¹ Data breaches are

being announced every day, and the Ethereum DAO hack shows 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,¹⁴² and often a 'single point of failure.'¹⁴³ 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, will usually 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,¹⁴⁴ and such standards will have to be referenced into existing law.

138. <http://www.lexology.com/library/detail.aspx?g=ee10aaf-3447-4088-81dd-7521244fecb3> (last visited October 3, 2016)

139. Section 43A, IT Act, read with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. (last visited October 3, 2016)

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

141. <http://www.lexology.com/library/detail.aspx?g=ee10aaf-3447-4088-81dd-7521244fecb3> (last visited October 3, 2016)

142. *Id.*

143. *See e.g.*, this explanation by Vitalik Buterin, a co-founder of Ethereum: <https://www.youtube.com/watch?v=UFDAStVXbc>. (last visited October 3, 2016)

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

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.”¹⁴⁵

The most well-known example of a DAO is ‘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.¹⁴⁶

Being of such a decentralized, pseudonymous nature, DAOs do not fit within existing definitions of legal entities like companies and partnerships.¹⁴⁷ 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 driven purely by consensus.¹⁴⁸ Further, they are not ‘located’ within any particular jurisdiction (they are considered ‘stateless’),¹⁴⁹ so the applicable law is itself a question.¹⁵⁰ The nature of their members’ ‘interest’ in

them is also unclear (as opposed to a company share or partnership stake).¹⁵¹ 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.¹⁵²

These theoretical difficulties become clearer to visualize when one thinks of the recent multi-million dollar hack of the Ethereum DAO, discussed previously.¹⁵³ 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.¹⁵⁴ This is in addition to the difficulty of pinning down responsibility due to anonymity/pseudonymity and decentralization. At the time of writing,¹⁵⁵ 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.¹⁵⁶

145. <https://www.tractica.com/automation-robotics/blockchain-daos-and-the-future-of-government/> (last visited October 3, 2016)

146. <http://fortune.com/2016/05/15/leaderless-blockchain-vc-fund/> (last visited October 3, 2016)

147. 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.pdf> suggesting possible legal organizational structures within which DAOs could fall. (last visited October 3, 2016)

148. <https://medium.com/@BlockChannel/what-is-a-dao-how-do-they-benefit-consumers-f7a0a862f3dc#.g8brl9tgq> (last visited October 3, 2016)

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

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

chure_10-06-16_LOWRES.PDF (last visited October 3, 2016)

151. *Id.*

152. <http://www.clydeco.com/insight/article/ethereums-dao-attack-smart-contracts-and-blockchain-face-their-first-big-te> (last visited October 3, 2016)

153. <http://fortune.com/2016/06/18/blockchain-vc-fund-hacked/> (last visited October 3, 2016)

154. <http://www.clydeco.com/insight/article/ethereums-dao-attack-smart-contracts-and-blockchain-face-their-first-big-te> (last visited October 3, 2016)

155. October, 2016.

156. <http://www.financialexpress.com/archive/legal-concept-of-association-of-persons/372324/>; *C.I.T. v. Indira Balkrishna*, 39 ITR 546. (last visited October 3, 2016)

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.

IV. Complications due to Immutability and Irreversibility

Blockchains cannot be ‘edited’ like conventional ledgers. Once transactions are recorded, they remain in the universal ledger unless every participant agrees otherwise.¹⁵⁷ 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.”¹⁵⁸ This is because while immutability preserves the integrity of transactions, it may become problematic when untrustworthy users have managed to conceal fraud.¹⁵⁹ 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.¹⁶⁰ 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”).¹⁶¹ 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.¹⁶² In the case of an ultra-decentralized technology like the blockchain, the difficulty of these questions is amplified.¹⁶³ 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.¹⁶⁴

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

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

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

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

163. http://www.clydeco.com/uploads/Files/CCo10565_Blockchain_brochure_10-06-16_LOWRES.PDF (last visited October 3, 2016)

164. *Id.*

ensure the harmony of international rules. In this vein, industry groups from around the world have founded the ‘Global Blockchain Forum,’ to “*help shape global regulatory interoperability*” and develop industry best practices.¹⁶⁵

VI. Contract Law Grey Areas

As discussed previously, a key feature of blockchains is the “*formation and execution of digital contracts.*”¹⁶⁶

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).¹⁶⁷ Therefore, automatic execution and machine language create new legal questions:

- 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.¹⁶⁸ 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.¹⁶⁹ (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)¹⁷⁰ may be difficult to pursue, since traditional contract law options like rescission will not be viable.¹⁷¹ 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.¹⁷²

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.¹⁷³ 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,¹⁷⁴ 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

165. <http://www.digitalchamber.org/global-blockchain-forum.html> (last visited October 3, 2016)

166. <http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bf8-8e13-1826e9d2733f> (last visited October 3, 2016)

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

168. <http://www.lexology.com/library/detail.aspx?g=bc1e03ba-1800-4bf8-8e13-1826e9d2733f>; <http://www.lexology.com/library/detail.aspx?g=ee10aa0f-3447-4088-81dd-7521244fecb3> (last visited October 3, 2016)

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

170. <http://www.clydeco.com/insight/article/arbitrating-blockchain-disputes-will-smart-contracts-require-smart-dispute> (last visited October 3, 2016)

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

172. <http://www.clydeco.com/insight/article/smart-contracts-where-law-meets-technology> (last visited October 3, 2016)

173. *Id.*

174. <http://www.clydeco.com/insight/article/arbitrating-blockchain-disputes-will-smart-contracts-require-smart-dispute> (last visited October 3, 2016)

code;¹⁷⁵ 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.¹⁷⁶

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.¹⁷⁷

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 paper on Bitcoins,¹⁷⁸ we concluded that Bitcoins could not be classified either as ‘securities’ or ‘derivatives’ under the Indian 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 currency, nearly anything can be represented on the blockchain. A recent working paper by several well-known thinkers on blockchain technology undertook a detailed analysis

of how blockchain tokens would fall within the ‘securities’ definition under U.S. law.¹⁷⁹ The 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. 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 property conveyances) under various laws;
- Formalities for assignment under intellectual property laws;
- The IT Act’s stipulations on digital 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 Exchange Management Act, 1999;

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

176. Richard Susskind, *Tomorrow’s Lawyers: An Introduction to Your Future* (Oxford University Press, 2013); http://www.weblaw.co.uk/ebooks/eGuide_BlockchainTheConceptandtheLaw.pdf; <http://www.lexology.com/library/detail.aspx?g=bce03ba-1800-4bf8-8e13-1826e9d2733f> (last visited October 3, 2016)

177. <http://www.clydeco.com/insight/article/smart-contracts-where-law-meets-technology> (last visited October 3, 2016)

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

179. <http://bollier.org/sites/default/files/misc-file-upload/files/DistributedNetworksandtheLaw%20report,%20Swarm-Coin%20Center-Berkman.pdf> (last visited October 3, 2016)

- 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, and forward contracts regulation under the Forward Contracts (Regulation) Act, 1952;
- 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').

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 order on mini-bonds, discussed earlier, is a good example of a regulation expressly enabling the use of the blockchain.

6. Practical Challenges

The blockchain is fascinating in theory, but some consider it overhyped.¹⁸⁰ They believe that the numbers on its funding, manpower, and adoption do not live up to the many ambitious estimates of its potential.¹⁸¹

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 recent August 2016 hack of the exchange Bitfinex, resulting in losses amounting to about USD 72 million.¹⁸² 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."¹⁸³

Organizations may thus face a security v. cost trade-off that "either means your blockchain is cheap but risky or expensive and secure."¹⁸⁴

180. <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 visited October 3, 2016)

181. *Id.*

182. <http://www.coindesk.com/bitcoin-price-bruised-bitfinex/> (last visited October 3, 2016)

183. <http://www.lexology.com/library/detail.aspx?g=ee10a0f-3447-4088-81dd-7521244fecb3> (last visited October 3, 2016)

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

II. Widespread Adoption

Mr. A. P. Hota, CEO and Managing Director of India's NPCI, recently said 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."¹⁸⁵ 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.¹⁸⁶ 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.¹⁸⁷

III. Necessity

The question arises why established industries and processes should break a working status quo and use the blockchain.¹⁸⁸ 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

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

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

187. <http://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html>; http://www.clydeco.com/uploads/Files/CCo10565_Blockchain_brochure_10-06-16_LOWRES.PDF (last visited October 3, 2016)

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

chargebacks/refunds by banks after fraudulent transactions. According 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.”¹⁸⁹ 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 applications outside Bitcoin are still largely untested.¹⁹⁰ Some experts, while positive about the technology, give it 10 to 20 years to become mainstream.¹⁹¹ 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.¹⁹²

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).¹⁹³

VI. Uncertain Regulatory Status

As mentioned previously, the World Federation of Exchanges lamented the lack of regulatory clarity on blockchain technology. This opinion is echoed widely,¹⁹⁴ and is supported by the various uncertainties discussed in the previous section.

VII. Energy Consumption

Some have also drawn attention to the substantial energy consumption by blockchain networks, because of the computationally intensive process of mining/verification.¹⁹⁵

189. *Id.*

190. <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-for-blockchain-going-mainstream-2016-8>; http://www.clydeco.com/uploads/Files/CCo10565_Blockchain_brochure_10-06-16_LOW-RES.PDF (last visited October 3, 2016)

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

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

193. *Also see id.*; <http://www.businessinsider.com/credit-suisse-on-the-challenges-for-blockchain-going-mainstream-2016-8>. (last visited October 3, 2016)

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

195. *Id.*

7. Conclusion

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. However, we would not recommend hasty regulation of this technology, since it is complex and calls for time and effort to be put into understanding its implications. 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 would hence be ideal. In this connection, the working groups consisting of industry and government representatives in India; the multi-stakeholder coalitions worldwide to protect blockchain innovation and develop standards; and the development of regulatory sandboxes are good first steps.

About NDA

Nishith Desai Associates (NDA) is a research-based international law firm with offices in Mumbai, Bangalore, Palo Alto (Silicon Valley), Singapore, New Delhi, Munich and New York. We provide strategic legal, regulatory, and tax advice coupled with industry expertise in an integrated manner.

As a firm of specialists, we work with select clients in select verticals. We are invariably involved in highly complex and innovative assignments. We specialize in cross-border work in a variety of practice areas, including Intellectual Property and Technology, International Tax, Fund Formation, Corporate & M&A, Private Equity & Venture Capital, International Litigation and Dispute Resolution, Employment and HR, and Private Clients. Our industry expertise spans Automotive, Funds, Financial Services, IT and Telecom, Pharma and Healthcare, Media and Entertainment, Real Estate, Infrastructure, Social Sector, and Education. Our key clientele comprise marquee Fortune 500 corporations.

Our role includes innovation and strategic advice in futuristic areas of law including those relating to the blockchain, Bitcoin, and fintech; Driverless Cars; Drones; Artificial Intelligence and Robotics; Internet of Things (IoT); Virtual Reality; Med-Tech; Ed-Tech; Direct Democracy; and the Privatization of Outer Space.

Our firm has received acclaim for its achievements and prowess, through the years:

- NDA was ranked the '**Most Innovative Asia Pacific Law Firm in 2016**' by the Financial Times - RSG Consulting Group in its prestigious FT Innovative Lawyers Asia-Pacific 2016 Awards. With a highest-ever total score in these awards, the firm also won Asia Pacific's best 'Innovation in Finance Law', and topped the rankings for the 'Business of Law'. While this recognition marks NDA's ingress as an innovator among the globe's best law firms, NDA has previously won the Financial Times - RSG award for 'Most Innovative Indian Law Firm' for two consecutive years in 2014 and 2015.
- **Chambers and Partners** has ranked us #1 for Technology, Media & Telecom (TMT), Tax and Employment (2016, and 2015).
- **Legal 500** has ranked us in band 1 for Investment Funds, Tax and TMT (2011- 2016).
- **IDEX Legal Awards:** In 2015, NDA 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". IDEX Legal recognized Nishith Desai as the Managing Partner of the Year in 2014.
- **Merger Market** has recognized NDA as the fastest growing M&A law firm in India for the year 2015.
- **World Tax 2015** (International Tax Review Directory) recognized NDA as a Recommended Tax Firm in India
- **International Financial Law Review** (a Euromoney publication) in its IFLR1000 has placed NDA in Tier 1 for Private Equity (2014).
- **India Business Law Journal (IBLJ)** has awarded NDA for Private Equity, Structured Finance & Securitization, TMT, and Taxation in 2015 & 2014; for Employment Law in 2015.

We believe strongly in constant knowledge expansion and have developed dynamic Knowledge Management ('KM') and Continuing Education ('CE') programs, conducted both in-house and for select invitees. KM and CE programs cover key events and global and national trends as they unfold, examine case studies, and debate and analyze emerging legal, regulatory and tax issues, serving as an effective forum for the cross-pollination of ideas. Our trust-based, non-hierarchical, democratically managed organization that leverages research and knowledge

to deliver premium services, high value, and a unique employer proposition has been developed into a global case study and published by John Wiley & Sons, USA in a feature titled 'Management by Trust in a Democratic Enterprise: A Law Firm Shapes Organizational Behavior to Create Competitive Advantage' in the September 2009 issue of Global Business and Organizational Excellence (GBOE).

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

Disclaimer

This report is a copyright of Nishith Desai Associates. No reader should act on the basis of any statement contained herein without seeking professional advice. The authors and the firm expressly disclaim all and any liability to any person who has read this report, or otherwise, in connection with their reliance upon the contents of this report.

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

	The Indian Aviation Sector		Tax Issues in M&A Transactions		Doing Israel - India Business
	August 2016		August 2016		August 2016
	EdTech: From IT to AI		International Commercial Arbitration		Fund Structuring and Operations
	July 2016		July 2016		July 2016
	Preparing For a Driverless Future		Start - Ups: What You Need To Know		Doing Business in India
	June 2016		June 2016		June 2016

NDA Insights

TITLE	TYPE	DATE
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
Pharma Patent Case Study	IP Lab	March 2012
Patni plays to iGate’s tunes	M&A Lab	January 2012
Vedanta Acquires Control Over Cairn India	M&A Lab	January 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.

Research has offered us the way to create thought leadership in various areas of law and public policy. Through research, we discover new thinking, approaches, skills, reflections on jurisprudence, and ultimately deliver superior value to our clients.

Over the years, we have produced some outstanding research papers, reports and articles. Almost on a daily basis, we analyze and offer our perspective on latest legal developments through our "Hotlines". 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 *NDA Insights* 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 papers and disseminate them through our website. Although we invest heavily in terms of associates' 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.

Our research has also contributed to public policy discourse, helped state and central governments in drafting statutes, and provided regulators with a much needed comparative base for rule making. Our *ThinkTank* discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged.

As we continue to grow through our research-based approach, we are now in the second phase of establishing a 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. The center will become the hub for research activities involving our own associates as well as legal and tax researchers from world over. It will also provide the platform to internationally renowned professionals to share their expertise and experience with our associates and select clients.

We would love to hear from you about any suggestions you may have 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 S California Ave., Suite 201
Palo Alto, California 94306, 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 6550 9856

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