Designing a Governance Framework for Blockchain Applications

Working Paper | November 2022

V | D H | Centre for Legal Policy

This report is an independent, non-commissioned piece of work by the Vidhi Centre for Legal Policy, an independent think-tank doing legal research to help make better laws.

About the Authors

Swarna Sengupta is a Research Fellow (Fintech) at the Vidhi Centre for Legal Policy.

Shehnaz Ahmed is a Senior Resident Fellow and Lead (Fintech) at the Vidhi Centre for Legal Policy.

Acknowledgements

The authors are grateful to Vipul Jain, Partner, AZB & Partners, Nikita Chawla, Counsel, AZB & Partners and Jai Vipra, Senior Resident Fellow at the Vidhi Centre for Legal Policy, for their comments and insights on an earlier draft of the report.

The authors are also thankful to Vidhi intern Vineet Sunil Jadhav for his research assistance on specific issues during his engagement with Vidhi.

Errors (if any) rest with the authors.

For any queries and clarifications regarding this Working Paper, please contact
shehnaz.ahmed@vidhilegalpolicy.in

Table of Contents

I. Setting the Context

In recent years, decentralised technologies like blockchain have taken the center stage both within India and globally. Such technologies enable sharing of ledgers for recording transactions or information without the need for reliance on a centralised entity for trust and instead seeks to introduce trust in transactions cryptographically. This enables blockchain to offer new services and revamp the existing legacy systems for recording information and transactions. The Government and private sector are, therefore, exploring the innovation potential of blockchain to create new structures of economic, social, and public interactions. It is predicted that by 2025, blockchain would account for 10% of the global gross domestic product.[1] It is estimated that by 2030 blockchain will be used as a foundational technology for 30% of the global customer base and blockchain will add a business value of over $176 million by 2025 and over $3 trillion by 2030.[2]

In India, both Government agencies and the private sector are taking proactive steps to support the use of blockchain technologies. In December 2021, the Ministry of Electronics and Information Technology ("**MeitY**") released the "National Strategy on Blockchain" setting out a national roadmap for the implementation of blockchain use cases in India.[3] It identified sectors such as real estate, trade financing, insurance, healthcare, and supply chain management, where blockchain could have potential use cases. State governments of Andhra Pradesh[4] and Maharashtra[5] are also exploring specific blockchain use cases. Telangana[6] and Tamil Nadu[7] have also published blockchain policies which can guide blockchain use in the state. Globally as well, government agencies are testing blockchain use cases in various sectors. As of March 2018,[8] 46 countries were exploring 200 blockchain-related initiatives. This number has increased manifold in recent years.

While the existing literature on blockchain focuses on identifying potential use cases of blockchain, it is silent on whether existing laws and policies are well-equipped to respond to these developments. Policymakers across the globe (including MeitY and state governments in India) experimenting with blockchain also acknowledge that to ensure scalability and sustainability of blockchain systems, assessing the legal implications of blockchain and thereafter framing a comprehensive framework to guide its use, is essential. This working paper ("**Working Paper**") seeks to examine the key legal issues for implementing blockchain based solutions and identify core foundational principles which should guide the use and implementation of blockchain. On this basis, it presents the contours of a governance framework that parties (both for public and private sector use cases) looking to join or implement blockchain networks can adopt so that it is legally sustainable in the long term.

[1] World Economic Forum, 'Building Block(chain)s for a Better Planet' (*Fourth Industrial Revolution for the Earth Series,* September 2018) <www3.weforum.org/docs/WEF_Building-Blockchains.pdf> accessed 15 September 2022.

[2] MeitY, 'National Strategy on Blockchain: Towards Enabling Trusted Digital Platforms' (December 2021) <https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf > accessed 15 September 2022; Gartner Research, 'Forecast: Blockchain Business Value, Worldwide, 2017-2030' (March 2017) <https://www.gartner.com/en/documents/3627117> accessed 22 September 2022.

[3] MeitY, 'National Strategy on Blockchain: Towards Enabling Trusted Digital Platforms' (December 2021) <https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf > accessed 15 September 2022.

[4] The Andhra Pradesh Government is testing blockchain use to record land transactions. The Hindu Business Line, 'In AP Capital, Blockchain Technology Secures Land Records' (Hyderabad, 8 January 2018) <https://www.thehindubusinessline.com/info-tech/in-ap-capital-blockchain-technology-secures-land-records/article10020465.ece> accessed 15 September 2022.

[5] The Maharashtra Government is testing blockchain use to verify caste certificates. Mehab Qureshi, 'Maharashtra to use Polygon Blockchain to Issue Verifiable Caste Certificates' *Indian Express* (Pune, 31 March 2022) <https://indianexpress.com/article/technology/crypto/how-maharashtra-is-using-polygon-blockchain-to-issue-verifiable-caste-certificates-7843949/> accessed 15 September 2022.

[6] Information Technology, Electronics and Communications Department , 'Blockchain Policy' (*Government of Telangana,* 17 May 2019) < https://it.telangana.gov.in/wp-content/uploads/2019/05/Telangana-Blockchain-Policy-Draft-May-2019.pdf> accessed 15 September 2022.

[7] Commissionerate of e-Governance and Tamil Nadu e-Governance Agency, 'Tamil Nadu Blockchain Policy 2020' (*Information Technology Department, Government of Tamil Nadu*, 2020) <https://tnesevai.tn.gov.in/CSCfiles/Downloads/PDF/Blockchan_Policy_TamilNadu.pdf> accessed 15 September 2022.

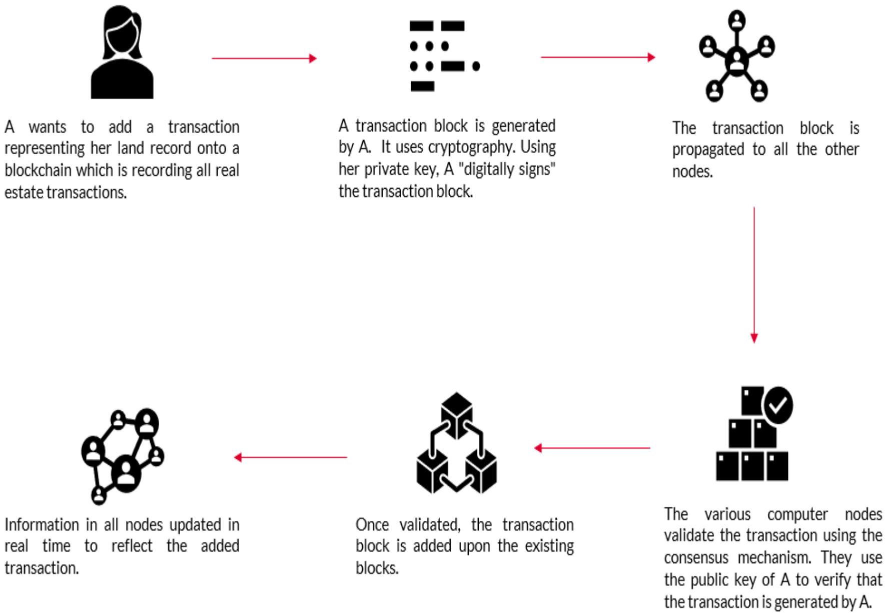
[8] Jamie Berryhill and others, 'Blockchains Unchained: Blockchain Technology and its Use in the Public Sector' (2018) Organisation for Economic Co-operation and Development Working Papers on Public Governance No.28 <https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf?expires=1663230968&id=id&accname=guest&checksum=EDD2B6D6CBFD52A4AC569DC4A87176A7> accessed 15 September 2022.

II. Conceptual Framework

Understanding the Technology

Blockchain technology is a type of distributed ledger technology ("**DLT**"). The Bank for International Settlements ("**BIS**") defines DLT as "processes and related technologies that enable nodes (i.e., computers participating on a network) in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's node".[9] DLT makes use of independent computers in a decentralised manner to record information in a ledger.[10] While "DLT" and "blockchain" are often used interchangeably, blockchain is a specific way of structuring data on a DLT platform i.e., by way of blocks.[11] BIS has defined blockchain as "a distributed ledger that is updated in groups of transactions called blocks. Blocks are then chained sequentially via the use of cryptography to form the blockchain."[12] While this Working Paper is cognisant of the technical difference between DLT and blockchain, however, for its analysis, the paper's focus is on the broad spectrum of decentralised technologies. Hence, any reference to blockchain herein may be construed as a reference to decentralised technologies in general, including DLT.

How Does Blockchain Work?



A wants to add a transaction representing her land record onto a blockchain which is recording all real estate transactions.

A transaction block is generated by A. It uses cryptography. Using her private key, A "digitally signs" the transaction block.

The transaction block is propagated to all the other nodes.

The various computer nodes validate the transaction using the consensus mechanism. They use the public key of A to verify that the transaction is generated by A.

Once validated, the transaction block is added upon the existing blocks.

Information in all nodes updated in real time to reflect the added transaction.

Figure 1: Recording a transaction on a blockchain – Process Flow

Blockchain works over a peer-to-peer network of nodes. Each node has a private key and public key. The public key of a participant is akin to a public address which is visible to the entire network. A private key is specific to an individual node and only known to them.[13] A node can initiate a new transaction record to be added onto the ledger.[14] Such an initiating node creates a new "block" which consists of the transaction record.[15] Thereafter, it uses its private key to digitally sign and encrypt

[9] Committee on Payments and Market Infrastructure, BIS, 'Distributed Ledger Technology in Payment, Clearing and Settlement' (2017) <https://www.bis.org/cpmi/publ/d157.pdf> accessed 15 September 2022.

[10] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

[11] Parma Bains, 'Blockchain Consensus Mechanisms : A Primer for Supervisors' (*International Monetary Fund Fintech Note/2022/003*, January 2022) <https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022003.ashx> accessed 15 September 2022.

[12] BIS, 'Annual Economic Report' (2018), 91 <https://www.bis.org/publ/arpdf/ar2018e5.pdf> accessed 15 September 2022.

[13] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[14] Financial Industry Regulatory Authority, 'Distributed Ledger Technology: Implications of Blockchain for the Securities Industry' (2017) <https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf> accessed 15 September 2022.

[15]Financial Industry Regulatory Authority, 'Distributed Ledger Technology: Implications of Blockchain for the Securities Industry' (2017) <https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf> accessed 15 September 2022.

the transaction block and broadcast it to all the other participating nodes.[16] The other nodes on the network thereafter use the initiating node's public key to verify that the data belongs to such node and collectively validate the block basis a pre-defined consensus mechanism.[17] If the validation is successful, then the block is added onto the blockchain ledger. The blockchain ledger is an append-only ledger wherein data blocks are added to form a chain of such blocks.[18] Existing literature argues that decentralisation i.e., the removal of intermediaries, increases the efficiency of the system by reducing cost and time.[19] Each transaction is time-stamped and validated by participating nodes which increases trust and transparency in the system. In the absence of a centralised point, there is no longer a singular point of failure or compromise, and the risk is distributed.

Key Features of Blockchain

Distributed and Decentralised

Distribution and decentralisation are the hallmarks of blockchain technology. Broadly, blockchain is a ledger or database which stores a list of transactions. However, unlike traditional recordkeeping systems it does not have a centralised authority which is responsible for maintaining/updating the database. The distributed nature of blockchain enables multiple nodes to operate on a peer-to-peer basis to validate and add blocks or data onto the ledger, without relying on a centralised authority.[20] Each transaction or data which is sought to be added by a network participant is sent to all the nodes for their validation. Once such a data block is validated by the nodes, it gets added to the ledger. Such addition is replicated across the network and the copy of the same is reflected in the ledger of all the participants.[21] Therefore, the validation of new entries or data is decentralised to a network of nodes without the reliance on a centralised entity.

Consensus Mechanism

The nodes in a network can validate new blocks of data through a consensus mechanism. Consensus mechanism refers to the set of rules and procedures that are employed throughout the blockchain network to effect any change in the ledger.[22] It is set out in the algorithm of the blockchain and can be of various types with each stipulating varied conditions. Two prominent consensus mechanisms are proof-of-work ("**PoW**") and proof-of stake ("**PoS**"). Blockchain networks which employ PoW, need participants to use computing power to solve

[16] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[17] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[18] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[19] Douglas Miller and others, 'Blockchain: Opportunities for Private Enterprises in Emerging Markets' (*International Finance Corporation World Bank Group,* 2019) <https://documents1.worldbank.org/curated/pt/260121548673898731/pdf/134063-WP-121278-2nd-edition-IFC-EMCompass-Blockchain-Report-PUBLIC.pdf> accessed 15 September 2022; Niti Aayog, 'Blockchain: The India Strategy: Towards Enabling Ease of Business, Ease of Living, and Ease of Governance, Part 1' (2020) <https://static.psa.gov.in/psa-prod/psa_custom_files/Blockchain_The_India_Strategy_Part_I.pdf> accessed 15 September 2022; Bertrand Copigneaux and others, 'Blockchain for Supply Chains and International Trade: Report on Key Features, Impacts and Policy Options' (2020) Panel for the Future of Science and Technology Study <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf> accessed 15 September 2022; Financial Conduct Authority, 'Discussion Paper on Distributed Ledger Technology' (2017) <https://www.fca.org.uk/publication/discussion/dp17-03.pdf> accessed 16 September 2022 ; Monetary Authority of Singapore 'Blockchain/Distributed Ledger Technology (DLT)' <https://www.mas.gov.sg/development/fintech/technologies---blockchain-and-dlt> accessed 15 September 2022.

[20] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[21] HM Treasury, Financial Conduct Authority and Bank of England, 'Cryptoassets Taskforce: Final Report' (2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final > accessed 15 September 2022.

[22] Parma Bains, 'Blockchain Consensus Mechanisms : A Primer for Supervisors' (*International Monetary Fund Fintech Note/2022/003,* January 2022) <https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022003.ashx> accessed 15 September 2022.

complex algorithmic asymmetrical mathematical challenges to add new blocks.[23] On the other hand, in PoS, participants need to stake assets which act as collateral to add and/or validate new additions to the ledger.[24] These consensus mechanisms seek to create trust in a decentralised environment and ensure that any change to the ledger is legitimate.

Cryptography

Each transaction on a blockchain employs a cryptographic hash function to ensure the authenticity of the data.[25] Using a cryptographic hash generates a "digital fingerprint similar to a human fingerprint that cannot be changed unless the data itself is changed."[26] Cryptography enables the transaction record to be time-stamped.[27] It also enables the creation of public and private keys. Thus, the use of cryptography ensures that any modification or tampering of the data on the blockchain is also visible to the participants.

Immutability

Owing to cryptography, the blockchain ledger is immutable i.e., it is difficult to modify any contents of the record stored on the blockchain and the same cannot be done unilaterally.[28] In traditional ledgers, participants can contact the centralised servers to modify the data. However, since blockchain employs a cryptographic distributed consensus, any unilateral modification is generally not feasible unless a significant number of nodes choose to modify a transaction.[29]

Pseudo-anonymity

Generally, the identities of the participants of a blockchain network are pseudo-anonymous. Their account details and transactions are visible to the network, but their real-life identities are not provided. Thus, transactions are linked and traced to account addresses with corresponding public keys instead of usernames and personal details.[30]

Types of blockchain

Blockchain architecture can be designed in different ways based on who can access and/or verify the information on the blockchain. The identification of the type of blockchain hinges on two questions[31]- *first*, who can read or access the information that has been stored on the blockchain; and *second*, who can submit or verify information

[23] Parma Bains, 'Blockchain Consensus Mechanisms : A Primer for Supervisors' (*International Monetary Fund Fintech Note/2022/003*, January 2022) <https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022003.ashx> accessed 15 September 2022.

[24] Parma Bains, 'Blockchain Consensus Mechanisms : A Primer for Supervisors' (*International Monetary Fund Fintech Note/2022/003*, January 2022) <https://www.imf.org/-/media/Files/Publications/FTN063/2022/English/FTNEA2022003.ashx> accessed 15 September 2022.

[25] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[26] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[27] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[28] Organization for Economic Co-operation and Development, 'OECD Blockchain Primer' <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf> accessed 15 September 2022.

[29] Jamie Berryhill and others, 'Blockchains Unchained: Blockchain Technology and its Use in the Public Sector' (2018) Organisation for Economic Co-operation and Development Working Papers on Public Governance No.28 <https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf?expires=1663230968&id=id&accname=guest&checksum=EDD2B6D6CBFD52A4AC569DC4A87176A7> accessed 15 September 2022.

[30] Jamie Berryhill and others, 'Blockchains Unchained: Blockchain Technology and its Use in the Public Sector' (2018) Organisation for Economic Co-operation and Development Working Papers on Public Governance No.28 <https://www.oecd-ilibrary.org/docserver/3c32c429-en.pdf?expires=1663230968&id=id&accname=guest&checksum=EDD2B6D6CBFD52A4AC569DC4A87176A7> accessed 15 September 2022.

[31] Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022.

on the blockchain. Basis the first question, blockchain may be categorised as public or private depending on whether the ledgers can be accessed by anyone or only by the participating nodes in the network.[32] Basis the second question i.e. whether network participants or nodes[33] need permission to make changes to the ledger, blockchain may be classified as permissioned or permissionless systems.[34] However, it has been pointed out that in practice, there is no strict categorisation of public and private or permissioned and permissionless blockchain systems, and the degree of openness, accessibility and decentralisation will determine the nature of blockchain which may take different forms[35] as discussed below.

Public Permissionless Blockchain

These blockchains are primarily hosted on public servers which can be accessed, read, and verified by any of the participants joining the network. Any of them can add or generate transactions onto the ledger of the blockchain.[36] The identities of the participants are mostly pseudo-anonymous or can even be anonymous.[37] It is fully decentralised with no control over the entry or exit of the participants. For example, the Bitcoin blockchain is a public permissionless blockchain wherein participants can join, exit, and re-join without any authorisation.

Public Permissioned Blockchain

While the data on such blockchains can be read by anyone, only a limited number of participants are allowed or authorised to write and submit the entries to the blockchain. [38] For instance, if the government uses a blockchain-based solution for storing information on land records akin to a land registry, the information

Types of Blockchain – Popular Blockchain Use Cases

Bitcoin

Bitcoin (BTC) is one of the most popular cryptoassets which operates on the Bitcoin blockchain platform. The Bitcoin blockchain is a peer-to-peer payment network. It does not involve any third party or central trusted intermediary to facilitate the trading of BTCs. It is a public permissionless blockchain wherein no specific authorisation is required to become a participant and participate in the blockchain network. Users need to download and install a Bitcoin wallet which will generate a Bitcoin address which users can share with each other. It will also enable the generation of private and public keys. Any transaction i.e., any transfer of BTC from one user's wallet to another is sought to be recorded on the Bitcoin blockchain as a new block. The transaction so propagated to the network is validated by way of mining. Mining involves the use of a consensus mechanism to validate and verify transactions which are thereafter added to the blockchain. The Bitcoin blockchain employs the PoW consensus mechanism. Miners validate transaction blocks by solving mathematical problems. As an incentive, miners are rewarded with new BTCs. They also receive the transaction fee paid by such users for mining a block on the blockchain.

Source: Bitcoin Foundation, 'How it works'; Bitcoin Foundation, 'Bitcoin'.

Walmart food tracing blockchain

Walmart in collaboration with IBM, used the Hyperledger Fabric blockchain platform to create a food supply traceability application. It was a private permissioned blockchain. Suppliers providing raw materials to Walmart had to upload different documents onto the blockchain such as supplier details, warehouse and infrastructure details, quality certificates, etc. These were all independent records or blocks on the blockchain. This chain of information as uploaded onto blockchain enabled Walmart to trace within seconds the quality, nature, and the supplier of the produce.

Source: Hyperledger, 'Case Study: How Walmart brought unprecedented transparency to the food supply chain.

[32] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[33] In this Working Paper we use the terms "nodes" and "participants" interchangeably to refer to computer users participating on a network, unless otherwise specified.

[34] Harish Natarajan and others, 'Distributed Ledger Technology and Blockchain' (2017) World Bank Fintech Note No.1 <https://olc.worldbank.org/system/files/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 15 September 2022.

[35] World Bank Group, 'Distributed Ledger Technology and Secured Transactions Frameworks: A Primer' (2020) Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives- Guidance Note Series < https://openknowledge.worldbank.org/bitstream/handle/10986/34009/Distributed-Ledger-Technology-and-Secured-Transactions-Framework.pdf?sequence=4&isAllowed=y> accessed 15 September 2022; Organization for Economic Co-operation and Development, 'OECD Blockchain Primer' <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf> accessed 15 September 2022.

[36] Organization for Economic Co-operation and Development, 'OECD Blockchain Primer' <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf> accessed 15 September 2022.

[37] Douglas Miller and others, 'Blockchain: Opportunities for Private Enterprises in Emerging Markets' (*International Finance Corporation World Bank Group,* 2019) <https://documents1.worldbank.org/curated/pt/260121548673898731/pdf/134063-WP-121278-2nd-edition-IFC-EMCompass-Blockchain-Report-PUBLIC.pdf> accessed 15 September 2022

[38] World Bank, 'Distributed Ledger Technology and Secured Transactions: Note 3. Distributed Ledger Technology and Secured Transactions Framework' (2020) < https://openknowledge.worldbank.org/bitstream/handle/10986/34009/Distributed-Ledger-Technology-and-Secured-Transactions-Framework.pdf?sequence=4&isAllowed=y> accessed 18 October 2022; Marcos Allende, 'LaCChain Framework for Permissioned Public Blocckhain Networks: From Blockchain Technology to Blockchain Networks' (2021) <https://publications.iadb.org/publications/english/document/LACChain-Framework-for-Permissioned-Public-Blockchain-Networks-From-Blockchain-Technology-to-Blockchain-Networks.pdf> accessed 15 September 2022.

regarding each entry may be accessible and can be viewed by any participants. However, any new entry can only be made by a select group of participants authorised to make or validate records. This may include entities such as the Registrar of a district or authorised personnel of that office.

Private Permissionless Blockchain

In this type of blockchain only those authorised can access the blockchain. All of these authorised participants can thereafter read, add or contribute to the data of the blockchain. [39] For instance, LTO network is a type of private permissionless blockchain wherein authorised nodes are given read and write privileges.[40].

Private Permissioned Blockchain

This is the most restricted type of blockchain. Here, within the authorised participants as well, only few nodes can read or submit and verify information on the blockchain.[41] There is a high level of visibility and tight control and supervision over the participants and the nature of their participation. For instance, a company deploying an internal blockchain for recording personnel data can have a few officers at the top-level management, who can view or access the data but only a particular manager or officer can make changes or additions to the information stored.

Key Participants

Identifying the key participants within the blockchain ecosystem is crucial to map their roles and determine their respective rights and duties. This is important in designing the governance framework. For this purpose, the Working Paper relies on a broad categorisation of the participants delineated in the existing literature.[42] In some cases, one entity can perform the various roles delineated below.

Developer

The blockchain developer develops/writes the code that builds the blockchain and the associated decentralised systems. They are responsible for developing and maintaining the core protocol and the interface for the blockchain application to work on.[43] Similar to a software developer, the blockchain developer will also be responsible to provide updates and fix any vulnerabilities in the code.

Administrator / Network Operator

The blockchain administrator is the operator and controller of the blockchain network. The blockchain administrator sets the rules and enforces compliance with the rules of the blockchain ledger.[44] The role and eligibility of a blockchain administrator may differ depending on the type of blockchain. In a permissionless blockchain, the blockchain administrator is involved in proposing changes to the network and ensuring the functioning of the blockchain application.[45] In a permissioned blockchain, the blockchain administrator will also

[39] World Bank, 'Distributed Ledger Technology and Secured Transactions: Note 3. Distributed Ledger Technology and Secured Transactions Framework' (2020) < https://openknowledge.worldbank.org/bitstream/handle/10986/34009/Distributed-Ledger-Technology-and-Secured-Transactions-Framework.pdf?sequence=4&isAllowed=y> accessed 18 October 2022.

[40] Binance Research, 'LTO Network' (February 2020) < https://research.binance.com/en/projects/lto-network> accessed 18 October 2022.

[41]World Bank, 'Distributed Ledger Technology and Secured Transactions: Note 3. Distributed Ledger Technology and Secured Transactions Framework' (2020) < https://openknowledge.worldbank.org/bitstream/handle/10986/34009/Distributed-Ledger-Technology-and-Secured-Transactions-Framework.pdf?sequence=4&isAllowed=y> accessed 18 October 2022. ;

[42]Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022; World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

[43] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

[44]Prof. Dr. Robby Houben, Alexander Snyers, 'Cryptocurrencies and Blocckhain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (2018) European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance Study <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> accessed 15 September 2022.

[45] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

have control over who can join or participate in the blockchain network.[46] In a permissioned blockchain, a specific individual or consortium of persons may act as blockchain administrators.[47] In public or permissionless blockchain, there is no specific identified group, and it could be the case that certain developers volunteer to act as blockchain administrators.[48]

Users

Blockchain networks consist of different users who interact with the blockchain network and each other to contribute and use the blockchain application.[49] Different participants may have different rights and varying levels of access to the blockchain platform depending on the specific blockchain arrangement. The Cambridge Centre for Alternative Finance recognises certain categories of such users, for instance auditors[50], miners[51], and end-users,[52] as participants in a blockchain network.[53]

External Gateways

Gateways are the interface between the end-users and the blockchain application through which the end-users access the blockchain network. They are generally the external application through which users interact to gain access to the core blockchain platform.[54] These can include the platforms, custodian wallets or the exchanges through which the participants access the blockchain network.[55]

Smart Contracts

Some blockchains deploy smart contracts as part of their functioning. Smart contracts are computer programs used to express contractual obligations, which are automatically performed using computer code on the blockchain network.[56] It can execute certain functions when specific preconditions as prescribed by parties are met.[57] Since there is automatic execution, human intervention, or the presence of trusted third parties to execute the contracts is minimal and limited.[58]Agreements which can be objectively measured and understood by code are the most suitable for execution by smart contracts. For instance, it has been pointed out that sale agreements and agreements whose performance is dependent on defined metrics can be easily executed through a smart

[46] Prof. Dr. Robby Houben, Alexander Snyers, 'Cryptocurrencies and Blocckhain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (2018) European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance Study <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> accessed 15 September 2022.

[47] SStructured Finance Industry Group, Digital Chamber of Commerce, Deloitte' Applying Blockchain in Securitization: Opportunities for Reinvention' (*Deloitte,* 2017) <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-sfig-report-applying-blockchain-in-securitization-opportunities-for-reinvention.pdf > accessed 17 September 2022.

[48] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

[49] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

[50] Auditors are responsible for examining the transactions or records which have been submitted for their validity and propagating the transactions which are valid to the rest of the network. Any invalid transactions are reported by the auditors. The auditors also have access to the system to conduct an independent audit of the same.

[51] Miners are nodes who are responsible for producing and submitting records for their possible inclusion onto the ledger.

[52] End-users are participants who interact with the blockchain network indirectly through a gateway.

[53] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

[54] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

[55] Michel Rauchs and others, 'Distributed Ledger Technology Systems: A Conceptual Framework' (*Cambridge Centre for Alternative Finance*, August 2018) <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf> accessed 15 September 2022.

[56]Stuart D. Levi, Alex B. Lipton, 'An Introduction to Smart Contracts and their Potential and Inherent Limitations' (*Harvard Law School Forum on Corporate Governance,* 26 May 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 15 September 2022.

[57] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf > accessed 15 September 2022.

[58] Dirk A. Zetzsche and others, 'DLT-Based Enhancement of Cross-Border Payment Efficiency- a Legal and Regulatory Perspective' (2022) BIS Working Papers No. 1015 <https://www.bis.org/publ/work1015.pdf > accessed 15 September 2022.

contract.[59] For instance, A agrees to buy B's property subject to the condition that B installs a gate at the entryway of the property and builds a fence around the land. B agrees to sell her property to A on receipt of payment which will be done once B has satisfied the above conditions. These promises can be encoded onto the blockchain containing the smart contract. A can transfer the agreed consideration to an escrow account which is linked with the smart contract. Once B satisfies the conditions stipulated above and it is marked as complete on the smart contract, the smart contract will operate to automatically release the funds from the escrow account to B's account.

[59] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf > accessed 15 September 2022.

III. Use Cases of Blockchain

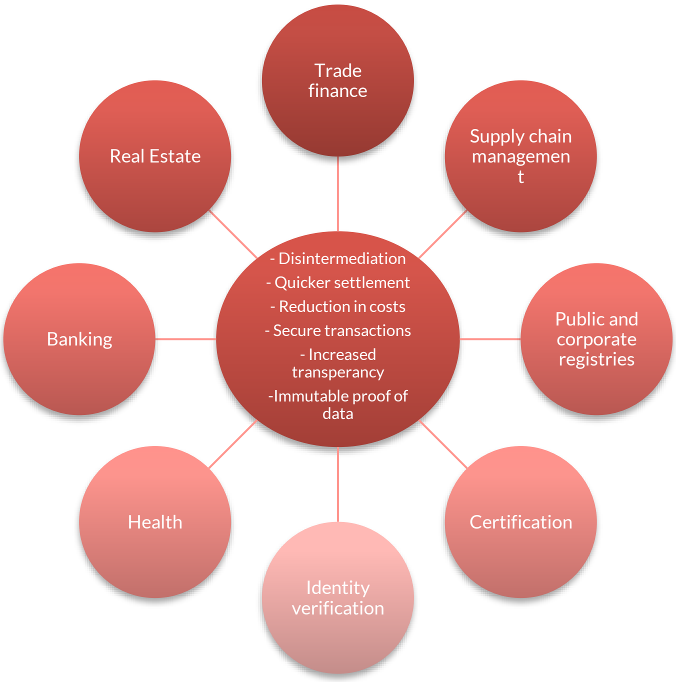


Figure 2: Benefits of blockchain technology and potential use cases

While blockchain technology use cases emanated from the financial sector, the discussion and application of this technology are rapidly expanding to other industries and the public sector. Globally, both the Government and the private sector are exploring multiple use cases of this technology and its associated opportunities and risks. This section sets out some key use cases of blockchain. A review of these use cases indicates that the application of this technology has spread across several industries. These include applications in trade financing, real estate, healthcare, supply chain management, banking, insurance, legal and even in governance.[60] However, most of these use cases are either still in their Proof-of-Concept ("**PoC**") phase or the use cases which have been deployed at a larger scale are mostly in the nature of information management systems. Issues such as the disruptive characteristics of blockchain and the high initial cost of implementation[61] have made it challenging for blockchain use cases to be scaled at a larger level.

Use Case 1: Trade Financing Documentations

Issue: *Currently, there are multiple documentation requirements spread across several parties, making the entire process cumbersome and time-consuming. Further, operational risks emanate since information can be manipulated or documents can be lost leading to disputes. There is also low interoperability of platforms with such documents making it difficult for multiple actors to access the information leading to rising compliance costs.*[62]

Value proposition of blockchain: *Blockchain can digitise these trade documents and provide a robust network for verifying and accessing such data. The blockchain will be a shared ledger for storing transactional documents and history which can be accessed by all the stakeholders in the chain. This will help in improving transparency, traceability, and interoperability.*[63] *This will lead to a decrease in compliance and operational costs. It will also provide secure transaction history for all parties involved.*[64]

Case Study: *In India, a leading private sector bank has developed its own blockchain solution. It provides cross-border open account trade finance and remittance services on the blockchain.*[65] *The 15 physical documents crucial to trade finance are digitised and uploaded on the*

[60] MeitY, 'National Strategy on Blockchain: Towards Enabling Trusted Digital Platforms' (December 2021) <https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf > accessed 15 September 2022.

[61] Niti Aayog, 'Blockchain: The India Strategy: Towards Enabling Ease of Business, Ease of Living, and Ease of Governance, Part 1' (2020) <https://static.psa.gov.in/psa-prod/psa_custom_files/Blockchain_The_India_Strategy_Part_I.pdf> accessed 15 September 2022

[62] Deloitte, 'How Blockchain Can Reshape Trade Finance' <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/grid/trade-finance-placemat.pdf> accessed 15 September 2022.

[63] Shuchih Ernest Chang and others, 'Blockchain-Enabled Trade Finance Innovation: A Potential Paradigm Shift on Using Letter of Credit' (2019) 12(1) Sustainability MDPI < https://ideas.repec.org/a/gam/jsusta/v12y2019i1p188-d301819.html> accessed 15 September 2022.

[64] Deepesh Patel and Emmanuelle Ganne, 'Blockchain and DLT in Trade: Where do we Stand?' (2020) <https://www.wto.org/english/res_e/booksp_e/blockchainanddlt_e.pdf> accessed 15 September 2022.

[65] ICICI Bank, 'ICICI Bank On-boards over 250 Corporates on its Blockchain Platform for Trade Finance' (*ICICI Bank Press Release*, 17 April 2018) <https://www.icicibank.com/managed-assets/docs/about-us/2018/blockchain-platform-for-trade-finance.pdf> accessed on 15 September 2022.

blockchain. This enables the participants to access a single verifiable and auditable source for all documents and information thereby reducing the reliance on intermediaries and costs. This data can be viewed and accessed in real-time across the world. The blockchain solution also allows the participants to track the documents and verify ownership of assets to execute digital trade finance contracts with ease and confidence.[66] *There are also platforms such as eCom Asia, DLT Ledgers and CargoX which provide data integration for all supply chain participants on a blockchain network.*

Use Case 2: Indian Public Distribution System

Issue: *The Indian Public Distribution System (“**PDS**”) has multiple process stages such as identification of beneficiary, procurement, storage, distribution, transportation, etc.*[67] *Some common challenges facing the PDS ecosystem include inaccurate or incomplete information, faulty beneficiary identification, leakage of food grains, issuance of ghost or duplicate ration cards and the lack of a monitoring system.*[68] *There is no mechanism for accountability across the supply chain.*[69]

Value proposition of blockchain: *A blockchain ledger can theoretically digitise the information regarding each beneficiary such that no registered beneficiaries are missed out.*[70]

Project example: *A PoC is being tested by the Centre for Excellence in Blockchain Technology in India to make the entire PDS ecosystem more efficient. They are exploring the use of blockchain to expedite payment to farmers once they have handed over their produce to the miller instead of having to wait for the entire PDS supply process to get over.*[71] *Blockchain however, is predominantly being proposed within the framework to streamline the supply chain wherein the food grain so procured is tracked on a blockchain and the transactions across different parties are time-stamped and recorded in the ledger such that real-time monitoring is possible and the requisite amount of food grains reaches the beneficiaries.*[72]

Use case 3: Public Registries

Issue: *Public registries such as land registries, shareholder registries, revenue registries, and Know-Your-Customer (“**KYC**”) registries are deployed to record crucial information. The registries also facilitate realisation of certain rights by persons. Most registries are stored on traditional computer software or on paper. In such cases, there is a high chance of recording inaccurate information or non-recording information. Therefore, information in such registries is not updated leading to persons losing out on rights or entitlements. Centralised databases where such registries are maintained have one point of failure and are more susceptible to manipulation leading to loss of data.*

Value proposition of blockchain: *Blockchain technology is in its core a ledger for record-keeping and information. Hence, utilising blockchains for maintaining such registries is one of the primary use cases for this innovative technology. There have been pilot projects for using blockchain to record land registration and ownership rights.*[73] *Blockchain registries offer immutable proof of data. The transactions are time-stamped and can be verified and authenticated by the network participants. It provides a single point of access for data. Since in blockchain all historical data is available it would create a robust and immutable source of authentication for registries which are maintained to prove rights of persons.*

[66] ICICI Bank, ‘ICICI Bank On-boards over 250 Corporates on its Blockchain Platform for Trade Finance’ (*ICICI Bank Press Release*, 17 April 2018) <https://www.icicibank.com/managed-assets/docs/about-us/2018/blockchain-platform-for-trade-finance.pdf> accessed on 15 September 2022.

[67] Sandeep Kumar Singh and others, ‘A Conceptual Model for Indian Public Distribution System Using Consortium Blockchain with On-Chain and Off-Chain Trusted Data’ (2021) 27(3) Information Technology for Development <https://www.tandfonline.com/doi/abs/10.1080/02681102.2020.1847024?journalCode=titd20> accessed 15 September 2022.

[68] Sandeep Kumar Singh and others, ‘A Conceptual Model for Indian Public Distribution System Using Consortium Blockchain with On-Chain and Off-Chain Trusted Data’ (2021) 27(3) Information Technology for Development <https://www.tandfonline.com/doi/abs/10.1080/02681102.2020.1847024?journalCode=titd20> accessed 15 September 2022.

[69] Centre of Excellence in Blockchain Technology, ‘Public Distribution System’ <https://blockchain.gov.in/pdspage.html> accessed 15 September 2022.

[70] Himani Mishra, Prateek Maheshwari, ‘Blockchain in Indian Public Distribution System: A Conceptual Framework to Prevent Leakage of the Supplies and its Enablers and Disablers’ (2021) 14(2) Journal of Global Operations and Strategic Sourcing <https://www.researchgate.net/publication/352223958_Blockchain_in_Indian_Public_Distribution_System_a_conceptual_framework_to_prevent_leakage_of_the_supplies_and_its_enablers_and_disablers> accessed 15 September 2022.

[71] Centre of Excellence in Blockchain Technology, ‘Public Distribution System’ <https://blockchain.gov.in/pdspage.html> accessed 15 September 2022.

[72] Centre of Excellence in Blockchain Technology, ‘Public Distribution System’ <https://blockchain.gov.in/pdspage.html> accessed 15 September 2022.

[73] Yunus Y. Lasania, ‘Telangana Government to Use Blockchain Tech for Securing Land Records’ *Livemint* (Hyderabad, 20 October 2017) <https://www.livemint.com/Politics/4IOMVhyOuK6k0LwSVGikZL/Telangana-govt-to-use-blockchain-tech-for-securing-land-reco.html ; https://www.undp.org/blog/using-blockchain-make-land-registry-more-reliable-india> accessed 15 September 2022.

Project examples: *The Andhra Pradesh*[74] *and Telangana*[75] *governments are seeking to upload land records on the blockchain to ensure they are secure and tamper resistant. The blockchain will record the ownership details, any change in ownership, details regarding encumbrances and provide the full history and status of the properties situated in these two States.*

*Further, the Securities and Exchange Board of India ("****SEBI****") is also exploring blockchain use cases to streamline shareholder records. SEBI has developed the Security and Covenant Monitoring System platform ("****System****") which is being hosted by Depositories to monitor securities, asset covers and covenants of non-convertible securities.*[76] *The System will use blockchain technology to record creation of securities, credit ratings of non-convertible securities and charges on the same. The information can be updated by entities such as Issuers, Debenture-Trustees, Credit Rating Agencies etc. It will be a permissioned blockchain wherein concerned stakeholders such as exchanges, depository institutions can access and view specific portions of information. All the data uploaded on the blockchain will be time-stamped, encrypted, cryptographically signed, and sequentially added so that they can be verified easily.*

Use 4: Corporate Governance

Issue: *The two most prominent areas of corporate governance where blockchain applications have been analysed are in maintenance of shareholder registries and shareholder voting. Shareholder voting is riddled with inefficiencies in many countries. There are various costs attached to the voting process such as the cost of attending physical meetings, compliance costs of appointing proxies and getting information,*[77] *and providing detailed information of meetings and in disbursing notices.*[78] *Additionally, when voting through a proxy there is no way for shareholders to verify whether the vote has been cast and what is the vote that has been cast.*[79]

Value proposition of blockchain: *Blockchain can be used to store all corporate information in an immutable ledger which can be accessed by shareholders directly. It will provide an immutable proof of ownership which can also afford real time monitoring by the board and the regulators.*[80] *Blockchain can also be applied to facilitate virtual meetings and shareholder voting therein. It can be used to record the time and date of the meeting. Documents required for the meeting can be uploaded on the blockchain which the shareholders can directly access.*[81] *Blockchains can be developed to follow a set of rules and use smart contracts to implement any terms of voting stipulated in the Articles of the Company or in shareholder agreements.*[82] *Blockchains may also be used to implement authentication protocols as well as mechanisms for shareholders to allocate proxies.*[83] *Owing to the inherent nature of blockchain, the shareholders after a meeting can access the blockchain and verify the manner in which the proxy had casted the vote.*[84]

[74] The Hindu Business Line, 'In AP Capital, Blockchain Technology Secures Land Records' (Hyderabad, 8 January 2018) <https://www.thehindubusinessline.com/info-tech/in-ap-capital-blockchain-technology-secures-land-records/article10020465.ece> accessed 15 September 2022.

[75] Telangana Blockchain District, 'Land Records (Dharani & CDAC)' <https://blockchaindistrict.telangana.gov.in/> accessed 15 September 2022.

[76] SEBI, 'Security and Covenant Monitoring' using Distributed Ledger Technology' (2021) <https://www.sebi.gov.in/media/press-releases/aug-2021/sebi-issues-circular-on-security-and-covenant-monitoring-using-distributed-ledger-technology-_52086.html> accessed 15 September 2022.

[77] Anne Lafarre and Christoph Van der Elst. 'Blockchain Technology for Corporate Governance and Shareholder Activism' (2018) Tilburg Law School Legal Studies Research Paper Series No. 07/2018 <https://www.researchgate.net/profile/Anne-Lafarre/publication/324670400_Blockchain_Technology_for_Corporate_Governance_and_Shareholder_Activism/links/5b349a0ca6fdcc8506d73db4/Blockchain-Technology-for-Corporate-Governance-and-Shareholder-Activism.pdf> accessed on 15 September 2022.

[78] Anne Lafarre and Christoph Van der Elst. 'Blockchain Technology for Corporate Governance and Shareholder Activism' (2018) Tilburg Law School Legal Studies Research Paper Series No. 07/2018 <https://www.researchgate.net/profile/Anne-Lafarre/publication/324670400_Blockchain_Technology_for_Corporate_Governance_and_Shareholder_Activism/links/5b349a0ca6fdcc8506d73db4/Blockchain-Technology-for-Corporate-Governance-and-Shareholder-Activism.pdf> accessed on 15 September 2022.

[79] Anne Lafarre and Christoph Van der Elst. 'Blockchain Technology for Corporate Governance and Shareholder Activism' (2018) Tilburg Law School Legal Studies Research Paper Series No. 07/2018 <https://www.researchgate.net/profile/Anne-Lafarre/publication/324670400_Blockchain_Technology_for_Corporate_Governance_and_Shareholder_Activism/links/5b349a0ca6fdcc8506d73db4/Blockchain-Technology-for-Corporate-Governance-and-Shareholder-Activism.pdf> accessed on 15 September 2022.

[80] Tracy Molino, 'Practical Application of Distributed Ledger Technology: Maintaining Corporate Records on the Blockchain' (*JDSUPRA,* 20 September 2018) <https://www.jdsupra.com/legalnews/practical-application-of-distributed-18294/> accessed 15 September 2022.

[81] Anne Lafarre and Christoph Van der Elst. 'Blockchain Technology for Corporate Governance and Shareholder Activism' (2018) Tilburg Law School Legal Studies Research Paper Series No. 07/2018 <https://www.researchgate.net/profile/Anne-Lafarre/publication/324670400_Blockchain_Technology_for_Corporate_Governance_and_Shareholder_Activism/links/5b349a0ca6fdcc8506d73db4/Blockchain-Technology-for-Corporate-Governance-and-Shareholder-Activism.pdf> accessed on 15 September 2022.

[82] Anne Lafarre and Christoph Van der Elst. 'Blockchain Technology for Corporate Governance and Shareholder Activism' (2018) Tilburg Law School Legal Studies Research Paper Series No. 07/2018 <https://www.researchgate.net/profile/Anne-Lafarre/publication/324670400_Blockchain_Technology_for_Corporate_Governance_and_Shareholder_Activism/links/5b349a0ca6fdcc8506d73db4/Blockchain-Technology-for-Corporate-Governance-and-Shareholder-Activism.pdf> accessed on 15 September 2022

[83] Anne Lafarre, Christoph Van der Elst. 'Blockchain Technology for Corporate Governance and Shareholder Activism' (2018) Tilburg Law School Legal Studies Research Paper Series No. 07/2018 <https://www.researchgate.net/profile/Anne-Lafarre/publication/324670400_Blockchain_Technology_for_Corporate_Governance_and_Shareholder_Activism/links/5b349a0ca6fdcc8506d73db4/Blockchain-Technology-for-Corporate-Governance-and-Shareholder-Activism.pdf> accessed on 15 September 2022.

[84] Anne Lafarre, Christoph Van der Elst. 'Blockchain Technology for Corporate Governance and Shareholder Activism' (2018) Tilburg Law School Legal Studies Research Paper Series No. 07/2018 <https://www.researchgate.net/profile/Anne-Lafarre/publication/324670400_Blockchain_Technology_for_Corporate_Governance_and_Shareholder_Activism/links/5b349a0ca6fdcc8506d73db4/Blockchain-Technology-for-Corporate-Governance-and-Shareholder-Activism.pdf> accessed on 15 September 2022

Project examples: *The Delaware General Corporation Act ("**Delaware Act**") was amended in 2017 to allow private companies registered under the Delaware Act to use blockchain to record and store company and corporate records such as share registries, books of account and minutes.*[85] *These amendments were carried out in pursuance of the Delaware Blockchain Initiative which seeks to explore the use of blockchain to enhance the regulatory compliance framework for companies so as to reduce their operational and compliance costs, expedite timelines and automate manual processes.*[86]

Various stock exchanges have also been exploring blockchain solutions for voting processes. For instance, NASDAQ has conducted a pilot project and developed a PoC in 2016 to use blockchain applications for facilitating e-voting for companies listed on NASDAQ Tallin. The blockchain technology enabled investors to view relevant information about the meetings, vote at meetings, transfer voting rights to a proxy, monitor the voting procedure of the proxy, and recall any such proxy vote.[87] *These blockchain-based e-voting systems not only allow shareholders to cast vote but also enable the companies to have an immutable record of information pertaining to previous meetings, shareholder voting patterns and transactions.*[88]

[85] Delaware General Corporation Law 2013, s 224.

[86] Delaware Office of the Governor, 'Governor Markell Launches Delaware Blockchain Initiative' *PR Newswire (*Delaware, 2 May 2016) <https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html> accessed 15 September 2022.

[87] Richard DeMarinis, Hedi Uustalu, 'Is Blockchain the Answer to E-voting? Nasdaq Believes So' (*Nasdaq,* 23 January 2017*)* <www.nasdaq.com/articles/blockchain-answer-e-voting-nasdaq-believes-so-2017-01-23> accessed 15 September 2022.

[88] Richard DeMarinis, Hedi Uustalu, 'Is Blockchain the Answer to E-voting? Nasdaq Believes So' (*Nasdaq,* 23 January 2017*)* <www.nasdaq.com/articles/blockchain-answer-e-voting-nasdaq-believes-so-2017-01-23> accessed 15 September 2022.

IV. Key Legal Issues

Privacy and Data Protection

Most privacy and data protection laws focus on traditional centralised databases, where an entity or entities determine the purpose and means of processing and actually processes the data. The emergence of decentralised technologies such as blockchain technologies challenges existing data protection laws and its traditional notion of "centralised controller-based data processing".[89] The following is a discussion of such legal issues raised by blockchain technologies in the context of privacy and data protection laws.

Identification of Controller and Processor

Most data protection regimes are constructed with a view that data management is carried out by certain specific central authorities. Therefore, most data protection laws focus on identifying such central authorities who are in control of or process personal data. For instance, the European Union ("**EU**") General Data Protection Regulation 2018 ("**GDPR**") distinguishes between "controller" and "processor". A controller is defined to refer to any legal person, public authority or any other body which alone or jointly with others, is in charge of stipulating the purpose and means of processing personal data.[90] On the other hand, a processor refers to any person or entity which is responsible for processing the personal data on behalf of the controller.[91] Identification of the controller and the processor is crucial to apportion duties on them. The identification of the controller and processor is also important to establish against whom data subjects (i.e. a natural person whose personal data is being processed by the controller and processor) or the users can claim their rights.[92] In India, the Personal Data Protection Bill, 2019 ("**PDP Bill**") which sought to lay down the data protection law for India, but has now been withdrawn, had also recognised the role of processors and controllers.[93]

Since blockchain is characterised by decentralised data management, it complicates the identification of such a controller and processor.[94] Private permissioned blockchains may present a simpler case for identifying a controller. In such a case, a central operator or a group of entities that has control over the blockchain and determines the purpose and means of the processing of personal data may qualify as a controller. Other participants in the system such as nodes or miners that operate the blockchain (and process personal data) for the operator may qualify as processors.[95] However, identification of such controllers and processors is challenging in the case of a public permissionless blockchain where typically no authorisation is required to participate on the

[89] Pritesh Shah, Daniel Forester, 'Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies' (*Practical Law, 2019) <* https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf> accessed 15 September 2022.

[90] GDPR, art 4(7).

[91] GDPR, art 4(8).

[92] Commission Nationale Informatique Libertés, 'Blockchain : Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf> accessed 15 September 2022.

[93] In the PDP Bill, a data fiduciary was akin to a controller as under GDPR. Section 3(13) defined data fiduciary as "any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;". Section 3(15) defined data processor as "any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary." The PDP Bill had been referred to a Joint Parliamentary Committee for its consideration which had formulated a new bill 'Data Protection Bill, 2021' which sought to cover both personal and non-personal data. The Data Protection Bill retained concepts of data fiduciary and data processor as in the PDP Bill but amended both of these definitions as given under the PDP Bill, to also include non-government organisations who can be data fiduciaries and data processors. *See* Lok Sabha, 'Report of the Joint Committee on the Personal Data Protection Bill, 2019' (December 2021) < http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf > accessed 18 October 2022.

[94] Garry Gabison, *Policy Considerations for the Blockchain Technology Public and Private Applications*, 19 SMU Sci. & Tech. L. Rev. 327 (2017) <https://scholar.smu.edu/scitech/vol19/iss3/4/ > accessed 15 September 2022.

[95] Pritesh Shah, Daniel Forester, 'Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies' (*Practical Law, 2019) <* https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf> accessed 15 September 2022.

blockchain or access the data on the blockchain.[96] There are multiple unknown participants or nodes who can each verify the data on such blockchain.[97] In this context, it is difficult to identify a controller and processor because it is possible that each node independently processes the same set of data and contributes to the addition of data, which may lead to each node qualifying as a controller. While one may argue that in such a case, each node is a joint controller, such an interpretation is not clear. Even progressive data protection regimes such as the GDPR which recognise joint controller responsibilities still require transparent and specific allocation of such responsibilities, which may not be feasible in public permissionless blockchains.[98] Alternatively, it is equally possible that none of the nodes in a blockchain is individually in complete control of the data and therefore, arguably there is no controller and no processor.[99] In most countries, data protection authorities and other concerned regulators have not clarified the applicability of blockchain-based solutions.

Legitimate Reasons for Processing Personal Data

Typically, data protection laws consider the processing of personal data as lawful if the law permits such processing. For instance, GDPR stipulates grounds for lawfully processing personal data, which include instances such as where the data subject has given their consent for processing their personal data for specified purposes,[100] where the processing is necessary for performing a contract to which the data subject is also a party,[101] or where it is necessary for the controller in pursuance of any legal obligation[102] or to protect the vital interests of the data subjects or others.[103] Currently, there is no clarity on whether such grounds will encompass continuous distributed storage on a blockchain.

Data Protection Rights of Data Subjects

Data protection regimes hinge on giving autonomy and control to a data subject over their data and personal information.[104] Therefore, data protection laws envisage principles and rights of data subjects vis-à-vis controllers and processors. Well recognised principles and rights include principles of data minimisation, limitation, right to information, right to portability, and right to object.

While not all rights and principles are at odds with every use of blockchain,[105] some blockchain architecture may pose significant challenges to the assertion of certain fundamental rights and principles. For instance, a well-recognised data protection principle is that a data subject must have a right to erasure or the right to be forgotten, pursuant to which a data subject can request controllers to erase previously stored personal data about them in certain cases such as where the data has become irrelevant or it is no longer needed for the purpose for which it was processed in the first place.[106] However, the exercise of this right is likely to be at odds with immutability - a core technical feature of the blockchain which ensures that the blockchain ledger is a permanent record keeper of

[96] Financial Conduct Authority, 'Discussion Paper on Distributed Ledger Technology' (2017) <https://www.fca.org.uk/publication/discussion/dp17-03.pdf> accessed 16 September 2022; Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022 .

[97] Financial Conduct Authority, 'Discussion Paper on Distributed Ledger Technology' (2017) <https://www.fca.org.uk/publication/discussion/dp17-03.pdf> accessed 16 September 2022; Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022 .

[98] Commission Nationale Informatique Libertés, 'Blockchain : Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf> accessed 15 September 2022.

[99] Michele Finck, 'Blockchains and the Data Protection in European Union' (2017) Max Planck Institute for Innovation & Competition Research Paper No. 18-01 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080322> accessed 15 September 2022.

[100] GDPR, art 6(1)(a).

[101] GDPR, art 6(1)(b).

[102] GDPR art 6(1)(c).

[103] GDPR, art 6(1)(d).

[104] Commission Nationale Informatique Libertés, 'Blockchain : Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf> accessed 15 September 2022.

[105] These include for instance the right to access information- since in blockchain the data is visible and accessible to all participants, we do not envisage any challenge to this right.

[106] For instance, GDPR art 17.

all information and no data is altered or modified.[107] New information gets continuously added to old information in the ledger without removing any of the earlier information,[108] which may preclude a data subject from exercising such a right to be forgotten.

Similarly, implementing other principles such as the principle of data minimisation[109], purpose limitation,[110] storage limitation[111] and data accuracy[112] also become challenging in the context of blockchain applications. For instance, the principle of purpose limitation sets out the contours within which personal data collected for a given purpose may be processed and put to further use. It primarily has two components: *first*, data must be collected for a specific purpose (purpose specification); and *second*, once data is collected, it must not be processed in a manner that is incompatible with the purpose for which it was collected (compatible use).[113] Therefore, in case of any change of purpose, each subsequent use must be specified at the time of such change. Arguably, the issue that emerges is "whether further processing of data added to blocks after the execution of a transaction for which it was originally added to the ledger can be considered compatible with the purpose limitation principle."[114] Similarly, the principle of accuracy requires that the personal data so stored must be updated and steps must be taken to correct or erase any inaccurate data.[115] Implementation of this requires the data to be altered or modified which may be difficult to execute in blockchain applications.

Such problems are further amplified within a public blockchain. The data which already exists on-chain can generally only be altered or modified with the consensus of all the nodes.[116] In a public permissionless blockchain there could be many nodes and the majority of such nodes would have to consent to such alteration and verify and validate each of the affected transactions backwards and rebuild the blockchain again.[117] This would require immense computational power and cooperation which might be unfeasible. The exercise of these rights becomes even more important for a data subject at the point of exiting the blockchain and there may be no reason to keep their personal information on such blockchain unless retention is mandated or permissible under applicable laws. Blockchain features may make it difficult to exercise such deletion and selective retention, therefore, raising concerns about the non-compatibility of such technologies with data protection laws.

Jurisdictional Considerations

Most data protection laws apply according to the data subject's location or the location of data processing.[118] However, since public blockchains may be decentralised spreading across various jurisdictions and the identity of

[107]Ashit Kumar Srivastava, Deval Garg, 'Reconciling Blockchain and Data Protection Regimes' (2021) 56(40) EPW <https://www.epw.in/journal/2021/40/commentary/reconciling-blockchain-and-data-protection-regimes.html> accessed 15 September 2022.

[108]Ashit Kumar Srivastava, Deval Garg, 'Reconciling Blockchain and Data Protection Regimes' (2021) 56(40) EPWhttps://www.epw.in/journal/2021/40/commentary/reconciling-blockchain-and-data-protection-regimes.html> accessed 15 September 2022.

[109] The personal data collected should be relevant and limited to what is necessary in relation to the purposes for which they are processed. See GDPR, art 5(1)(c).

[110] The personal data shall only be collected for specified and legitimate purposes, See GDPR, art 5(1)(b).

[111] The personal data collected shall be stored such that identification of data subject is possible but only for the time period for which such storage is necessary to be meet the purpose of processing and no longer than that. See GDPR art 5 (1) (e).

[112] The personal data collected should be kept up to date and any inaccuracy should be rectified without any delay. See GDPR, art 5 (1) (d).

[113] Organisation for Economic Co-operation and Development, 'Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (2013) < https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188> accessed 15 September 2022.

[114] Dr. Michèle Finck, 'Blockchain and General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?' (2019) Panel for the Future of Science and Technology Study < https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 15 September 2022.

[115] GDPR, art 5(1)(d).

[116]Dr. Michèle Finck, 'Blockchain and General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?' (2019) Panel for the Future of Science and Technology Study < https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 15 September 2022.

[117] Matthias Berberich & Malgorzata Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers' (2016) 2 Eur Data Prot L Rev 422.

[118] For example GDPR, art 3.

participants is generally pseudo-anonymous, determining the territorial application and enforcing regulations against such decentralised systems is not straightforward.[119]

Cross Border Transfer of Data

The aforesaid challenges in determining the applicable jurisdictions' law also impinge on obligations relating to cross-border transfer of data. Data protection laws can impose restrictions or conditions on cross-border flow of data which include ensuring that recipient jurisdictions have adequate data protection frameworks in place.[120] Blockchain applications, especially public blockchains cannot control the flow of data across the nodes which might be located across various countries.[121] Data localisation obligations may also be a challenge especially for public permissionless blockchains.

Existing Legal Position in India

In 2017, the Supreme Court of India[122] recognised the right to privacy as a fundamental right, primarily emanating from Article 21 of the Indian Constitution. The Court also recognised informational privacy as an important aspect of the right to privacy.[123] To provide a meaningful right to privacy, it is important for the government to put in place a data protection law that can protect the informational privacy of citizens.[124] At present, the protection of personal data is governed by the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI Rules**") issued thereunder. India is yet to enact a separate data protection law. The PDP Bill which sought to create a comprehensive data protection framework in India, has now been withdrawn by the Government and a new data protection law is in the process of being framed.[125] This section discusses the implications of blockchain technology viz. the existing legal framework under the IT Act and SDPI Rules and the prevalent discourse on data protection norms in India.

Section 43A of the IT Act holds a body corporate liable for compensation for any negligence in employing reasonable security practices and procedures while dealing with "sensitive personal data or information".[126] The SPDI Rules issued pursuant to section 43A of the IT Act expands on the scope of the reasonable practices and procedures referred to in section 43A and incorporates several well-recognised data protection principles. The IT Act and the SPDI Rules were conceptualised keeping in mind centralised systems with a single entity (i.e. a body corporate) that controls the collection, possession or handling of personal data. In blockchain, the data is shared mostly across all the participating nodes, and they all contribute to the addition of the data and the control over the data is decentralised. Therefore, it is difficult to identify a central entity on whom such a duty and liability as envisaged under the IT Act and its rules can be affixed.

[119] Pritesh Shah, Daniel Forester, Carolin Raspe, 'Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies' (*Practical Law,* 2019) <https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf> accessed 15 September 2022.

[120] For instance, GDPR, ch 5.

[121] Pritesh Shah, Daniel Forester, Carolin Raspe, 'Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies' (*Practical Law,* 2019) <https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf> accessed 15 September 2022.

[122] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

[123] Privacy relates to the right of a person over his or her personality. Privacy consists of three aspects- (i) protection from intrusion of a person's physical body, (ii) informational privacy and (iii) privacy of choice.. Informational privacy is thus, a component of privacy. Informational privacy involves the right of an individual to have control over their personal information. This especially relates to the right of an individual to control the transfer and processing of their personal information in the virtual world The individual should decide what is the extent of their personal information that they want to share with the world. Thus, it is also the right to self-determination. *See*, Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

[124] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 'A Free and Fair Digital Economy: Protection Privacy, Empowering Indians' <https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf> accessed 15 September 2022.

[125] Sourabh Lele, 'Centre Withdraws Personal Data Protection Bill, Industry Disappointed' *The Business Standard* (New Delhi, 4 August 2022) <https://www.business-standard.com/article/economy-policy/centre-withdraws-personal-data-protection-bill-industry-disappointed-122080301781_1.html> accessed 15 September 2022.

[126] IT Act, s 43A.

Key Takeaways

1. *Existing data protection laws are designed for centralised databases / systems where a single entity or an identified group of entities is responsible for processing personal data and determining the purpose and means of such processing.*

2. *The decentralised and pseudo-anonymous nature of blockchain networks complicates the identification of such a controller and processor as mentioned above. While private blockchains may present a simpler case, the identification of such entities becomes more complex for public blockchains, where typically no authorisation is required to join and participate in such network.*

3. *The blockchain architecture may also pose significant challenges to the assertion of certain well-recognised data protection principles. For instance, the right to be forgotten or erasure of data may be difficult to implement due to the immutability of blockchain ledgers. Similarly, the technical feasibility of a data subjects' right to update or correct information on the ledger may also not be straightforward.*

Smart Contracts

Smart contracts are a type of agreement stored on a blockchain-based platform where a computer code executes all or parts of the agreement. Smart contracts can be of different types depending on the level of automation. At one end of the spectrum are smart contracts which are essentially natural language contracts with some or all the contractual obligations capable of being executed automatically.[127] However, as blockchain progresses further, there will be the inception of hybrid or fully automatic smart contracts wherein code will be used to delineate and execute most or all of the contractual terms.[128] Regardless of whether the smart contract contains natural language elements or is solely coded, the mere fact that it is self-executing in nature does not automatically exclude it from being governed under the established principles of contractual law.[129] The important question to answer is if smart contracts can adhere to the existing legal framework and if not, why and to what extent.

Some scholars argue that since smart contracts are self-executable, their performance is assured without the need for any judicial intervention.[130] But, the same is not true. There are certain mechanisms under contract law such as the remedies for breach of contract, ascertaining performance, remedies in case code execution results in wrong outcomes, etc. which may still require regulatory clarity.[131] Some common legal issues raised by smart contracts are set out below.

[127] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf > accessed 15 September 2022.

[128] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf > accessed 15 September 2022.

[129] Elisabeth M.S. Frommelt, 'Liability Challenges in Blockchain Ecosystem' (2020-2021) 21(2) UC Davis Business Law Journal 165 <https://blj.ucdavis.edu/archives/vol-21-no-2/UCD-Frommelt.pdf> accessed 15 September 2022.

[130] Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1, GEO. L. TECH. REV., 305 < https://www.ilsa.org/ILW/2018/CLE/Panel%20%2311%20-%20THE%20LAW%20AND%20LEGALITY%20OF%20SMART%20CONTRACTS%201%20Georgetown%20Law%20Technology%20Rev.._.pdf> accessed 15 September 2022.

[131] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf > accessed 15 September 2022.; Deepti Pandey, Harishankar Raghunath, 'Stationing Smart Contract as a 'Contract': A Case for Interpretative Reform of the Indian Contract Act, 1872' (2020) 13 NUJS L. Rev. 4 <http://nujslawreview.org/wp-content/uploads/2021/01/13-4-Pandey-Raghunath-Stationing-Smart-Contracts.pdf> accessed 15 September 2022.

Formation of Smart Contracts

Most common law jurisdictions recognise an agreement to be legally valid if there is a valid offer, acceptance of such an offer, certainty as to the intentions of the parties, and lawful consideration.[132] Generally, the established rules on offer and acceptance and consequent contract formation may not pose major challenges to smart contracts.[133] An offer can be deemed to be made when one party encodes contractual terms and deploys the same on the blockchain.[134] There could be deemed to be valid acceptance when the counterparty signs the smart contract through a private key or through its conduct specified in the smart contract.[135] For instance, in a simple smart contract wherein Party A promises to release money in the account of Party B if Party B sends a good, the coded promise to pay on delivery of goods can be a valid offer which can be validly accepted by Party B on either signing the same through a private key or by sending the goods over to Party A. On delivery of the goods, the smart contract will automatically release the payment to Party B without the intervention of Party A.

However, the United Kingdom ("**UK**") Law Commission[136] points out that while smart contracts which incorporate natural language agreements may experience fewer or no challenges, novel issues may arise in the case of solely coded smart contracts, where parties have engaged in limited or no natural language negotiations. In such cases, as per the UK Law Commission, whether the deployment and interaction of the parties with the code amount to an agreement will depend on the facts and circumstances of the case. For instance, A deploys a smart contract on a blockchain which provides that if 10 X cryptoassets are sent to the program, the program will send a crypto token to the account from which the cryptoasset is sent. Suppose, B sends 10 X cryptoassets to A's program, and the program automatically transfers a token to B's account. In such a case, the moment A programmed the transfer of 1 crypto token on receipt of 10 X cryptoassets without any condition, it may be interpreted as an offer from A. However, in case A's program was instructed to send out the token not automatically at the receipt of the cryptoassets, but subject to certain conditions, such as identification checks or compliance with some existing laws, it may be interpreted that A's intention is to only invite offers, which A can accept or reject depending on the satisfaction of the conditions set out in the program. Therefore, in certain cases, interaction with the smart contract will clearly amount to an offer and acceptance, whereas in certain cases, especially where there are conditions prescribed, or which involve multiple parties with multilateral transactions, the determination of contract formation may not be straightforward.[137]

Interpretation and Performance Challenges

Smart contracts are desirable when the agreement primarily contains straightforward promises,[138] which can be easily coded to be automated. However, many contractual promises are open-ended or subjective which require the parties and the court to interpret the intention of the parties in the context of changing circumstances to facilitate effective performance.[139] Contractual terms which make obligations subject to "good faith", "reasonable satisfaction" and "best efforts" are often used in contracts which is challenging to incorporate into the smart contract code.[140] Further, contract law recognises certain exceptions to liability for non-performance of contract, such as impossibility. For instance, force majeure or act of God which may lead to frustration of the contract

[132] R Yashod Vardhan (ed), *Pollock & Mulla: The Indian Contract Act, 1872* (15 edn, LexisNexis 2018).

[133] Larry A. DiMatteo, Michel Cannarsa, Cristina Poncibo (ed), *The Cambridge Handbook on Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2020).

[134] Smart Contracts Alliance, 'Smart Contracts: Is the Law Ready?' (*Chamber of Digital Commerce,* September 2018) <https://digitalchamber.s3.amazonaws.com/Smart-Contracts-Whitepaper-WEB.pdf> accessed 15 September 2022.

[135] Smart Contracts Alliance, 'Smart Contracts: Is the Law Ready?' (*Chamber of Digital Commerce,* September 2018) <https://digitalchamber.s3.amazonaws.com/Smart-Contracts-Whitepaper-WEB.pdf> accessed 15 September 2022.

[136] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf > accessed 15 September 2022.

[137] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf > accessed 15 September 2022.

[138] European Insurance and Occupational Pensions Authority, 'Discussion Paper on Blockchain and Smart Contracts in Insurance' (2021) <https://www.eiopa.europa.eu/sites/default/files/publications/consultations/eiopa-discussion-paper-on-blockchain-29-04-2021.pdf> accessed 15 September 2022.

[139] Primavera De Filippi, Aaron Wright, *Blockchain and the Law: Rule of Code* (Harvard University Press 2018).

[140] Stuart D. Levi, Alex B. Lipton, 'An Introduction to Smart Contracts and their Potential and Inherent Limitations' (*Harvard Law School Forum on Corporate Governance,* 26 May 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 15 September 2022.

rendering performance impossible, may be difficult to address in the performance of smart contracts.[141] Coded contractual terms require an exactitude which is not always possible in contractual relationships since negotiations and provisions are often left ambiguous or flexible to address unforeseen circumstances and advance business convenience.[142] Performance through smart contract is further complicated in the presence of well-established principles such as the doctrine of substantial performance which discharges parties from their contractual obligations even if they have not fulfilled the precise terms of the contract, but, as long as they have substantially discharged their obligations.[143] It is not clear how such contingencies and flexibilities can be accommodated by smart contracts since they are immutable and irreversible owing to their existence on the blockchain.[144] The immutable feature of blockchain also deters parties from carrying out necessary amendments to the contract or even terminating the contract at will. While in natural language contracts, novation of terms of the agreement and termination of an agreement can be affected if both the parties mutually agree, in public permissionless blockchains modifying the code on the blockchain is not easy and would require a lot of computational power.[145] This also heavily increases transaction costs associated with implementing smart contracts.[146]

Formality Requirements for Executing a Contract

Although the existing law on contract formation relating to offer, acceptance, consideration, etc. may not create any legal restrictions for the adoption of smart contracts, there might be avenues of potential conflict with laws which may specify certain formality requirements for a valid contract. For instance, general legal principles of contract formation recognise both oral and written contracts. However, some laws can stipulate that a specific type of contract must be "in writing" to be a valid contract.[147] In such cases, it will be useful to study existing laws to examine if the requirement in writing can be fulfilled by a contract which has been solely executed through computer codes without any natural language agreement, either on paper or digitally. The UK Law Commission identifies two codes which are used to draft such smart contracts - one, is source code which is in natural language and is human readable, and the second is machine code, which is in a binary form. It concludes that when a smart contract is drafted using source code, it can be held to be a contract in writing since it is a visible representation of words which can be read by an expert in programming.[148] However, the UK Law Commission is of the view that since machine code is in binary form and cannot be read by humans, it would not be considered "in writing".[149] However, such an interpretation regarding source code must be supported by applicable laws, which must clarify that the expression "in writing" includes source code.[150] Similarly, laws may require that agreements are duly signed by authorised representatives of the parties. While most laws treat digital signatures at par with physical signatures, the law will typically set out the form of such digital signature. Smart contracts usually use a range of

[141] Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022

[142] Stuart D. Levi, Alex B. Lipton, 'An Introduction to Smart Contracts and their Potential and Inherent Limitations' (*Harvard Law School Forum on Corporate Governance,* 26 May 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 15 September 2022.

[143] R Yashod Vardhan (ed), *Pollock & Mulla: The Indian Contract Act, 1872* (15 edn, LexisNexis 2018).

[144] Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1, GEO. L. TECH. REV., 305 < https://www.ilsa.org/ILW/2018/CLE/Panel%20%2311%20-%20THE%20LAW%20AND%20LEGALITY%20OF%20SMART%20CONTRACTS%201%20Georgetown%20Law%20Technology%20Rev.._.pdf> accessed 15 September 2022.

[145] Stuart D. Levi, Alex B. Lipton, 'An Introduction to Smart Contracts and their Potential and Inherent Limitations' (*Harvard Law School Forum on Corporate Governance,* 26 May 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 15 September 2022.

[146] Stuart D. Levi, Alex B. Lipton, 'An Introduction to Smart Contracts and their Potential and Inherent Limitations' (*Harvard Law School Forum on Corporate Governance,* 26 May 2018) <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/> accessed 15 September 2022.

[147] For instance, in India, the Transfer of Property Act, 1872 specifies sale deeds to be necessarily in writing.

[148] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[149] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[150] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

digital signatures.[151] Laws recognising digital signatures may need to be amended to accord recognition to the form of digital signatures used by smart contracts.

In some jurisdictions including India, payment of stamp duty and registration of certain types of contracts are mandated by law for being admissible as evidence in a court of law. Determining the place of contract formation is essential to ascertain the place where the contract needs to be registered and which state's stamp duty needs to be paid. For smart contracts which operate on a peer-to-peer network, since the nodes may be distributed across the country or even across the world, it might be difficult to ascertain the place of contract formation in the absence of the smart contract specifically stipulating the place of contract. Laws and guidelines which stipulate the place of formation for electronic records might be required to be formulated with respect to smart contracts.[152] Similarly, certain other laws require the presence of witnesses to deem an agreement to be a valid contract. Generally, witnesses need to be present physically for the same. However, since smart contracts are envisaged to be carried out completely digitally, from formation to execution, online mechanisms for facilitating witness verification may need to be explored. Further, in certain regulated sectors, customer verification procedures may be required prior to entering into a transaction. For smart contracts operating on a public blockchain, implementing these verification procedures might be a challenge since the identities of the parties might be pseudo-anonymous or anonymous.

Enforcement Challenges

Smart contracts also raise legal challenges at the enforcement stage. For instance, in a smart contract on a public permissionless blockchain, it may be difficult to identify the parties.[153] The pseudo-anonymous nature of such blockchain hinders the ability of parties to seek and enforce remedies in case of breach of contract. Enforcing specific performance or levying compensation against a counterparty will not be feasible without the means of identifying the party.

The second issue is the difficulty in identifying the place of the contract, which is necessary for identifying the law governing the contract and the determination of an appropriate forum for seeking remedies. The decentralised nature of blockchain means that multiple parties could be contracting from anywhere in the world. [154] Further, due to the general pseudo-anonymous nature of public permissionless blockchains, it will not be easy for courts to rely on the domicile of the parties to determine jurisdiction. Unless it is stipulated specifically in the contract itself, the decentralised nature of blockchain and the pseudo-anonymous identities of the participants create challenges in determining the appropriate jurisdiction where contract breach claims can be brought.[155]

The third issue lies in enforcing certain specific remedies such as declaring a contract void or voidable. Since smart contracts are automatically executed without the need for human intervention and operate on the immutable blockchain ledger, technical feasibility of undoing such smart contract which has already been executed is not straightforward.[156] Further, terminating a smart contract for breach or otherwise may also prove to be difficult. This is because since the smart contract code is recorded on an immutable ledger, no one party can unilaterally delete or modify any code on a blockchain. In public blockchains especially, the party intending to terminate the

[151] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[152] For instance, in India generally Court judgments (see for instance Bhagwandas Goverdhandas Kedia v. M/s Girdharilal Parshottamdas AIR 1966 SC 543) relating to receipt rule applies for determining where the contract was formed for e-contracts. It states that when acceptance is communicated through instantaneous communication channels, the contract is formed when the acceptance is intimated and received by the offeror. Further, section 13(3) of the IT Act specifies that save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business and is deemed to be received at the place where the addressee has his place of business. A combined reading of the judgments and section 13(3) of the IT Act is generally used to determine the place of contract formation in case the contract does not explicitly state the same.

[153] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 Mod L Rev 1073.

[154] Nathan Fulmer, 'Exploring the Legal Issues of Blockchain Applications' (2018) 52 Akron L Rev 161.

[155] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[156] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

contract would need privileges to terminate the automatic execution of the code.[157] Unless parties specifically incorporate such abilities to amend or terminate a contract during the time of smart contract creation coding, this will present a huge challenge for the adoption of smart contacts.

Existing Legal Position in India

The formation, performance, interpretation, and enforcement of smart contracts will have to be studied in the context of specific laws in India such as the Indian Contract Act, 1872 ("**Contract Act**"), IT Act, and the Indian Evidence Act, 1872 ("**Evidence Act**").

Contract Act: The Contract Act sets forth the components of a valid agreement in India, which includes a valid offer, acceptance, legal intention, consensus ad idem and consideration. Smart contracts can broadly fulfil these essential ingredients of a valid agreement and constitute a legally binding contract under Contract Act. In smart contracts, such proposals and offer terms can be incorporated into the code and deployed on the blockchain for other participants to access.[158] The cryptographic signing of a smart contract by the counterparty through a private key can comprise a valid acceptance.[159] Similarly, fulfilling the promises laid out in the offer will also constitute acceptance by conduct.[160] Regarding consideration, the Contract Act does not examine the adequacy of the consideration but instead focuses on the existence of lawful consideration. The mutual promises as encapsulated within the smart contract code can comprise consideration. In many cases, parties may undertake necessary steps to ensure that the legal intention to enter into a contract may be easily deduced in case of a conflict. However, novel questions may arise in the case of fully automated smart contracts which are not preceded by any human communication. Further, as discussed above, smart contracts may face challenges within the Contract Act in terms of performance and enforcement.

IT Act and Evidence Act: The IT Act lends legal recognition to contracts in electronic form. Under section 10A, a contract is not deemed to be invalid merely because the same is expressed in an "electronic form" or by means of an "electronic record". However, whether such "electronic form" and electronic record" includes blockchain-based smart contract, is one of the preliminary points that would require clarification.[161] Further, issues regarding signing of smart contracts may also require additional clarification. Section 5 of the IT Act accords legal recognition to electronic signatures. A combined reading of section 2(ta) and section 3A provides that an electronic signature will be recognised under the IT Act if it follows and fulfils the authentication technique specified under the second schedule of the IT Act. The second schedule of the IT Act recognises e-authentication techniques which includes hash and asymmetric crypto system techniques.[162] It has been pointed out that a smart contract especially smart contracts which are solely coded can be signed by various methods through code.[163] It is not clear if all such techniques necessarily adhere to the authentication techniques specified in the second schedule. Thus, unless these methods are notified under the IT Act or the law preconditions that electronic signatures used for smart contracts will be legally recognised only if they adhere to the authentication techniques set out in the IT Act, the issue of legal recognition of authentication techniques for smart contracts is not clear. This may pose a problem under Evidence Act as well. Under it, electronic signatures, electronic records, and electronic forms are to have the same meaning as under IT Act and hence, the requirements under IT Act for a recognised electronic signature and electronic forms and electronic records would apply.[164] Therefore,

[157] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[158] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[159] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[160] Contract Act, s 8.

[161] IT Act, s 2(r) defines electronic form as "with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device". IT Act, s 2(t) defines electronic record as "data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche".

[162] IT Act, sch 2.

[163] Law Commission, *Smart Legal Contracts: Advice to Government* (Law Com No 401, 2021) <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/11/Smart-legal-contracts-accessible.pdf> accessed 15 September 2022.

[164] Evidence Act, s 3.

admissibility of smart contracts and smart contracts relying on authentication techniques not recognised by the IT Act may be questionable.

Key Takeaways

1. *Generally, the existing rules on contract formation (offer, acceptance, and consideration) can be extended to smart contracts.*

2. *Typically, smart contracts which incorporate or are preceded by some natural language agreements or communication will be able to satisfy the fundamental requirements of contract formation. However, novel issues may arise in the case of solely coded smart contracts where parties have engaged in limited or no natural language negotiations. In such cases, specific facts and circumstances of the case have to be examined to identify the legal intention of parties to enter into a contract.*

3. *Smart contracts are desirable when the agreement contains straightforward promises. However, if such promises are open-ended or subjective requiring courts to interpret the intention of parties, adoption of smart contracts may be challenging.*

4. *Application of contractual principles of force majeure, the impossibility of performance, the doctrine of substantial performance and the incorporation of well-known contractual standards which makes obligations subject to "good faith", "reasonable satisfaction" and "best efforts" are at times at odds with certain characteristics of blockchain. Therefore, smart contracts may not be the ideal choice where parties desire some flexibility.*

5. *The decentralised and pseudo-anonymous nature of blockchain raises challenges in the enforcement stage. This is true for public permissionless blockchain where nodes may be scattered across the globe and identifying specific parties responsible for a breach is not straightforward.*

6. *Laws which impose certain formalities for recognising contracts such as written requirements for contracts, payment of stamp duty, registration of contracts and attestation by witnesses will also require examination in the context of blockchain applications.*

Jurisdictional Challenges

Participating nodes in blockchains, especially public permissionless blockchains may be situated anywhere across the world. The transnational reach of blockchain raises two questions relating to jurisdiction – *first*, what is the applicable law which will govern the legal relationships of the parties; *second*, what would be the appropriate forum to raise any dispute relating to blockchain applications?

In public permissionless blockchains where the nodes may be situated across different countries, may expose participants to multiple and often potentially conflicting assertions of governing law. Typically, for a specific law to apply, there must be some "minimum contact" which occurs in such jurisdiction.[165] In a decentralised network it is difficult to prove where such contact has taken place and the extent of such contact. Since the distributed nature of blockchain provides access and control over information to all the nodes, a straightforward application of common law principles of jurisdiction may result in every such transaction done by a node to be held as minimum contact thereby attracting the laws of every jurisdiction where such node is situated. This may lead to conflict of

[165] Tricia Leigh Gray, 'Minimum Contacts in Cyberspace: The Classic Jurisdiction Analysis in a New Setting' (2002) 1(1) Journal of High Technology Law < http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/GrayMinimumContacts.pdf> accessed 16 September 2022.

laws and overregulation since the participants will be subject to the laws of multiple jurisdictions.[166] On the other hand, if the applicable law is not determined it might lead to a situation of regulatory arbitrage. With private and permissioned blockchains, it may be easier to stipulate a framework for determining the governing law that will be applicable to transactions on such blockchains.

Enforcement of rights (whether under a contract or a law) is not possible if users do not have a forum to approach for legal recourse. Most countries have specific rules for determining a court's jurisdiction. This may include factors such as the place of domicile of the defendant or the place where the cause of action has arisen.[167] The pseudo-anonymous and decentralised nature of blockchain may hinder the identification of the domicile of parties or the determination of the place where the cause of action has taken place.

Existing Legal Position in India

In India, the Code of Civil Procedure, 1908 ("**CPC**") sets out the rules for determining the jurisdiction of a civil court in case of civil disputes. Sections 15-20 of CPC stipulate that a civil court will have the territorial jurisdiction to try a civil suit if – (a) the cause of action, wholly or in part, arises within its local limits; (b) the defendant carries on business or resides therein, and (c) in cases of suits concerning immoveable property, where the property is situated. Due to the decentralised and pseudo-anonymous nature of a public permissionless blockchain, it may be difficult to ascertain the jurisdiction on the basis of (a) and (b) mentioned above.[168] However, this difficulty can be mitigated if the participants in a blockchain network specify contractually which court will have jurisdiction in case of a dispute. The Supreme Court has recognised that parties to a contract are permitted to specify the competent courts to adjudicate a dispute arising from the contract.[169] However, the Court has also clarified that this does not entitle parties to contractually confer jurisdiction on any court which inherently does not have jurisdiction in law to adjudicate on the given matter.[170] There must be some nexus of the chosen jurisdiction with the subject-matter of the contract or with regard to the parties.[171]

Key Takeaways

1. *The transnational reach of blockchain networks and public permissionless blockchains raises two important questions regarding the applicable law governing the network, and the identification of the appropriate forum to adjudicate disputes arising out of such arrangements.*

2. *Unlike public permissionless blockchains, it may be simpler to contractually agree on such governing law and competent courts to try disputes under a blockchain arrangement in the case of private permissioned blockchains with a limited number of identified participants.*

Structure and Governance

The operation of blockchain needs to be within the established legal contours. The applicability of legal rules to a blockchain-based solution is closely related to its structure and the rules for its governance. This is necessary to identify the rights of participants and the consequences in cases of default from agreed rules or protocols. Any failure of the blockchain is distributed across multiple nodes across multiple jurisdictions, instead of just being

[166] John McKinlay and others, 'Blockchain: Background, Challenges and Legal Issues' (*DLA Piper,* 2018) <https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/> accessed 15 September 2022.

[167] Nishith Desai Associates, 'The Blockchain: Industry Applications and Legal Perspectives' (2018) <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/The_Blockchain.pdf> accessed 15 September 2022.

[168] Nishith Desai Associates, 'The Blockchain: Industry Applications and Legal Perspectives' (2018) <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/The_Blockchain.pdf> accessed 15 September 2022.

[169] Hakam Singh v. Gammon (India) Ltd 1971 SCR (3) 314.

[170] Hakam Singh v. Gammon (India) Ltd 1971 SCR (3) 314.

[171] Hakam Singh v. Gammon (India) Ltd 1971 SCR (3) 314.

confined to a small group of selected parties as is the case in traditional systems.[172] Therefore, an examination of the structure and governance mechanisms of blockchain networks is important to identify legal protections that `may be required by participants.

Identification of Participants

A blockchain network is likely to comprise of multiple participants with a shared objective but each participant may have different roles and responsibilities. For a legal claim to stand or for legal rights to be enforced, the party against whom such a claim will lie will need to be identified. Typically, in public blockchains, the identities of the participants are likely to be pseudo-anonymous.[173] This poses a severe challenge in identifying the responsible participant and enforcing any claim against them. However, in private blockchains, it is possible to have a mechanism to establish and verify the identity of the participants.

Governance Model

The governance model refers to the mechanism through which nodes operate and adapt in a network and the way decisions are taken. Typically, public blockchains are governed by all or most participants. Therefore, such blockchains are preferred where control over decisions by a few is not the primary objective. Such blockchains generally do not have a formal governance structure and rely on "systemic governance based on technologies".[174] However, in case of use cases which require that control over network governance and decisions is in the hands of a selected few, a private blockchain may be a preferred option. Many private blockchains may incorporate some form of formal governance structure. One such approach is to form a consortium, which is an association of organisations designed to develop, promote and access blockchain technology.[175] Consortia may be formed for different objectives.[176] For instance, a tech-focused consortium may bring together different entities to develop the technology, including standards instead of use cases. An industry-focused consortium may bring together participants from a particular industry to explore use cases within that specific industry. For instance, a consortium of major banks in Europe founded we.trade on the IBM Blockchain Platform to facilitate a more effective, safe and simplified framework for cross-border trade. The we.trade network connects buyers, sellers, insurers and logistic companies together under one platform.[177] After fulfilling appropriate KYC requirements, banks induct buyers and sellers onto the blockchain.[178] These traders can thereafter independently create orders, manage the payment processes and seek funding on the blockchain platform with ease.[179] Transactions are recorded on the blockchain and smart contracts are deployed to ensure payment is done once the deal or transaction terms as recorded on the blockchain are satisfied.[180] In India as well, 15 banks formed a consortium called the Indian Banks' Blockchain Infrastructure Company Private Limited to use blockchain to record and verify letters of credit, goods and services tax and e-way bills to eliminate fraud and quicken transaction time.[181]

[172] Philipp Paech, 'The Governance of Blockchain Financial Networks' (2017) 80 Mod L Rev 1073.

[173] Vipul Kharbanda, Aman Nair, 'Analysing Non-Financial Use Cases of Blockchain in India' (2022) Centre for Internet and Society Working Paper <https://cis-india.org/internet-governance/non-financial-blockchain-uses-pdf> accessed 15 September 2022.

[174] Jersain Zadamig Llama Covarrubias, Irving Norehem Llama Covarrubias, 'Different Types of Government and Governance in the Blockchain' (2021) 10(1) Journal of Governance and Regulation <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859793> accessed 15 September 2022.

[175] Tech London Advocates' Blockchain Legal and Regulatory Group, 'Blockchain: Legal and Regulatory Guidance' (*The Law Society,* 2020) p 128 < https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report> accessed 15 September 2022.

[176] Tech London Advocates' Blockchain Legal and Regulatory Group, 'Blockchain: Legal and Regulatory Guidance' (*The Law Society,* 2020) p 128 < https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report> accessed 15 September 2022.

[177] Claran McGowan, 'Anatomy of an Intelligent Blockchain Trading Solution' (*IBM Blog,* 14 April 2020) <https://www.ibm.com/blogs/client-voices/we-trade-provides-intelligent-trading-solution/ > accessed 15 September 2022.

[178] Claran McGowan, 'Anatomy of an Intelligent Blockchain Trading Solution' (*IBM Blog,* 14 April 2020) <https://www.ibm.com/blogs/client-voices/we-trade-provides-intelligent-trading-solution/ > accessed 15 September 2022.

[179] Claran McGowan, 'Anatomy of an Intelligent Blockchain Trading Solution' (*IBM Blog,* 14 April 2020) <https://www.ibm.com/blogs/client-voices/we-trade-provides-intelligent-trading-solution/ > accessed 15 September 2022.

[180] Claran McGowan, 'Anatomy of an Intelligent Blockchain Trading Solution' (*IBM Blog,* 14 April 2020) <https://www.ibm.com/blogs/client-voices/we-trade-provides-intelligent-trading-solution/ > accessed 15 September 2022.

[181] Joel Rebello, '15 Banks to Start New Trade Finance System Using Blockchain Tech' *The Economic Times* (India, 15 June 2021) <https://economictimes.indiatimes.com/industry/banking/finance/banking/15-banks-to-start-new-trade-finance-system-using-blockchain-tech/articleshow/83545043.cms> accessed 16 September 2022.

The consortium which is typically responsible for the business governance of the blockchain network is responsible for the selection of business lines, fundraising, vendor selection, and software.[182] Currently, the consortium may be organised in different forms – contractual consortium model, joint venture model, developer agreement and participant agreement model as described below.[183]

- Contractual Consortium Model: This involves the execution of an agreement between the members of a consortium including the developer of the blockchain network. The consortium members will be users of the platform. However, it can also include other participants whose use of the platform may be governed by separate end user license agreements. There will be governance structures with defined membership. While consortium members will have higher rights as they may contribute to the development of the technology, end users will have lower influence over the platform as they would receive it as a service.

- Joint Venture model: The consortium members enter into a joint venture to form a separate legal entity ("**JV Entity**") that will be responsible for the platform. This JV Entity will be responsible for stipulating the terms of the platform or the agreements that will govern all participants and end users.

- Participant Agreement Model: In cases where one single entity is leading the project, it may not be possible to use the contractual consortium model and joint venture model which are typically driven by multiple parties. In the participant agreement model, the network operator (which is typically the tech provider) will offer a standard set of terms and conditions which are then offered to a range of participants of the platform.

- Developer Agreement Model: This is also suitable for cases where the project development is led by a single entity. In this model, several participants enter into a multi-party agreement between themselves and the network operator for a common purpose. However, the network operator continues to control decisions relating to the platform.

The choice of an appropriate model will depend on the objective of the project, the number of members driving the project and their risk appetite. Irrespective of which model is adopted, the adoption of any of these models requires an examination of legal risks and the execution of agreements to govern the relationship of the members. There is no specific law to govern these issues but will be determined by the mutual agreement of the parties involved. Legal issues that must be examined in the context of such models include – eligibility of consortium members, defining the scope and extent of control of members on the decisions relating to platform development, dispute resolution, exit mechanism, apportionment of liability, IPRs that individual members may have to license to the JV Entity, each other, and the ownership of new IPRs created in the process, and confidentiality.

While the aforesaid consortium models are relevant from a business governance perspective, which looks at the commercial development and exploitation of a blockchain platform, it has been pointed out that governance structures must be in place for operational governance, including developing information and other security standards while using a blockchain network.[184] This may include rules to verify members joining the blockchain network, identifying who is responsible for approving such new members, exit mechanism for participants to leave the network, data storage and governance standards.[185]

[182] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

[183] Tech London Advocates' Blockchain Legal and Regulatory Group, 'Blockchain: Legal and Regulatory Guidance' (*The Law Society,* 2020) p 130-141 < https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report> accessed 15 September 2022.

[184] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

[185] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022. ; Jersain Zadamig Llama Covarrubias, Irving Norehem Llama Covarrubias, 'Different Types of Government and Governance in the Blockchain' (2021) 10(1) Journal of Governance and Regulation <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859793> accessed 15 September 2022.

Participant Onboarding and Exit

For private permissioned blockchains, it is usually left to the network operator or the governing body of the network to determine rules of membership and verify whether applicants meet such criteria. Such rules are necessary in the case of blockchains dealing with sensitive information and where it may not be necessary to open the network to multiple participants. While determining such rules, it is also important to consider if there is provision for participants to exit or to be removed. Such flexibility may be useful for the sustainability of the network.

Role and Duties of Participants

Traditional frameworks of liability primarily operate basis a centralised model, wherein there is a central authority on whom responsibility can be affixed. Due to the decentralised nature of blockchain arrangements, such affixation of liability on a single entity is not straightforward. Particularly in the case of public blockchains, multiple nodes may have equal permission and rights with respect to the data on the blockchain.[186] Therefore, identifying attribution of liability in case of default is complicated, where either all nodes would be responsible, or none would be. Therefore, both in permissioned and permissionless blockchain, identification of the role of the participants is of utmost importance. It is imperative to determine the different powers and roles that each node has, and which are the responsible nodes therein. The duties of each of the nodes would be different. For instance, for nodes identified as network developers, the duties could include incorporating technological designs that would balance both privacy requirements and anti-money laundering/combating of the financing of terrorism ("**AML/CFT**") compliances.

Internal Dispute Resolution

With the delineation of roles and responsibilities, rules governing the operation of the blockchain network and the setting up of governance structures, it is imperative to have a mechanism for redressing grievances in case of default by any participant. Given the complex and technical nature of blockchain, it will not be easy to resort to traditional dispute adjudication mechanisms (such as courts) for quick redressal of grievances. In such cases, it may be worthwhile for the network to design an internal dispute resolution mechanism, the details of which are discussed in Chapter VI.

In light of the above, it is necessary that the relationship between the blockchain network, the network operator and the participants are clearly documented. Similarly, participants must agree on the terms and conditions applicable to the blockchain network as discussed above, which will include issues relevant to both business and operational governance.

Key Takeaways

1. *The applicability of legal rules to a blockchain network is closely related to its structure and rules for governance. This is relevant to identify the rights and liabilities of participants. Due to the decentralised nature of blockchain, there is a possibility that either all nodes may be held liable for any breach or failure of the network, or no node is held liable since it is challenging to fix liability on a particular node. Both these consequences are not desirable as it disincentivises serious players to join the network.*

2. *Some key issues that emerge in the structure and governance model of blockchain networks are set out below:*

(a) *Governance models refer to the mechanism through which the nodes operate and take decisions in a network.*

(b) *In cases where decisions regarding the network may be required to be confined to selected nodes/participants, private blockchains will be preferred. Even within such a*

[186] Vipul Kharbanda, Aman Nair, 'Analysing Non-Financial Use Cases of Blockchain in India' (2022) Centre for Internet and Society Working Paper <https://cis-india.org/internet-governance/non-financial-blockchain-uses-pdf> accessed 15 September 2022.

blockchain network, formal governance structures may be incorporated based on the objective of the project, the number of members driving the project and their risk appetite. However, the adoption of any model requires an examination of legal risks and the execution of agreements to govern the relationship of the members.

(c) *It is necessary that the relationship between the blockchain network, the network operator and the participants are clearly documented. Any blockchain network will also require rules regarding the eligibility criteria of participants that can join the network, enumeration of rights and duties of participants, and participant onboarding and exit. In the absence of any specific laws governing such models, it is useful for participants to agree on such important terms governing their participation in the network to provide them certainty, and legal protection.*

(d) *The aforesaid features of the structure and governance model is easier to implement in case of private permissioned blockchains and may not be applicable to public permissionless blockchains.*

Ancillary Legal Issues

This part highlights ancillary legal issues raised by existing literature. This Working Paper captures these issues to present the reader with a comprehensive overview of legal issues that blockchain solutions may bring. However, given that the existing research on most of these ancillary issues is at a nascent stage, this Working Paper does not take a position on these issues and accordingly does not provide any detailed recommendation.

Intellectual Property Rights

The interaction of blockchain applications with intellectual property rights ("**IPR**") may be viewed from two perspectives - one, where the subject matter of IPR is a blockchain-based application itself; and second, as a use case, where blockchain is used to further IPR management. For the purposes of this Working Paper, the discussion will focus on the former as the latter is a specific use case, which is not within the scope of the Working Paper.

Ownership of IPR in the blockchain: IPR issues emanate at the time of development of blockchain. First, it is important to understand if any intellectual property ("**IP**") needs to be licensed by participants to develop the blockchain application and then once the final application is developed, questions on ownership of IP and its licensing will arise. The owner or the license holder of such IP must be identified, failing which, it will be difficult to identify legal rights or legal remedies that can be bestowed in relation to the blockchain invention. In the context of private blockchains, it is important for consortium members or participants to document their rights to use an IP, whether in creating a blockchain application or in the blockchain application itself. However, these issues may be complicated in the case of public permissionless blockchains. For instance, in public permissionless blockchains, it is difficult to ascertain who exactly owns the blockchain software or protocol since so many nodes contribute to the development of the software.[187] It will have to be ascertained who made the contributions and the nature of the improvements and developments on the blockchain which would qualify them to be owners.[188] Further, existing literature also highlights that in instances where a user-facing app hosts the blockchain network, there may be a conflict as to whether the blockchain developer or the trusted intermediary for whom the app is developed, is the owner of the blockchain-based user application.[189]

[187] Mark Cianci, 'Legal Implications of Decentralized Autonomous Organisations' (*Bloomberg Law,* 2022) <https://www.ropesgray.com/-/media/Files/articles/2022/04/20220414_Bloomberg_DAO_Article.pdf?la=en&hash=658041824B53B872F7A3554798E1971418EDA41E> accessed 16 September 2022.

[188] Mark Cianci, 'Legal Implications of Decentralized Autonomous Organisations' (*Bloomberg Law,* 2022) <https://www.ropesgray.com/-/media/Files/articles/2022/04/20220414_Bloomberg_DAO_Article.pdf?la=en&hash=658041824B53B872F7A3554798E1971418EDA41E> accessed 16 September 2022.

[189] Tech London Advocates' Blockchain Legal and Regulatory Group, 'Blockchain: Legal and Regulatory Guidance- Second Edition' (*The Law Society,* 2022) < https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-second-edition> accessed 15 September 2022.

Patentability: Blockchain applications are increasingly being adopted by companies and businesses to gain competitive advantages over their competitors that still rely on traditional systems and products. Therefore, many companies and institutions are now coming forward to file patents over these blockchain inventions to prevent other companies from developing competing technology so as to preserve this competitive edge.[190] A grant of a patent also unlocks various financial avenues for a company since they can license such patent applications to third parties. For instance, Mastercard is one of the leading companies which holds various patents for their blockchain innovations ranging from patents for blockchain-based immutable data records to fractional cryptocurrency banking.[191] While various blockchain applications have already received patents[192], there is still considerable debate as to whether blockchain-based innovations are patentable.[193] Generally, blockchains will be seen within the ambit of computer programmes or algorithms and hence, jurisprudence relevant to these inventions will be considered, to evaluate whether blockchain is patentable.[194] Across different global regimes, including India, there is a consensus that computer programmes or abstract ideas which include computer programmes are not patentable since they are the basic tools of scientific and technological works.[195] However, courts in India have recognised that if a computer programme is a technical contribution then it may be eligible for a patent.[196] Technical contribution involves assessing whether the invention created any technical effect i.e., if it provides a novel solution to any existing technical problem and thereby is a technical advancement in such a space.[197] Additionally, an invention needs to fulfil other conditions as provided in court decisions or legislations, which include the satisfaction of the claim that it is "non-obvious", "novel" or "inventive".[198] Such requirements may be difficult to prove in the context of blockchain because it can be argued that each blockchain application improves upon the same existing technology, and is not novel.[199] Alternatively, proponents of blockchains being eligible for patents argue that blockchains can be used to develop unique processes which can improve the functionality of computer processes through immutability and decentralisation, and therefore be eligible for a patent.[200]

Competition Law

The Competition Commission of India ("**CCI**") and various scholars globally have highlighted that as blockchain applications gain traction in more sectors and become more pervasive in the market, there may be instances of

[190] Ioannis Lianos, 'Blockchain Competition: Gaining Competitive Advantage in the Digital Economy- Competition Law Implications' in Philipp Hacker and others (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press, 2019) ; Jörg Weking and others, 'Impact of Blockchain Technology on Business Models- A Taxonomy and Archetypal Patterns' (2020) 30 Electron Markets <https://link.springer.com/article/10.1007/s12525-019-00386-3> accessed 16 September 2022;

[191]Vicki Hyman, 'How Mastercard's Blocckhain Whiz has Turned Risk into Opportunity' (*Mastercard,* 29 October 2022) <https://www.mastercard.com/news/perspectives/2020/how-mastercard-s-blockchain-whiz-has-turned-risk-into-opportunity/> accessed 16 September 2022 ; Ricardo Esteves, 'Mastercard Wins Patent for "Managing Fractional Reserves of Blockchain Currency"' *News BTC* (https://www.newsbtc.com/news/blockchain/mastercard-wins-patent-for-managing-fractional-reserves-of-blockchain-currency/; Nikhilesh De, 'Mastercard Patent Filings Tout Blockchain for Immutable Data Records' *CoinDesk* (17 September 2022) <https://www.coindesk.com/markets/2018/09/17/mastercard-patent-filings-tout-blockchain-for-immutable-data-records/> accessed 16 September 2022.

[192]Chip Law Group, 'Who is Leading the Global Blockchain Patent Race?' (*Lexology,* 22 November 2021) <https://www.lexology.com/library/detail.aspx?g=e129bc47-15a5-4a39-9335-b81d7c3783a5> accessed 16 September 2022.

[193]Inayat Chaudhry, ' The Patentability of Blockchain Technology and the Future of Innovation' (*American Bar Association Landslide 10(4),* 2018) <https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/march-april/patentability-blockchain-technology-future-innovation/#ref30> accessed 16 September 2022.

[194] Inayat Chaudhry, ' The Patentability of Blockchain Technology and the Future of Innovation' (*American Bar Association Landslide 10(4),* 2018) <https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2017-18/march-april/patentability-blockchain-technology-future-innovation/#ref30> accessed 16 September 2022.

[195] Alice Corp. v. CLS Bank International, 573 U.S. 208 (2014); Telefonaktiebolaget LM Ericsson v Intex Technologies (India) Limited 2015 SCC OnLine Del 8229; The Patents Act, 1970, s 3(k).

[196] Telefonaktiebolaget LM Ericsson v Intex Technologies (India) Limited 2015 SCC OnLine Del 8229; Ferid Allani vs Union Of India & Ors 2019 SCC OnLine Del 11867.

[197] Ferid Allani v. Union of India & Ors. 2019 SCC OnLine Del 11867.

[198]For example, 35 U.S. Code, s 102; Patent Act, 1970 ; Office of the Controller General of Patents, Designs & Trademarks, 'Frequently Asked Questions- Patents' (2020) <https://ipindia.gov.in/writereaddata/Portal/Images/pdf/Final_FREQUENTLY_ASKED_QUESTIONS_-PATENT.pdf> accessed 16 September 2022.

[199] S.S. Rana & Co. 'Patentability of Blockchain Technology' (2018) <https://ssrana.in/articles/patentability-block-chain-technology/ > 16 September 2022.

[200] S.S. Rana & Co. 'Patentability of Blockchain Technology' (2018) <https://ssrana.in/articles/patentability-block-chain-technology/ > 16 September 2022.

anti-competitive behaviour related to blockchain.[201] For instance, it has been discussed that private permissioned blockchains may impose conditions relating to access and entry.[202] This may lead to deliberate exclusion of certain categories of participants which may result in a concerted refusal to deal.[203] Additionally, since on a blockchain, the information on the ledger is visible to all participating entities, it may enable competitors to get access to each other's information.[204] At the same time, the same information may not be readily visible to non-participating entities.[205] Unless adequate safeguards are taken, this may lead to competitors on the blockchain forming agreements and supervising each other's conduct.[206]

The CCI and the European Blockchain Observatory and Forum have also highlighted that blockchains can also be used to further abusive conduct.[207] They have highlighted that if dominance is established[208] for a particular blockchain application, then there might be instances where the blockchain can be used to facilitate abusive conduct. For instance, a dominant blockchain may refuse to provide access which can be anti-competitive if the blockchain or rather the data in the blockchain is an "essential facility" which is required by the third party to undertake the relevant activity in the market.[209]

[201] Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022 ; Dr. Thibault Schrepel, 'Collusion by Blockchain and Smart Contracts' (2019) 33(1) Harvard Journal of Law Technology <https://jolt.law.harvard.edu/assets/articlePDFs/v33/03-Schrepel.pdf> accessed 16 September 2022.; Pike, C, and A. Capobianco (2020), Antitrust and the trust machine><http://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf> accessed 16 September 2022.

[202] Dr. Thibault Schrepel, 'Collusion by Blockchain and Smart Contracts' (2019) 33(1) Harvard Journal of Law Technology <https://jolt.law.harvard.edu/assets/articlePDFs/v33/03-Schrepel.pdf> accessed 16 September 2022.

[203] Organization of Economic Co-operation and Development Secretariat, 'Blockchain Technology and Competition Policy' (2018) < https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf> accessed 16 September 2022.

[204] Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022.

[205] Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022.

[206] Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022.

[207] Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Young LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022. ; https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

[208] It will be required to be established based on relevant geographical and product market.

[209] Essential facility is an infrastructure which is essential for entities to operate in a market, but which cannot be easily replicated. *See* Chinmaya Goyal and others, 'Discussion Paper on Blockchain Technology and Competition' (*Competition Commission of India and Ernst & Ypung LLP,* April 2021) <https://www.cci.gov.in/search-filter-details/524> accessed 16 September 2022; Arshiya Rail Infrastructure v. Ministry of Railways 2012 SCC OnLine CCI 53.

V. The Global Approach to Blockchain

Globally most countries have a positive response to blockchain adoption. Countries are at different stages in their assessment and adoption of blockchain. Most countries are still exploring and examining the use cases of blockchain technology for different sectors considering the specific needs of their countries. However, almost all jurisdictions are cognisant and acknowledge the innovation potential of blockchain and therefore, have initiated some type of conversation on the same. This Working Paper examines the approach of 20 countries ("**Surveyed Jurisdictions**")[210] to study the global approach toward blockchain technology in policy discussions. For the United States (US), the Working Paper focuses on 7 specific states.[211] Based on a review of the publicly available literature (i.e., official government documents) on policy discussions on blockchain adoption in different countries, this Working Paper has limited its study of the global approach to these Surveyed Jurisdictions. Based on an examination of policy approaches in the Surveyed Jurisdictions, the Working Paper classifies global policy approaches toward blockchain adoption under three categories.

Issuance of Consultation/Strategy Papers and Guidance Notes

Nine of the Surveyed Jurisdictions (Bangladesh, Dubai, Germany, Hong Kong, UK, Thailand, Malaysia, China and Australia) are still in the process of exploring the costs and benefits of blockchain through the publication of strategy papers and consultation papers. Most of these documents are at an exploratory stage and generally do not take any position on the requisite legal or regulatory changes. However, they highlight the need for examining the existing legal regime considering blockchain use.

Most of these policy papers also identify the various areas where the government seeks to introduce blockchain technologies. Some common areas include exploring the potential of blockchain in integrating supply chains, facilitating identity verification (Australia, Bangladesh, Hong Kong, Malaysia and Germany) and in the financial sector (UK and Thailand). For instance, the 2020 Australian Government's National Blockchain Roadmap ("**Australian Blockchain Roadmap**") identifies the potential to use blockchain along the supply chain in the agricultural sector to reduce frauds, delays, and inefficiencies in the supply chain.[212] Notably, these Surveyed Jurisdictions also contemplate the deployment of such technologies in the public sector, especially for public utilities. Some of these foundational documents also attempt to lay down broad policy principles or goals that need to guide adoption of blockchain technology.

- The 2019 strategy paper by the German Federal Government ("**German Blockchain Strategy Paper**") [213] sets out that any blockchain policy should advance innovation, guarantee financial stability, boost investments, develop a level-playing field for all technologies and be in line with Germany's goals on environmental sustainability and climate protection.[214] The Bangladesh National Strategy stresses that any blockchain deployment must promote innovation, facilitate fair competition, and ensure accountability and

[210] Malta, Italy, Cyprus, China, Gibraltar, France, Liechtenstein, Switzerland, European Union, Singapore, Dubai, Hong Kong, Thailand, UK, Australia, Bangladesh, Germany, Malaysia, Abu Dhabi, and the United States.

[211] Illinois, Arkansas, Nevada, Arizona, Maryland, Delaware, and Vermont.

[212] Department of Industry, Science, Energy and Resources, Australian Government, 'The National Blockchain Roadmap: Progressing Towards a Blockchain-Empowered Future' (2020) <https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf> accessed 16 September 2022.

[213] Federal Ministry of Economic Affairs and Energy, Federal Ministry of Finance, 'Blockchain Strategy of the Federal Government: We Set Out the Course for the Token Economy' (2019) <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3> accessed 16 September 2022.

[214] Federal Ministry of Economic Affairs and Energy, Federal Ministry of Finance, 'Blockchain Strategy of the Federal Government: We Set Out the Course for the Token Economy' (2019) <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3> accessed 16 September 2022.

trust.[215] It also specifies that any policy to adopt blockchain must ensure that the interests of all stakeholders are reflected in such adoption and it protects the interests of the beneficiaries by guaranteeing information security and privacy.

- The 2019 Dubai Blockchain Policy ("**Dubai Policy**") was released by the Dubai Government in pursuance of the Dubai Blockchain Strategy.[216] It sets out the Dubai Government's official guidance on the applicable norms and rules that must guide blockchain deployment in government services or government blockchain use cases.[217] The Dubai Policy recognises ten public policy principles which must guide blockchain adoption. These include promoting accountability and transparency norms, protecting consumer interest, ensuring legislative stability, efficient governance, and securing public safety and security.

- In China, the Supreme Court of China in 2022 and the Ministry of Industry and Information Technology in 2021 released guidance notes on blockchain application in the judiciary and for industrial development respectively. The Supreme Court guidance opinion[218] identifies certain principles for effective implementation of blockchain technology in the judiciary. These include principles such as building blockchain applications which can enable interconnectivity, and which follow robust security standards, and deploying the blockchain solution in line with laws and regulations, etc.[219]

The policy papers also set down the issues which would require further discussion and generally specify the action plan that the Government seeks to implement next for sustainable adoption of blockchain technologies. Notably, a common recommendation in some of the policy papers (Australia, Dubai, Malaysia, Thailand, UK, Hong Kong and Bangladesh) is to develop an appropriate regulatory and policy framework to accommodate the deployment and scaling of blockchain solutions.

- For instance, the Bangladesh National Roadmap identifies lack of legal and regulatory framework and unclear blockchain governance framework as one of the major roadblocks in blockchain adoption and hence, recommends formulating a framework.[220]

- The Australian Blockchain Roadmap and the guidelines published by the Bank of Thailand ("**Thailand Guidelines**")[221] identifies data protection and privacy as the major areas where legal interventions will be

[215] Information and Communication Technology Division, Government of the People's Republic of Bangladesh, 'National Blockchain Strategy: Bangladesh- Pathway to be a Blockchain-enabled Nation' (2020) <https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf> accessed 16 September 2022.

[216] The Dubai Policy specifies that it will come into force the day it is published in the Official Gazette. There might be a possibility that this Policy is converted into law later, however, on a review of publicly available information as of the publication of this Working Paper, we do not have clarity if it has been turned into a law.

[217] Smart Dubai City Office, 'Dubai Blockchain Policy' (2019) <https://www.digitaldubai.ae/docs/default-source/publications/dubai-blockchain-policy.pdf?sfvrsn=4a4bb396_4> accessed 16 September 2022.

[218] The Supreme People's Court of the People's Republic of China, 'Opinions of the Supreme People's Court on Strengthening Blockchain Application in the Judicial Field' (2022) <http://www.chinadaily.com.cn/m/supremepeoplescourt/2022-05/25/content_37550749.htm> accessed 16 September 2022.

[219] The Supreme People's Court of the People's Republic of China, 'Opinions of the Supreme People's Court on Strengthening Blockchain Application in the Judicial Field' (2022) <http://www.chinadaily.com.cn/m/supremepeoplescourt/2022-05/25/content_37550749.htm> accessed 16 September 2022.

[220] Information and Communication Technology Division, Government of the People's Republic of Bangladesh, 'National Blockchain Strategy: Bangladesh- Pathway to be a Blockchain-enabled Nation' (2020) <https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf> accessed 16 September 2022.

[221] Bank of Thailand, 'Guideline for Blockchain Technology Adoption in Financial Services' (2021) <https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2564/ThaiPDF/25640101.pdf> accessed 16 September 2022. We have relied on an unofficial translated version of the Thailand Guidelines.

required.[222] The German Blockchain Strategy also identifies data protection laws and dispute resolution processes as two important legal issues.[223]

- The Dubai Policy lays down a framework for government and private sector entities joining/deploying a government blockchain network[224] or deploying government use cases. The policy sets out guidelines for forming a blockchain network. [225] Notably, although, Abu Dhabi has not yet released a policy paper, it has constituted the Abu Dhabi Blockchain and Virtual Assets Committee ("**ADBVAC**") comprising of stakeholders from the Government and their partners to look into blockchain adoption in Abu Dhabi. The primary objective of ADBVAC is to consult with stakeholders to build a robust regulatory framework which will address legal and governance risks in the areas of AML/CFT, investor protection etc.[226]

Dubai Policy – Key Features

- *Any government entity seeking to form any blockchain network must get approval from the Smart Dubai City Office ("**SDO**") (Article 5).*
- *Network operators must formulate and follow on-boarding and off-boarding procedures to ensure transparency. There should be clear terms and conditions of use that govern the participation in the network (Article 6).*
- *Network operators must notify any new members to the SDO and follow SDO's directions regarding removal of any member or denying membership to any member (Article 6).*
- *Network operators must formulate and maintain a transparent operating model which outlines the roles and responsibilities of the different members, the consensus mechanism to be deployed, the voting structure, revenue generation model and guidance on dispute resolution mechanism (Article 7).*

Source: Dubai Blockchain Policy.

- The Hong Kong Monetary Authority ("**HKMA**") in its whitepaper on DLT ("**HKMA DLT Whitepaper**")[227] highlights specific legal issues such as data protection, competition law, liability, cross-border enforcement etc. for which assessment with existing laws would be required before deploying DLT-based solutions.

- The Thailand Guidelines also sets out certain governance stipulations that a blockchain application must lay down. These include setting down customer on-boarding/off-boarding guidelines, defining roles and responsibilities of different participants, and identifying and implementing robust security standards.[228] The HKMA DLT Whitepaper also identifies similar governance guidelines and further stipulates that there must be guidelines for conflict resolution and risk management.

Legislative Changes

Although blockchain use cases are still being explored and the entire gamut of its potential and associated risks is yet to be seen, some Surveyed Jurisdictions (9) and US States (7) are taking proactive steps to accommodate blockchain applications through legislative changes. Primarily, such changes seek to bring legal certainty and help

[222] Department of Industry, Science, Energy and Resources, Australian Government, 'The National Blockchain Roadmap: Progressing Towards a Blockchain-Empowered Future' (2020) <https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf> accessed 16 September 2022.

[223] Federal Ministry of Economic Affairs and Energy, Federal Ministry of Finance, 'Blockchain Strategy of the Federal Government: We Set Out the Course for the Token Economy' (2019) <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3> accessed 16 September 2022.

[224] Dubai Blockchain Policy, Article (1); Blockchain network is defined as "*a network of entities or devices connected together utilising Blockchain to jointly manage and share a ledger and perform transactions.* "; Use case is defined as "*a series of related interactions between a user and a system that enables the user to achieve a goal.*"; Government is defined as "the Government of Dubai".

[225] Smart Dubai City Office, 'Dubai Blockchain Policy' (2019) <https://www.digitaldubai.ae/docs/default-source/publications/dubai-blockchain-policy.pdf?sfvrsn=4a4bb396_4> accessed 16 September 2022.

[226] Abu Dhabi Government Media Office, 'Abu Dhabi to Launch Blockchain and Virtual Assets Strategy' (2022) <https://www.mediaoffice.abudhabi/en/economy/abu-dhabi-to-launch-blockchain-and-virtual-assets-strategy/ > accessed 16 September 2022.

[227] Hong Kong Monetary Authority, 'Whitepaper 2.0 on Distributed Ledger Technology' (2017) <https://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171024e1.pdf> accessed 16 September 2022.

[228] Bank of Thailand, 'Guideline for Blockchain Technology Adoption in Financial Services' (2021) <https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2564/ThaiPDF/25640101.pdf> accessed 16 September 2022. We have relied on an unofficial translated version of the Thailand Guidelines.

countries to project themselves as blockchain and innovation-friendly jurisdictions to attract investments. There are three dominant approaches that such countries have adopted.

Enacting an Enabling Law or Subordinate Legislation

Some Surveyed Jurisdictions (Malta, Italy, Cyprus, China and Gibraltar) and US states such as Illinois have specifically enacted standalone broad-based laws or subordinate legislations for DLT, which include blockchain use and deployment. These laws focus on developing an enabling framework with safeguards for the sustainable and safe use of blockchain technologies without providing for overly prescriptive legal rules. Safeguards include specifying the activities for which blockchain can be used or it involves establishing oversight mechanisms to monitor the use and functioning of the players involved in providing blockchain services.

In Malta, the Malta Digital Innovation Authority Act, 2018 ("**MDIA Act**") establishes the Malta Digital Innovation Authority ("**MDIA**").[229] MDIA is tasked with promoting governmental policies to promote innovative technology, including DLT and protect the interests of the participants. In this regard, the Malta Technology Arrangements and Services Act, 2018 ("**The Technology Arrangement Act**") seeks to regulate designated innovative technology arrangements ("**ITA**") and designated technology services ("**ITS**") through the MDIA.[230] ITAs include software and architectures used for designing and delivering DLT and smart contracts.[231] ITS refers to review or audit services or technical administration services with reference to ITAs.

Malta - The Technology Arrangement Act: Key Features

- *A software, architecture or smart contract must be recognized by the MDIA under this Act to qualify as an ITA. (Article 5)*
- *ITS providers must also register with the MDIA and are deemed to be fiduciaries with respect to the information they handle on behalf of the customers. (Article 9)*
- *The MDIA can certify the qualities, features, attributes, behaviours or aspects of an ITA as fit for one or more purposes and then issue a certificate which shall state the details of how the ITA is identified, including any public key or brand name. (Article 8)*
- *The MDIA can also stipulate specific requirements for obtaining certificate. These include obligations such as that the ITA needs to be fit and proper, the administrator of any organization which has such ITA needs to be a fit and proper person, and that the software used in the ITA has been reviewed by an independent auditor. (Article 8)*

Source: The Technology Arrangement Act

Similarly, in Gibraltar, the Financial Services (DLT Providers) Regulations, 2020 ("**DLT Regulations**") have been enacted under the Gibraltar Financial Services Act, 2019 ("**GFS Act**"). The DLT Regulations stipulates a licensing regime implemented by the Gibraltar Financial Services Commission ("**GFSC**") for service providers who use DLT to provide storage or to transmit value belonging to others.[232] The DLT Regulations provide a set of 10 regulatory principles that DLT providers[233] need to adhere to as ongoing obligations.[234] These include obligations relating to conducting its business with integrity, honesty, skill, and due diligence.[235] Additionally it must maintain adequate financial resources, have corporate governance mechanisms, security protocols and fraud detection mechanisms.[236] Auditors can audit the functioning of a DLT provider and report any matter of material significance to the GFSC.[237]

In China as well, the Cyberspace Administration of China released regulations on the management of blockchain information ("**China Regulations**") to regulate blockchain information services in 2019.[238] Blockchain information services are defined as services which provide information to the public through blockchain-based applications.[239] The China Regulations lays down guidelines that service providers who provide blockchain information services

[229] Malta Digital Innovation Authority Act 2018.

[230] Innovative Technology Arrangements and Services Act 2018.

[231] Innovative Technology Arrangements and Services Act 2018, sch 2.

[232] Gibraltar Financial Services Act 2019, Part 7, Schedule 2, Para 139; DLT Regulations, Part 2 (1).

[233] DLT provider is an entity who has received the license to carry on DLT business.

[234] DLT Regulations, Part 3 (5).

[235] DLT Regulations, sch.

[236] DLT Regulations, sch.

[237] DLT Regulations, Part 4.

[238] Regulations on the Management of Blockchain Information Services 2019.

[239] China Regulations, art 2.

need to comply with. These include stipulations such as the duty of the service providers to implement information content security management,[240] publish management rules[241], provide the real identity of the users of the blockchain information service[242] etc.

In the US, Illinois has enacted the Illinois Blockchain Technology Act, 2020 ("**Blockchain Act"**) for blockchain and smart contracts. It stipulates the permissible and impermissible uses of blockchain.[243] Illinois has also enacted the Blockchain Business Development Act, 2020, which enables the creation of a facilitative environment for such technologies, without creating any regulatory oversight. Under this Act, the Department of Commerce and Economic Opportunity is mandated to promote blockchain technology and create regulatory frameworks to promote the adoption of the same.[244] In Italy a decree on "Urgent provisions on support and simplification for businesses and the public administration" which has been converted into law provides definitions of DLT and smart contracts. It gives legal recognition to electronic timestamps and the use of DLT to enable the electronic storage of documents.[245] Similarly, in Cyprus a Bill is being considered by the Government which seeks to provide legal recognition to records stored on the blockchain, smart contracts and to accord property status to DLT-based tokens.[246]

Illinois – Blockchain Act

- *The Blockchain Act outlines the permitted uses of blockchain. It gives legal recognition to records and signatures submitted through a blockchain. It also provides that where blockchain is used to create, store, or verify smart contracts, such smart contracts would be legally enforceable and also admissible as evidence in a proceeding. (Section 10)*
- *Instances where blockchain based record will not be permitted will include instances where a law mandates information or contract to be in a specific format, to be displayed or stored in a specific form or when a law requires a contract to be in writing and the blockchain containing such electronic record is not capable of being retained or accurately reproduced later. (Section 15)*
- *Certain types of notices cannot be given through blockchain. These include notices of cancellation of any public service utility, eviction/foreclosure, cancellation/termination of insurance policies and any notice for recalling any product which is hazardous to health and safety. (Section 15)*

Source: Blockchain Act.

Amending Existing Laws

Under this approach, France, and US states such as Arkansas, Nevada, Arizona, Maryland, Delaware and Vermont have amended certain existing laws to recognise blockchain records or accommodate certain use cases of blockchain applications. Primarily, these amendments aim to deal with specific legal aspects of blockchain applications or certain use cases and is not a comprehensive overhaul of laws to account for all legal issues that may emanate from such technologies.

Some US states (such as Arkansas[247], Nevada[248] and Arizona[249]) have amended the Uniform Electronic Transaction Act, 1999 ("**UETA**") to recognise blockchain or smart contracts as legal electronic records.[250] These amendments widen the ambit of "electronic records"[251] to include blockchain based records. The amendments of Arkansas and Arizona also provide for legal recognition to electronic signatures that are secured through

[240] China Regulations, art 5.

[241] China Regulations, art 7.

[242] China Regulations, art 8

[243] Blockchain Technology Act 205 ILCS 730 2020.

[244] Blockchain Business Development Act 205 ILCS 725 2020.

[245] Urgent Provisions on Support and Simplification for Business and the Public Administration 2019.

[246]Bill on the Distributed Ledger Technology Law of 2021 <https://mof.gov.cy/assets/modules/wnp/articles/202109/949/docs/dlt_bill_en_for_public_consultation.docx > accessed 16 September 2022.

[247] Arkansas Code 2019, Title 25, s 25-32-122.

[248] Nevada Revised Statutes 2014, Chapter 719.

[249] Arizona Revised Statutes, Title 44, s 44-7061.

[250] The primary objective of the UETA is to legally recognise electronic documents/records at par with physical documents It stipulates a set of legal rules which governs electronic transactions and use of electronic records. Every state in the US can adopt the UETA and make modifications to it depending on their requirements. See Uniform Electronic Transactions Act 1999.

[251] UETA defines electronic record to mean a record created, generated, sent, communicated, received, or stored by electronic means. UETA s 2(7).

blockchain. They have also made amendments to provide for a definition of smart contract and have conferred legal validity to the same within the UETA.[252]

Vermont has amended its Court Procedure rules to allow digital records registered in a blockchain to be admitted to the court as evidence.[253] It provides for rules of authentication and admissibility such as requirements for filing declarations relating to the details of the record entered into the blockchain.[254] It also stipulates the presumptions that the Court will make with respect to such blockchain-registered digital records. This include presumptions relating to the authenticity of the record, data and time of the records, and the source of the blockchain.[255] Maryland[256] and Delaware[257] have amended their corporation acts to allow certain company records to be stored using blockchain. In France, the French Financial Code has been amended to allow the use of DLT to issue, transfer and deliver security tokens.[258]

Enacting a New Law or Regulation for Specific Use Cases of Blockchain

Under this approach, three Surveyed Jurisdictions (Switzerland, European Union, and Liechtenstein)[259] have enacted specific laws to address particular use cases of blockchain.

In Switzerland, the Federal Government has adopted the Ordinance on the "Adaptation of Federal Law to Developments in Distributed Ledger Technology" ("**Swiss DLT Law**") to recognise DLT securities.[260] These are ledger-based securities which operate only over the securities ledger and are representative of a right.[261] The entry into the securities ledger is akin to certifying the right as a physical security.[262] The focus of the Swiss DLT Law is on the functioning and obligations associated with the securities ledger.

Swiss DLT Law – Key Features

- *There are four requirements that a securities ledger needs to adhere to be classified as a securities ledger. First, providing technological processes which provides the creditor with the right to dispose any DLT security, second, securing integrity of the ledger, third, maintaining transparency by way of recording the rights and functioning associated with the ledger and fourth, providing the creditor the right to inspect and verify the data on the ledger. (Article 973d)*

- *The law governs issuers of the DLT securities. Issuers must disclose and inform any person buying such a DLT security, the functioning of the securities ledger and the technical designs of the issued DLT security. The issuer is held liable for any loss that the buyer bears owing to any misinformation. (Article 973i)*

- *It also introduces DLT trading facilities which are multilateral trading facilities for DLT securities. It needs to obtain a DLT trading license under the Financial Market Infrastructure Act, 2015 and adhere to requirements as specified by the Swiss Federal Government to operate such a facility. (Article 73a)*

Source: Swiss DLT Law.

[252] Arizona has defined smart contracts to mean an event-driven computer program which is executed on a distributed, decentralised, and shared ledger and is capable of automating transactions such as executing directions relating to transfer of assets, see s 44-7061 (E) (2) Arkansas defines a smart contract to mean a business logic that runs on a blockchain and stores execution rules on a shared and replicated ledger to use it to negotiate, verify and execute the terms of a contract, see s 25-32-122 (3)(d).

[253] Vermont Statutes Annotated, 12 V.S.A. s 1913.

[254] Vermont Statutes Annotated, 12 V.S.A. § 1913, s 1913(a)(2).

[255] Vermont Statutes Annotated, 12 V.S.A. § 1913, s 1913 (3).

[256] Morrison Foerster, 'Blockchain Technology Embraced by Maryland Legislature' (2019) <https://www.mofo.com/resources/insights/190501-blockchain-technology-maryland-legislature> accessed 16 September 2022.

[257] Delaware General Corporation Law 2013, s 224.

[258] Decree No. 2018-1226 Relating to the Use of a Shared Electronic Recording Device for the Representation and Transmission of Financial Securities and for the Issue and Sale of Minibonds 2018.

[259] Certain countries such as the European Union are also trying to enact laws regarding cryptoassets which is a specific use case of DLT. Vidhi has earlier written a detailed paper on cryptoassets- Shehnaz Ahmed, Swarna Sengupta, 'A Blueprint of a Law for Regulating Cryptoassets' (*Vidhi Centre for Legal Policy,* January 2022) <https://vidhilegalpolicy.in/wp-content/uploads/2022/01/220127_Blueprint-of-a-Law-for-Regulating-Cryptoassets-1.pdf> accessed 15 September 2022.

[260] Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology 2021.

[261] Swiss DLT Law, art 973d.

[262] Diego Benz and others, 'Ledger-based Securities' (2021) <https://blockchainfederation.ch/wp-content/uploads/2021/10/SBF-2021-01-Ledger_Based_Securities_2021-10-12.pdf> accessed 16 September 2022.

In Liechtenstein, blockchain was increasingly being used to create various tokens, thereby facilitating a token economy.[263] Therefore, it enacted the Token and Trusted Technology Service Provider Act, 2019 ("**Liechtenstein Act**") to provide legal certainty to such tokens and address any risks associated with their use.[264] The Liechtenstein Act aims to regulate tokens[265] and the rights represented through such tokens. It provides recognition to the concept of Trustworthy Technologies ("**TT**") which are technologies which facilitate the assignment and disposal of tokens.[266] TT systems are systems which use TT to provide services of storage and transfer of tokens.[267] Blockchain is a type of TT System.[268]

Liechtenstein Act: Key features

- *Token holders have the right to dispose tokens, cancel tokens and protect any good faith acquisition of tokens from interference by third parties. (Articles 6, 9, 10)*
- *TT service providers are persons who provide services relating to tokens. The Act identifies various TT service providers such as token issuers, TT key depositaries, and TT Exchange Service Provider. TT service providers must register under the Act and the Financial Market Authority ("**FMA**") is identified to be the regulator of TT service providers. (Articles 2, 12)*
- *TT service providers are subject to certain obligations - duty to maintain internal control mechanisms to ensure that token issuers have access to all basic information, and duty to make necessary disclosure to both the FMA and to the general public, duty to maintain minimum capital requirements and to retain records. (Articles 16, 17)*

Source: Liechtenstein Act

Similarly, in 2022, the EU published its regulations on the functioning of DLT market infrastructures ("**EU Regulations**").[269] It recognises 3 kinds of DLT market infrastructure- (a) DLT multi-trading facilities ("**DLT MFs**") which only trades DLT-based financial instrument[270], (b) DLT settlement systems ("**DLT SS**") which records, safekeeps and settles transactions related to DLT financial instruments[271], and (c) DLT trading and settlement systems ("**DLT TSS**") which combines the functions of both the above.[272] It stipulates an authorisation regime for DLT MTFs, DLT SS and DLT TSS wherein they need specific permission to operate.[273] The EU regulations also lay down additional requirements that DLT market infrastructure operators need to adhere to such as establishing business plans, publishing documents on the functioning of the DLT system, implementing operational risk management mechanisms etc.[274]

Clarifying the Applicability of Existing Laws

Two Surveyed Jurisdictions (France and Singapore) have issued guidance documents clarifying the applicability of data protection laws to blockchain technologies.

In France, the Commission Nationale Informatique Libertés ("**CNIL**") (the data protection authority) has clarified how GDPR obligations can be applied to blockchain applications.[275]It has set out guidelines to identify the

[263] Government Principality of Liechtenstein, 'Consultation Launched on Blockchain Act' (2018) <https://www.regierung.li/en/press-releases/212310> accessed 16 September 2022.

[264]Government Principality of Liechtenstein, 'Consultation Launched on Blockchain Act' (2018) <https://www.regierung.li/en/press-releases/212310> accessed 16 September 2022 ; Embassy of the Principality of Liechtenstein, 'Liechtenstein's Parliament Approves Blockchain Act Unanimously' (2020) <http://www.liechtensteinusa.org/article/liechtensteins-parliament-approves-blockchain-act-unanimously> accessed 16 September 2022; Token and Trusted Technology Service Provider Act 2019.

[265] Liechtenstein Act, Article 2 (1)(c); Tokens are defined as a piece of information on a TT system which represents a person's right in rem and can be assigned to one or more TT identifiers.

[266]Token and Trusted Technology Service Provider Act 2019, art 2(1)(d).

[267] Token and Trusted Technology Service Provider Act 2019, art 2(1)(b).

[268] Financial Market Authority, 'TT Service Providers' <https://www.fma-li.li/en/client-protection/safeguarding-client-protection-in-different-sectors/tt-service-providers.html> accessed 16 September 2022.

[269] Regulation on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology and Amending Regulations (EU) No 600/2014 and (EU) No909/2014 and Directive 2014/65/EU, 2022.

[270] EU Regulations, art 2(6).

[271] EU Regulations, art 2(7).

[272] EU Regulations, art 2(10).

[273] EU Regulations, art 8, 9, 10.

[274] EU Regulations, art 7.

[275] Commission Nationale Informatique Libertés, 'Blockchain : Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (2018) <https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf> accessed 15 September 2022.

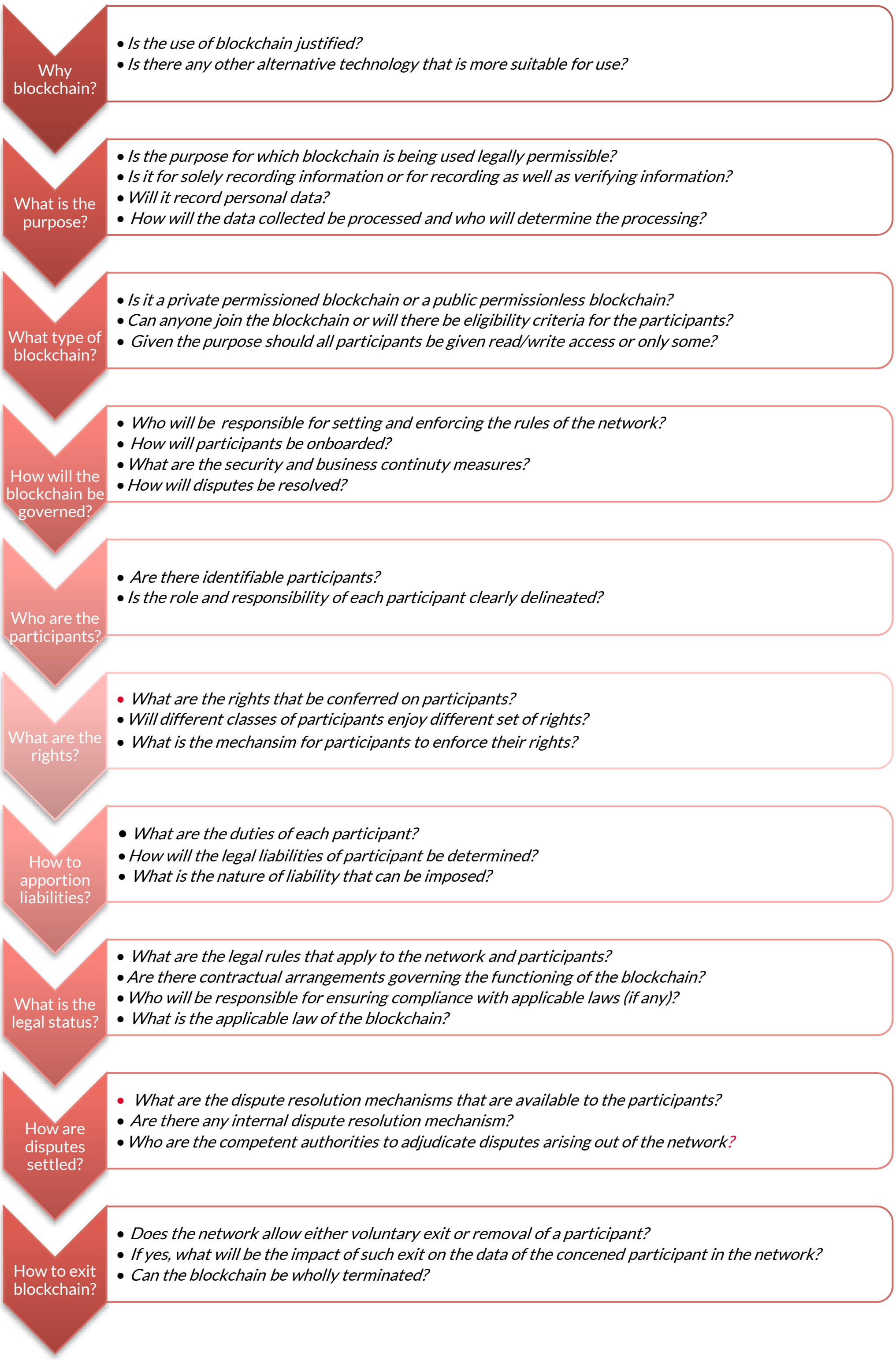
controller and processor in a blockchain network. The CNIL states that a participant would be identified as a controller if it is a natural person, and the processing of personal data is done by such a participant in relation to a professional or commercial activity. A participant can also be a controller if it is a legal person and registers personal data onto the blockchain. If a group of participants are carrying out processing activities, then either they should designate the controllers and, in the absence of the same, they will all be deemed to be joint controllers as per Article 26 of the GDPR. The CNIL states that either the smart contract developer or the miners who validate transactions involving personal data will be identified as processors. The CNIL also provides recommendations on risk minimisation during blockchain processing of personal data. CNIL recommends an examination of whether blockchain processing of personal data is necessary and if not, exploring other solutions that may be adopted. It clarifies that how personal data is stored will also inform the risk assessment of blockchain. In terms of GDPR rights conferred on data subjects, the CNIL notes that while some rights such as the right to access are compatible with blockchain, rights such as the right of erasure and right to rectification cannot feasibly be exercised in a blockchain. Thus, it recommends that controllers should choose appropriate blockchain designs to enable data subjects to exercise such rights as much as possible. For instance, if the controller chooses to record the personal data using a hash-key function, it can make certain data inaccessible to view by others which would come close to fulfilling the right of erasure.

In Singapore, the Personal Data Protection Commission's ("**PDPC**") guidance paper ("**PDPC Guidance Paper**") lays down recommendations on how blockchain applications can be designed to comply with Singapore's Personal Data Protection Act ("**PDPA**").[276] The guidance paper makes a distinction between the data protection norms that can be made applicable to permissioned blockchains versus those that can be made applicable to permissionless blockchains. For permissionless blockchains, since it is impossible to pinpoint a central controller, PDPC recommends that such blockchains should not be used to store any personal data or for any activity which would entail storing personal data. On the other hand, for permissioned blockchains, it recommends that personal data which is stored on the blockchain must be encrypted and anonymised with limited access to only authorised participants for a specific purpose. The blockchain operators should also formulate and enforce PDPA obligations contractually by stipulating guidelines that controllers or intermediaries need to adhere to. Significantly, the paper recommends that for blockchains handling personal data, the operators should implement a Data Protection Management Programme ("**DPMP**"). The DPMP would entail- (a) establishing an oversight committee; (b) designating a Data Protection Officer from each participating organization who would be responsible for overseeing whether such organization is complying with the PDPA; (c) formulating policies which clearly stipulate the roles and responsibilities of each participant; (d) conducting regular data protection impact assessment to identify any risk points in the blockchain processing and mitigating the same; and (e) undertaking regular reviews of the data protection practices implemented to ensure they are in line with the current best practices.

[276] Personal Data Protection Commission Singapore, 'Guide on Personal Data Protection Considerations for Blockchain Design' (2022) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Blockchain-Guide_final.ashx?la=en> accessed 16 September 2022.

VI. The Foundation and Contours of a Blockchain Governance Framework

Blockchain can help in unlocking efficiencies and provide novel solutions to erstwhile legacy problems. However, there are legal issues that may confront blockchain's use and adoption and render it a challenge. Therefore, any implementation of blockchain applications should be grounded in a comprehensive and robust governance framework which will guide the operation of the application. Such a framework needs to create an enabling environment and should account for the legal risks and challenges to counter the same. The framework will bring about certainty regarding the operation of the blockchain and therefore, incentivise the scaling of blockchain applications. The



Why blockchain?

- *Is the use of blockchain justified?*
- *Is there any other alternative technology that is more suitable for use?*

What is the purpose?

- *Is the purpose for which blockchain is being used legally permissible?*
- *Is it for solely recording information or for recording as well as verifying information?*
- *Will it record personal data?*
- *How will the data collected be processed and who will determine the processing?*

What type of blockchain?

- *Is it a private permissioned blockchain or a public permissionless blockchain?*
- *Can anyone join the blockchain or will there be eligibility criteria for the participants?*
- *Given the purpose should all participants be given read/write access or only some?*

How will the blockchain be governed?

- *Who will be responsible for setting and enforcing the rules of the network?*
- *How will participants be onboarded?*
- *What are the security and business continuty measures?*
- *How will disputes be resolved?*

Who are the participants?

- *Are there identifiable participants?*
- *Is the role and responsibility of each participant clearly delineated?*

What are the rights?

- *What are the rights that be conferred on participants?*
- *Will different classes of participants enjoy different set of rights?*
- *What is the mechansim for participants to enforce their rights?*

How to apportion liabilities?

- *What are the duties of each participant?*
- *How will the legal liabilities of participant be determined?*
- *What is the nature of liability that can be imposed?*

What is the legal status?

- *What are the legal rules that apply to the network and participants?*
- *Are there contractual arrangements governing the functioning of the blockchain?*
- *Who will be responsible for ensuring compliance with applicable laws (if any)?*
- *What is the applicable law of the blockchain?*

How are disputes settled?

- *What are the dispute resolution mechanisms that are available to the participants?*
- *Are there any internal dispute resolution mechanism?*
- *Who are the competent authorities to adjudicate disputes arising out of the network?*

How to exit blockchain?

- *Does the network allow either voluntary exit or removal of a participant?*
- *If yes, what will be the impact of such exit on the data of the concened participant in the network?*
- *Can the blockchain be wholly terminated?*

governance framework itself needs to be based on certain foundational principles which will form the base of any blockchain governance design. The foundational principles along with the governance framework will act as the baseline to ensure the rights of the various participants are protected and the operation of the blockchain is carried out legitimately and in a safe and sustained manner.

The formulation of a governance framework involves the participants to make a variety of choices and decisions, starting with whether the use of blockchain for that specific purpose and in that specific sector is desirable and feasible. The type of blockchain also plays a huge role in determining the kind of specifications that can be workable in the governance framework. Permissioned blockchains will enable the imposition of more control and supervision than permissionless blockchains. Hence, various contours of the blockchain governance framework will only be applicable if a permissioned blockchain is chosen. A snapshot of the various decisions that need to be undertaken by participants while adopting a blockchain application or while participating in a blockchain network is provided below.

Foundational Principles | Blockchain Governance Framework

These principles have been culled out basis the specific characteristics of and risks blockchain poses. The principles of transparency and accountability are important because of the decentralised and distributed nature of blockchain which makes it difficult for participants to understand the functioning of the blockchain network and to identify the responsible parties. The principle of legitimacy is important to ensure that blockchain applications are legally recognised and the rights of the participants are legally protected. The principle of data governance and security is crucial to ensure that any processing of personal data by the blockchain application is carried out within a robust and comprehensive data protection and security framework.

Principle of Transparency

All participants must have the right to information regarding the governance structure, rights, duties, and powers of each participant, functioning and processes of the blockchain network.

This enables participants to make informed decisions and provide informed consent to join a blockchain network.

It also ensures that there are accountability mechanisms in the functioning of the blockchain application.

Principle of Legitimacy

This involves examination of two issues: (a) whether the use of blockchain for the stated objective is legitimate under applicable laws; and (b) the legitimacy and reliability of the data stored on the system.

If the use case is not grounded in legal principles, rights and obligations of participants do not have a legal backing, leaving users without any legal recourse in case of any malfunctioning.

Further, there must be processes to ensure that information in the system is accurate, updated, and verifiable and processed in accordance with law.

Principle of Accountability

Blockchain system must have rules to govern functioning and obligations of participants.

There must be mechanisms to attribute liability, determine the nature and consequence of liability and provide recourses to participants in case of breach.

This is necessary to ensure compliance with both legal rules and contractual obligations.

Principle of Data Governance & Security

If blockchain systems process personal data, there must be robust data governance mechanisms, in accordance with domestic and internationally recognised standards of data protection.

This also involves establishing mechanisms to ensure that participants can own and manage their own data. This entails employing interoperable systems which would enable participants to port their data across blockchain systems.

The principle of security means that blockchain network also has security measures to protect data stored on the system.

Incorporating the Foundational Principles in the Governance Framework

Principle of Transparency

What is the governance structure employed on the blockchain network?

What are the different rights, powers, and obligations of each participant?

Which participants can read or access the information stored in the blockchain?

What is the process of arriving at consensus within the blockchain?

Are the participants made aware of the risks and benefits of using the blockchain-based service?

Principle of Legitimacy

What is the legal certainty of the use of blockchain and smart contracts for the stated purpose?

How are the rights and liabilities of participants protected?

What is the information stored on the blockchain?

Is the information accurate and verifiable?

Who can write or validate data in the blockchain?

What are the security measures that have been implemented in the blockchain?

Principle of Accountability

How is liability determined for any loss of data or malfunctioning of the system?

What are the recourses available to a participant?

How does the blockchain ensure compliance with legal standards?

What are the mechanisms to assure the quality of service between participants?

Are dispute resolution mechanisms clearly defined?

What are the mechanisms to monitor compliance with rules?

Principle of Data Governance &

Does the blockchain system process personal data? If yes, does the system account for data protection laws and recognised standards?

What processes and standards are incorporated for protecting privacy and confidential information?

Does the system have mechanisms to address security vulnerabilities?

What are the risk mitigation strategies, including business continuity measures that the system employs?

Does the system have mechanisms to ensure interoperability?

Contours of the Governance Framework

Basis the principles, the Working Paper presents the quintessential terms of use which should accompany the adoption and operation of any blockchain application. The Working Paper interprets the governance framework of a blockchain network as the minimum baseline governance standards which would guide the functioning of a blockchain network throughout its lifetime. However, it is important to note that most of these contours will depend on the type of blockchain and the entities involved. Most of these standards will be easily implementable and feasible for permissioned and private blockchains rather than permissionless and public blockchains.

Objective of the Blockchain Network

Adopting blockchain technology for a stated objective is a strategic decision that must be undertaken after a due consideration of the pros and cons of using the technology for the stated objective. This stipulation would be akin to the objects clause of a company as provided in its charter documents. Clear identification of the objective is necessary to assess the activities that the blockchain network will have to undertake for achieving the objective. It also ensures that participants at the time of joining are aware of the purpose of the blockchain and what kind of data they are expected to provide to facilitate the same. Incorporating specific objectives also provide guidance to the whole network and all the participants on what is the permissible scope and activities so that any deviation from the stated objectives can be easily detected.

1. *The governance framework must clearly stipulate the objective of the blockchain network. This will also involve setting out the primary activities that the network will undertake to meet the stated objective.*

2. *For instance, a blockchain network set up to integrate information about the supply chain of a particular sector, may involve storing sensitive financial information of vendors and other personal details of the suppliers and vendors to facilitate payments and verification. Here, the governance framework must stipulate along with its primary*

objective of recording supply chain information, that it would collect certain categories of personal information to facilitate the stated objective.

Legal Recognition of the Blockchain

Before commencing with the operation of the blockchain network, participants must undertake an assessment of whether blockchain-based records or the smart contracts (if any) so deployed on the blockchain network are legally recognised and legally permissible under the existing laws and to ensure that there is no prohibition. This would be necessary to establish and ensure the legitimacy and legal validity of the blockchain network and also determine regulatory compliances.

1. *Examine if the laws of a particular jurisdiction within which the blockchain network is operating legally recognises blockchain-based records and smart contracts. For instance, in India assessment needs to be undertaken under laws such as the IT Act, Evidence Act and stamp laws to assess if it accommodates blockchain-based records.*

2. *Assessment under sectoral laws also needs to be undertaken for blockchain networks operating in specific sectors, to check for the legal recognition of blockchain under those specific laws.*

Legal Structure for Governing Blockchain

Blockchain applications primarily operate between multiple players and stakeholders with the aim of creating and deploying industry-wide solutions and efficiencies.[277] To support the development and use of such blockchain applications, collaborations between stakeholders need to have legal certainty.[278] This requires such collaborations to be formally organised, failing which it may expose the entire network to unlimited liability for any wrongdoing by any of the participants. A clear legal structure is also useful to document the legal relationship amongst the participants and between the participants and the blockchain network itself. Having a legal structure is also important to enable the blockchain network to interact with third parties who will otherwise be hesitant in interacting with it if the governance structure, legal relationship, and legal status as relating to the participants and the blockchain network is not clarified.

The legal structure of such blockchain arrangements can be examined at two levels – first is the legal structure of the entity or entities that deploy or promote the blockchain; and the second is the legal structure governing the relationship between promoters and participants and also between participants inter se. The legal structure will depend on many factors, including commercial legal and taxation considerations.[279] For instance, a blockchain application may be provided by the government, its agencies, a company, consortium of industry players or through public-private partnerships. Each of these promoter entities may choose to adopt a legal structure suitable to its needs, which may include joint venture agreements, developer agreements or setting up a new legal entity. Choice of legal structures will also include different contractual arrangements wherein the relationship and governance of the blockchain network are promulgated by way of legally enforceable contracts between the participants.[280]

1. *Legal structure of blockchain arrangements must be clearly examined and set out at two levels – (a) structure of the entity or a group of entities collaborating to develop and promote blockchain; and (b) structure to govern the relationship between such promoters and participants and between participants inter se.*

[277] World Economic Forum,'Redesigning Trust: Blockchain Deployment Toolkit'(2020)<https://bit.ly/3VRB6TW>accessed 15 September 2022.

[278] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit'(2020)<https://bit.ly/3VRB6TW>accessed 15 September 2022.

[279] Rob Massey and others, 'Governance and Structuring Considerations in Blockchain Consortia' (2020) <https://bit.ly/3HxIpfm> accessed 16 September 2022.

[280] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://bit.ly/3VRB6TW> accessed 15 September 2022.

2. *Typically, such structuring is governed by contractual arrangements, which should stipulate rights, obligations, and liabilities (in case of default) by participants.*

3. *If a blockchain arrangement is governed through contracts, it must be clarified if there is an overarching contract common to all participants or if there are separate contracts that will be negotiated with individual participants.*

Eligibility Criteria for Participants

The eligibility criteria will be relevant for private and permissioned blockchain, where the objective is to limit the network to specific individuals. In such cases, the framework must lay down the eligibility criteria or the conditions that must be satisfied by an entity to become a part of the network. For deployment of blockchain applications in certain sectors, it is critical to set out such eligibility criteria. For instance, in the financial sector, participants may have to meet prudential requirements, and be required to submit information about their financial health, management, and risk management strategies. Here, eligibility conditions have to be designed keeping in mind specific requirements of the sector. Having a specific set of eligibility criteria also ensures that if there are any legal preconditions relating to the sector where the blockchain operates, those are met by the joining participants. In a public permissionless blockchain regardless of specifying conditions, monitoring the entry of the participants is difficult since by design it is open to all.

1. *In most private and permissioned blockchain systems, the governance framework must clearly set out the eligibility criteria for participants to join the network.*

2. *The eligibility criteria must be objective to ensure that the network is not biased against similarly placed prospective participants.*

3. *In certain sectors, the blockchain network may require prospective participants to undergo a verification process, where such applicants are required to submit specified information, including personal information. While such a mechanism may not be in line with the pseudo-anonymity features of blockchains, such information and verification procedures may be critical for highly regulated sectors. Such a mechanism is also useful to carry out enforcement action against any rogue participant.*

Identifying and Enumerating the Role of each Participant

The presence of multiple participants in a blockchain network may give rise to potentially competing and conflicting interests. There may be participants who are incentivised to influence the network in a manner that it functions to propagate their business or commercial interests. In some cases, certain participants may be inclined to prioritise financial returns from the network over the quality of services. To ensure that such competing interests do not hamper the smooth functioning of the network, it is important for the governance framework to identify and delineate the role of each participant.

1. *The governance framework must identify the different types of participants within the blockchain network. This will include identifying the developers, administrators, and users.*

2. *It is also crucial to identify the participants who will collect and process data within the blockchain. Such identification is necessary especially for compliance with data protection laws which imposes obligations on controllers and processors.*

3. *Upon identification of the different categories of participants, the role of each participant within the network must be clearly delineated. For instance, a node identified as the developer may be responsible for the maintenance and functioning of the blockchain code and infrastructure. It may or may not be part of the administrative or*

management structure of the blockchain, but access wise such a blockchain developer node may have administrator access and would ideally be able to edit, read and verify transactions on a blockchain.

4. *Having such clearly specified roles ensures that there is no confusion or overlap in between the duties of the participants. Even if a participant has been conferred with multiple roles, the same must be stipulated.*

Terms and Conditions of Participation

Once participants join a blockchain network, the governance framework must set out clear terms and conditions ("**T&Cs**") governing their participation in the network. The T&Cs will vary depending on the purpose of the blockchain as well as the industry in which such blockchain operates. Since blockchain operates over multiple layers of distributed networks with each participant operating their independent nodes, such written T&Cs in a governance framework will help in setting the minimum standards that must be complied with by an otherwise disparate ecosystem. The T&Cs primarily act as a set of representations and warranties that each participant undertakes to meet at all times during their tenure in the blockchain network. It also facilitates trust within the blockchain ecosystem because it assures each participant of their co-participant's compliance with relevant obligations. Regardless of the legal structure of the blockchain arrangement, specifying such T&Cs are essential to ensure that the functioning of the blockchain is being carried out in a legally compliant manner and this new form of arrangement is not being used to subvert the law.

1. *The governance framework must stipulate the T&Cs governing the participation of the participants to the network.*

2. *This may include conditions relating to disclosure norms, compliance with applicable laws, maintenance of specified security standards, risk mitigation strategies and requirements for inspection and audit to ensure that participants are complying with network rules and T&Cs.*

3. *T&Cs may also set out conditions for smooth operational functioning of the blockchain, such as requirements to maintain updated and compatible versions of software necessary to facilitate transactions on the blockchain.*

4. *In the case of blockchain solutions in regulated sectors, the T&Cs must ideally contain the legal obligations required to be met by participants in the specific sector with regard to the specific activities that the blockchain network undertakes. This is necessary to ensure that the blockchain solution is carried out in a legally compliant manner and this arrangement is not used to subvert the law. For instance, in the case of a blockchain network collating and processing personal information of end users, the T&Cs may require entities designated as controllers and processors within the network to maintain data governance standards and security measures as enumerated in the applicable law. Similarly, if the blockchain operates in a regulated sector wherein players of such a market require licenses and authorisations to carry out their functions, the T&Cs should encapsulate that such participants need to obtain and keep updated their authorisations for joining the network and their continued participation.*

Rights of Participants

Specifying rights of participants is necessary to ensure that participants can interact with the blockchain ecosystem with legal certainty and legitimacy. The blockchain arrangement being a legal relationship, it is critical that participants are given rights and these rights can be exercised freely.

1. *The governance framework must lay out the rights of each participant to provide legal certainty and legitimacy to interactions of participants with the network and inter-se.*

2. *While some rights may be common to all, certain rights may vary depending on the category of the participant.*

- *For instance, participants that are designated as controllers and processors in accordance with applicable data protection laws may be conferred with rights to lawfully collect and process data in accordance with the objective of the network.*

- *Similarly, participants whose personal information is collected or processed by the network must be conferred with rights based on well-recognised data protection principles such as the right to access their personal information, right to update their information, right to port their data, etc.*

3. *Similarly, rights of participants vis-à-vis accessing, editing, updating information on the ledger, amending existing rules of the network and whether they have a right to reverse transactions done on the network, must be stipulated.*

Duties and Liabilities of Participants

As a natural corollary to the rights conferred on participants, the governance framework must set out the duties and liabilities of such participants. This will enable participants to guide their actions and interactions within the blockchain, failing which, such arrangements may leave scope for the exercise of discretionary powers and ad-hoc governance without any checks and balances. The stipulation of duties is also important to establish what instances would attract liability.

1. *The governance framework must also set out provisions for determining the rights and duties of the participants.*

2. *Like rights, the duties may vary depending on the category of the participant.*

- *For instance, administrators may have the duty to ensure that there is no wrongful or illegal transmission of data over the network, and that decisions within the network are carried out in accordance with rules of the network. In case, where such administrator is designated as a "controller" or "processor" it will have the duty to ensure that any collection and processing of personal data is in compliance with existing laws and internationally recognised data governance standards.*

- *Similarly, the governance framework may require a blockchain developer to maintain the infrastructure and code in accordance with internationally recognised data and security standards.*

- *Blockchain users will have the duty to maintain the confidentiality of information shared within the network as may be stipulated in the governance framework and to comply with T&Cs.*

3. *The governance framework must also specify the liability that will be attracted if a participant defaults in complying with its duties. This may involve specifying the nature of sanctions that the network may impose on defaulting members, which can include monetary penalty or suspension or removal from the network itself.*

4. *There may be provisions on exclusion or exemption from liability. In case of administrators, the governance framework may consider providing safe harbour*

protection (exemption from liability) for publication of illegal / unauathorised content on the blockchain network, if such content was not under the control of the administrator and if the administrator has taken all the necessary due diligence to carry out its functions in accordance with the rules of the network.

5. *Although specific participants will have specific duties which will, therefore, attract different liabilities, realistically, it may be challenging to identify all the participants in every type of blockchain network. In this scenario, the first point of regulatory supervision or for satisfaction of contractual obligations and claims may be the customer-facing interfaces of the blockchain network such as the external gateways.*

Operating Procedures

Operating procedures set out how a blockchain network will function by helping in mapping the chain of governance and management of the blockchain network. It will clarify how key operating decisions will be taken within the network. Further, it should also specify the source of funding for the network and the revenue allocation to ensure transparency. The role of the participants in taking decisions relating to the network as well as their role in revenue generation may also be specified.

1. *The governance framework must specify the operating procedures that will govern the functioning and management of the blockchain network. This will include specifying procedure relating to the following:*

(a) Identifying relevant categories of participants who will vote and on what matters.

(b) Manner of voting by participants and counting votes. This may be linked to the consensus mechanism and the number of participants.

(c) Requirements for participants to contribute monetarily to the development of the network (if any).

(d) Determining revenue allocation from the network to the participants, including revenue (if any) from IP of the blockchain.

Ownership of IP

Broadly, a blockchain network will consist of the back end blockchain software and the user-facing technological interface (such as an app) or the blockchain solution. Typically, the blockchain software may be a pre-existing software used by the developer to service multiple clients and the user-facing interface will be the bespoke software developed by the developer to meet the stated objective of the blockchain solution.[281] Issues relating to ownership and licensing of the IP in the blockchain software and the bespoke blockchain application is an important commercial consideration for participants. Establishing clearly who the owner of the IP is will enable the delineation of the specific rights that the participants have with respect to the IP protected material of the blockchain and the permitted scope of use of the same. These issues will depend on who brings what kind of IP to the solution and whether such IP needs to be licensed to participants to operationalise the blockchain application.

1. *The governance framework must clearly identify the IP in the technology which forms the basis of the blockchain application as well as the IP in the application itself.*

[281] See Tech London Advocates' Blockchain Legal and Regulatory Group, 'Blockchain: Legal and Regulatory Guidance' (*The Law Society*, 2020) p 128 < https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report> accessed 15 September 2022.

2. *The governance framework must also clearly state who owns such IP, and how it may be shared. This may also require contractual arrangements to license (including the terms of license) IP to relevant users for the smooth functioning of the blockchain application.*

3. *Clarity on these issues is important to identify the owner and licensee of IP in the technologies, rights of such entities and the permissible scope of use. This is necessary to identify if there is any unauthorised use of the IP.*

4. *There may be instances where IP in underlying technologies is owned by specific participants. Such participants and the nature of IP that they are contributing must be identified. This is important to design licensing arrangements for such IP to be licensed to the network or other participants, as may be suitable.*

5. *Further, the governance framework must either clearly stipulate or lay down a mechanism to identify who would be the IP owner if the initial IP used to build the technology is enhanced by the blockchain network as part of building the solution.*

6. *There may also be instances where the blockchain application uses IP of third-party service providers in which case, the terms of use must be specified in the governance framework.*

7. *The governance framework must also lay down if there is any scope for commercial licensing of the IP in the blockchain solution to third parties and the mechanism to license the same.*

Data Governance Standards: Protecting Privacy and Confidentiality

The very functioning of blockchain hinges on the use of data. Therefore, it calls for mechanisms to manage and protect such data as per applicable laws and well-recognised standards. One of the first tasks is to evaluate the nature of data being collected and processed by the network. Second, the treatment of such data must be specified. Typically, in the case of personal data, data protection laws may get triggered. For other kinds of confidential information, especially sensitive commercial information, participants may desire that the network implements measures to protect the confidentiality of such information. Therefore, it is important to have clearly set out policies to govern the data collection and processing.

1. *The governance framework must clearly stipulate the nature of information / data that the network will collect and process. For instance, this could include personal information (such as name, address, financial information of individuals), login information (such as IP address, device information, operating system) or commercial information (such as information about the turnover, vendors, clients of a company).*

2. *The next step is to identify and disclose if all participants or selected participants will have access to all information and the extent of access to such information.*

3. *The third step is to outline all the measures, processes and standards that will govern the collection, storage, and use of such data.*

4. *It is also important to examine if all such data will be on-chain, or only a subset of such data. If any data is stored off-chain, the governing framework must outline the privacy protections that are employed.*

5. *Any entity or entities that use blockchain technology when collecting or processing personal data should examine their accountability under existing laws, including the role of any service providers that they engage.*

6. *In the event data protection laws are triggered, it is important that the governance framework clearly identify the 'controllers" and "processors" and set out their respective roles under such laws.*

7. *For networks that store, collect or process personal data, there must be a privacy policy setting out the manner of collecting, storing, and processing such data. This must also include specifying the grounds for collecting and processing data, time frame for and extent of storing data, grounds for sharing data, and identification of grievance redressal mechanism for any breach of the policy.*

8. *For blockchain networks that will trigger data protection laws, it is important to weigh the benefits and risk of opting for a public permissionless blockchain and a private permissioned blockchain. Opting for a blockchain architecture closer to a private permissioned blockchain may be useful to follow consistent data privacy practices and comply with applicable laws. Such an architecture can employ various structures and processes to authorise approved participants, ensure such participants follow strict practices for better data privacy and implement such technical measures to regulate the personal data that participants process on the network.*[282]

9. *For data that qualifies for protection under data protection laws, applicable laws and the privacy policy will protect such data. However, as discussed, the network may also have access to other confidential information (such as sensitive commercial information). In such cases, the governance framework may identify such data that requires to be protected under a confidentiality clause and enumerate how such confidentiality clauses will protect the data.*

10. *It may be useful to set up an oversight committee consisting of specified participants to ensure that the network adheres to such data governance and protection standards.*

11. *Periodical audit of data security and protection standards must be undertaken to ensure compliance with applicable law and well-recognised standards and identify risks, which may require intervention.*

Risk Management

Similar to any other business organisation, the blockchain network is also susceptible to suffering from operational risks i.e. "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."[283] For blockchain networks, this could include risks and losses arising from system failures, sudden downtimes, security breaches or data theft. Therefore, it is important to establish and operationalise a risk management framework to protect against such losses and ensure that there is business continuity.

1. *The governance framework should have a mechanism to identify, assess, monitor, and mitigate operational risks.*

2. *Formulating a risk management mechanism could include:*

[282] Pritesh Shah, Daniel Forester, Carolin Raspe, 'Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies' (*Practical Law,* 2019) <https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf> accessed 15 September 2022.

[283] This was in the context of capital marked under Basel II Framework, see Basel Committee on Banking Supervision, 'International Convergence of Capital Measurement and Capital Standards: A Revised Framework' (2006) <https://www.bis.org/publ/bcbs128.pdf> accessed 16 September 2022.

(a) *identifying and implementing apposite cybersecurity standards and measures (such as having backup archival storage, software safeguards etc.);*[284]

(b) *identifying and implementing data standards to ensure that there is no data loss owing to non-uniform data formats and data storage processes.*[285]

(c) *Outlining an audit mechanism of the blockchain system which would enable the detection and monitoring of any operational risks.*

3. *Once processes relating to preventing or assessing operational risks have been identified, the risk management framework should also specify the steps to be undertaken in case loss does occur and the steps that must be taken to mitigate the same. This would be in the form of establishing business continuity and disaster recovery plans, which include implementing processes to address any business disruption or loss of critical infrastructure.*[286] *These plans could include adopting technical measures such as having a backup or alternate software, or facilitating private key regeneration in the event of a security breach etc.*[287]

Exit Mechanism

Blockchain networks are generally voluntary networks wherein participants join at their will. Therefore, it is imperative that the network has a mechanism to allow participants to exit the network. This is particularly important for private permissioned blockchain where entry to and participation in the network is regulated. Since blockchain operates over a network of peer nodes and data provided thereon, if proper control mechanisms are not instituted for such exit, then participants will be able to leave the network in an ad-hoc manner which would severely impinge the functioning of the blockchain, and the data contained thereon.[288]

1. *The governance framework should specify the mechanism and process for participants to exit a blockchain network and the consequences of such exit on the functioning of the blockchain to ensure that the integrity of the network is not hampered.*

2. *In terms of process, the governing framework may specify the following:*

(a) *Form in which exit request needs to be made and to whom such requests should be made.*

(b) *The manner of sanctioning the exit.*

(c) *Timeline for withdrawing access to the concerned participant submitting the request.*

3. *The governing framework should specify how the data of the exiting participant is to be managed. Typically, a participant exiting the blockchain may not want their data to be permanently retained by the blockchain. However, this brings the question of whether such data is removable from the blockchain as blockchain is by default immutable. This*

[284] Lory Kehoe and others, 'Six Control Principles for Financial Services Blockchain' (*Deloitte,* October 2017) <https://www2.deloitte.com/de/de/pages/financial-services/articles/blockchain-control-principles-in-financial-services.html> accessed 16 September 2022.

[285] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

[286] Ian Storkey, 'Operational Ris Management and Business Continuity Planning for Modern State Treasuries' (2011) International Monetary Fund Technical Note <https://www.imf.org/external/pubs/ft/tnm/2011/tnm1105.pdf> accessed 16 September 2022; Lory Kehoe and others, 'Six Control Principles for Financial Services Blockchain' (*Deloitte,* October 2017) <https://www2.deloitte.com/de/de/pages/financial-services/articles/blockchain-control-principles-in-financial-services.html> accessed 16 September 2022.

[287] Lory Kehoe and others, 'Six Control Principles for Financial Services Blockchain' (*Deloitte,* October 2017) <https://www2.deloitte.com/de/de/pages/financial-services/articles/blockchain-control-principles-in-financial-services.html> accessed 16 September 2022.

[288] KPMG International, 'Realising Blockchain's Potential: Introducing KPMG Blockchain Technology Risk Assessment Solution' (2018) <https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/09/realizing-blockchains-potential.pdf> accessed 16 September 2022.

will require the network to first select and employ apposite technologies[289] *that would enable the selective removal of blockchain stored data without breaking the consistency of the blockchain.*

4. *The management of the exiting participant's data would also involve specifying how the exiting participant may have access to the data that was stored on the blockchain, upon their exit.*[290]

5. *The governance framework should also specify the extent of data that will be retained by the network of the exiting participant and the purpose of such retention (such as for complying with future legal summons or to maintain the integrity of the blockchain history).*

6. *Further, the governance framework can also lay down exit formalities that the exiting participant needs to comply with. For instance, this could entail signing confidentiality agreements or relinquishing any IP materials or IP licenses relating to the blockchain network.*

Removal of Participants

It is important to explicitly specify the grounds leading to the removal of participants from the blockchain network. These instances need to be objective to avoid any scope for dispute or arbitrary action. This is because the removal of participants may necessitate adjudication or reasoned decision-making calling for more advanced considerations. [291]

1. *The governance framework must specify the objective grounds on the basis of which participants may be removed from the network and the participants of the network who can participate in the decision-making process regarding removal.*

2. *The impact of such removal on the network and its processes must also be outlined. For instance, the governance framework may specify how an expelled participant's access to the network will be restricted, treatment of the data of such participant, intimating other participants about such removal, and its impact on ongoing transactions with other participants or third parties etc.*[292]

3. *Decisions may also have to be taken regarding the extent of the data of the expelled participant that can and should be retained on the blockchain network for potential legal action in the future.*

4. *The governing framework should also stipulate the process for removal / expulsion. Since the blockchain arrangement is a legal relationship, any removal of a participant as a form of a sanction should follow due process. This could include stipulating notice requirements to the concerned participant and providing a reasonable opportunity to present their case or to be heard. It could also prescribe a tiered process wherein the*

[289] For instance one technology which has been developed to facilitate the partial removal of blockchain data is- Ali Dorri, Salil S. Kanhere, Raja Jurdak 'MOF-BC A Memory Optimized and Flexible Blockchain for Large Scale Networks' 92 Future Computer Generation Systems 357 <https://www.sciencedirect.com/science/article/abs/pii/S0167739X17329552> accessed 16 September 2022.

[290] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

[291] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

[292] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

concerned participant is given time to comply with the breached conditions and if they are not able to comply within such time, they are removed.

Jurisdictional Stipulations

The participating nodes in a blockchain can be spread across multiple places, raising challenges regarding the determination of the relevant jurisdiction whose law will apply to the network and its participants. Arguably, every jurisdiction which has a node would be able to exercise jurisdiction. However, there may be instances where none of the jurisdictions in which nodes are situated has sufficient nexus to establish jurisdiction. Such situations could lead to overregulation or under-regulation, both of which is not desirable. The lack of clarity on the jurisdictional scope of the blockchain network would severely undermine dispute resolution processes and enforcement.

1. *The governance framework must stipulate the jurisdiction that will be applicable to the network and govern the relationship between the participants. These stipulations are important for blockchain systems operating across borders or inter-state.*

2. *Jurisdiction stipulations will first include identifying the jurisdictions' law that will govern the functioning of the blockchain and the relationship of the participants. This is necessary to bring legal certainty, to provide legitimacy to the blockchain application and will help in enforcing legal obligations and adjudicating violations of governing rules of the blockchain.*

3. *Specifying the applicable law will help bring predictability to the functioning of the network and the participants as it will ensure that they do not need to comply with multiple conflicting laws.*

4. *The governance framework could also specify the forum in which any blockchain related dispute can be adjudicated. Since blockchain is decentralised, it often becomes difficult especially in the context of public permissionless blockchains to determine which country's court of law will have jurisdiction over the dispute and based on what will such jurisdiction be exercised. If the desired forum is specified, then it would ensure that there is no conflict in the choices of forum.*

5. *In determining the appropriate jurisdiction and governing law, it is important that the network can establish a nexus to such jurisdiction.*

Dispute Resolution

A dispute resolution mechanism is crucial for establishing and facilitating accountability, legitimacy, and legal certainty of a blockchain network. Participants desirous of joining the blockchain network are likely to look for recourse in the event of any failure, misuse, illegality, or breach of terms governing the network. The lack of such recourse and the fear of incurring loss owing to the same would diminish the value of blockchain and can severely affect the rate of its adoption. As blockchain is a decentralised technology where nodes can be spread across jurisdictions (and pseudonymous participants in certain cases), it may be challenging for participants to avail traditional dispute resolutions mechanisms such as courts. Therefore, it may be useful for the governance framework to set out a dispute resolution mechanism to decide disputes relating to the functioning of the network.

1. *The governance framework should set up a dispute resolution for settling disputes between participants. This may include instances of dispute relating to violations of terms and conditions governing the functioning of the blockchain network and participants.*

2. *There may be some disputes which might be better resolved through an internal dispute resolution mechanism. For instance, this could be disputes involving on-chain*

transactions, processing of data on-chain or where resolution would require complex technical expertise or deeper software knowledge.[293] *Having an internal dispute resolution mechanism can ensure that on-chain grievances are resolved quicker, cheaper and in a more efficient manner.*

3. *Therefore, dispute resolution mechanisms may be tiered. In such cases, the first resort may be to resolve the dispute amicably through an internal dispute resolution mechanism, failing which parties can resort to other formalised forms of adjudication.*

4. *The dispute resolution process should clearly stipulate the matters/contraventions that will be covered by the internal dispute resolution mechanism. Further, it is also important to state if all participants are eligible to avail of the dispute resolution mechanism.*

5. *For an internal dispute resolution mechanism, the following matters should be specified:*

(a) The matters / disputes that will be covered by such mechanism.

(b) The adjudicatory body that will adjudicate on such disputes, the composition, and mode of selection of such body.

(c) The power of such adjudicatory body to enforce its orders.

(d) Provision for appeal (if any) from the orders of such adjudicatory body.

6. *The participants should agree to be bound by the orders passed under the internal dispute resolution mechanism. Sanctions such as suspension from membership or removal from the blockchain network can be imposed.*

7. *Such a dispute resolution mechanism is likely to be more effective in the case of private permissioned blockchain where participant identities are known and there is information available regarding them as opposed to public permissionless blockchains where the participants are pseudo-anonymous and can be participating from anywhere in the world.*

Termination of the Blockchain Network

In case of a permissioned private blockchain that has been set up for a stated objective, participants may desire to have an option to terminate the network under certain conditions. Needless to say, the technical feasibility of such termination and its impact on the data / information stored in the network will have to be thoroughly examined.

1. *The governance framework may provide a provision to terminate the network.*

2. *In such cases, the governance framework may specify the following:*

(a) Conditions under which the network can be terminated. This could include termination at will, failure to meet critical milestones or directions by court or applicable law. Each of these instances may have its own conditions. For instance, if the blockchain network can be terminated at will, then it needs to be specified if such decision must be a unanimous decision of all parties or if a specific number of participants must approve it.

[293] World Economic Forum, 'Redesigning Trust: Blockchain Deployment Toolkit' (2020) <https://widgets.weforum.org/blockchain-toolkit/pdf/WEF_Redesigning_Trust_Blockchain_Deployment%20Toolkit.pdf> accessed 15 September 2022.

(b) There must be a clear exit plan setting out how the data will be managed, deleted, transferred and if there are any continuing obligations.

VII. Conclusion and Way Forward

As governments and the private sector vigorously explore and implement blockchain-based solutions in various sectors, it is critical to examine the legal and regulatory issues that may emanate from such decentralised technologies. Legal certainty is necessary to incentivise participants to join the network and provide legal protection to participants. This Working Paper seeks to present some important legal considerations that must guide the design of a blockchain application. As the technology evolves, it is important that the design takes into account such legal considerations to not only promote innovation but also protect users.

As various Central Government Ministries, state governments and regulators in India are exploring implementing blockchain-based solutions for public sector use in India, the following preliminary measures may be considered to support and scale up this technology, while also ensuring that the interests of users are protected.

First, the National Strategy on Blockchain released by MeitY should be supplemented with a National Policy for Implementing Blockchain Applications. This policy should delineate key public policy principles and standards that can guide the public sector use case of blockchain solutions. The policy can lay down the minimum benchmarks that must be met by blockchain-based applications for public sector use. As various government agencies explore blockchain use cases for various sectors, the National Policy will be useful to guide such applications and ensure that all such applications adhere to common minimum standards. A similar approach is also seen with the Dubai Policy which delineates certain public policy principles that must inform government use cases of blockchain.

Second, it may be useful for the Government to set up an expert committee to assess specific laws including sectoral laws to study if such laws can accommodate blockchain applications. This is relevant for laws relating to data protection obligations under the IT Act, SPDI Rules or under sectoral laws (such as Reserve Bank of India guidelines/circulars). For instance, the IT Act may have to be relooked to examine if express legal recognition should be conferred on records stored on blockchain. Further, the IT Act may be reviewed to ensure that the techniques used for authenticating smart contracts are legally recognised under the IT Act. This will also have implications on the evidentiary value of smart contracts under the Evidence Act. It may be also useful to clarify the applicability of the Prevention of Money Laundering Act 2002 provisions to participants of blockchain applications. In certain cases, the government may issue guidance / clarifications regarding the applicability of specific laws to blockchain applications as has been done by regulators in France and Singapore regarding the applicability of data protection laws to blockchain applications.

Third, as the government and private sector are exploring blockchain use cases across sectors, it may be useful to set up a standard-setting body consisting of stakeholders from the government and private sector. This body can be responsible for setting minimum technical, security and data governance standards for blockchain applications storing information about Indian users.

www.vidhilegalpolicy.in

Vidhi Centre for Legal Policy
D-359, Defence Colony
New Delhi – 110024

011-43102767/43831699

vidhi@vidhilegalpolicy.in