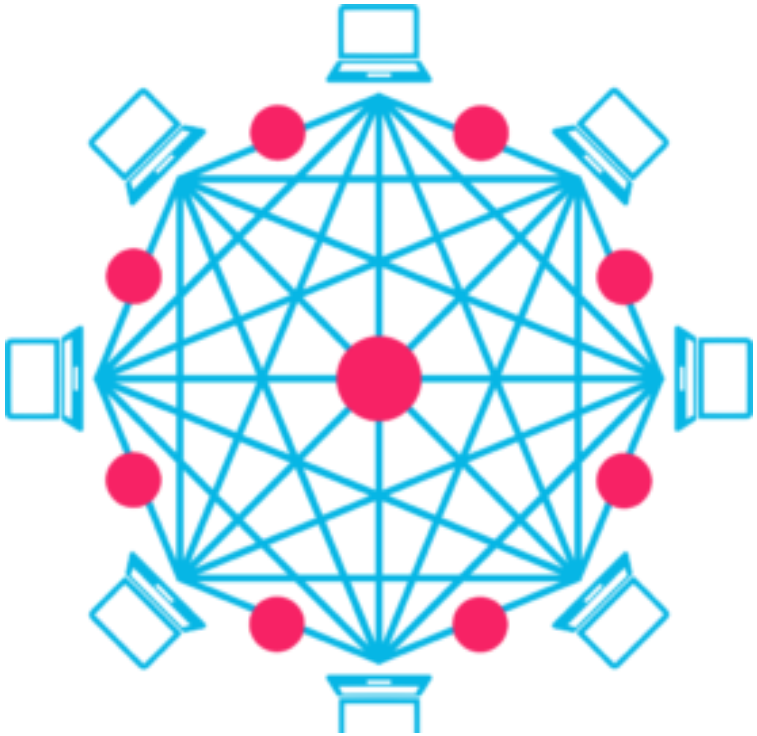
GameChanger
Law Advisors

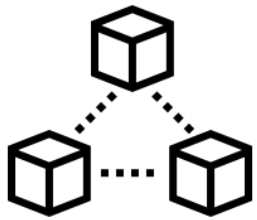
Decrypting Blockchain Technology: Basic Concepts & Legal Issues

"The blockchain is a global spreadsheet -- an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degrees, financial accounts, medical procedures, insurance claims, votes, transactions between smart objects, and anything else that can be expressed in code"

- Don Tapscott, Co-founder & Executive Director, Blockchain Research Institute



Blockchain and Blockchain Technology

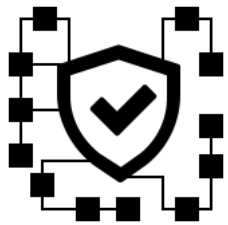


Global digital ledger containing a list of transaction records or blocks that is secured using cryptology

Each block contains a link to a previous block, a timestamp and transaction data

It is a decentralized technology, i.e. the network works on a peer-to-peer basis. Not dependent on any centralized system to function (Eg. a bank)

- Although used initially for cryptocurrency transactions, new uses include include smart contract, e-health, accountability and measurement of social impact, authenticating evidence, title searches and many others.
- The technology that is used to facilitate the blockchain is referred to as blockchain technology.
- A blockchain network may be public and open (permissionless) like the internet or structured within a private group like an intranet (permissioned).



Key Aspects of Blockchain & How it Works

DIGITAL SIGNATURE

- Used to authorize a Transaction
- Made up of a Private Key + Public Key

PRIVATE KEY

- Akin to a Password
- Used to create a Transaction

PUBLIC KEY

- Akin to a 'Send' button in an e-mail
- Used to verify a Transaction
- Unique to every Transaction

DETERMINING VALIDITY

- All nodes in the network need to validate transaction / block to add it to the chain

MINING

- "Miner" nodes compete to solve a complex algorithm to verify the block
- In Bitcoin, this is known as 'Proof of Work'

TRANSPARENCY

- All information regarding the transaction, i.e. the chain, is available to the entire peer network (other than a private key) and is always available to the public.

PUBLIC RECORD

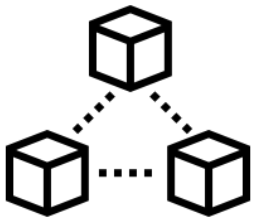
- Every node receives a record of the transaction history
- Helps to map the flow of information
- Applicability: Title Searches

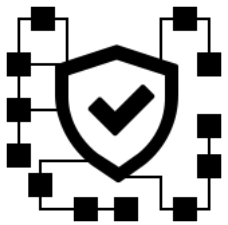
IDENTITY

- In public networks, participants are only identifiable through IP Address or the Public Key

Recent Developments in India

- "*The Government does not consider crypto-currencies legal tender or coin and will take all measures to eliminate use of these cryptoassets in financing llegitimate activities or as part of the payment system. The Government will explore use of block chain technology proactively for ushering in digital economy*." - Arun Jaitely (Union Budget 2018-19)
- NitiAayog, which has been tasked with exploring use-cases for blockchain technology, has recently in February 2018 announced the implementation of 'IndiaChain': to develop a national blockhain network to create a secure database of records, reduce fraud and increase speed of contract enforcement. The first use-case identified is for issuance of digital certificates in the education sector.
- Rise in number of blockchain technology based Indian start-ups developing innovative use-cases in identity verification, healthcare, manufacturing, contract management & supply chain management





By 2020, 10% of global commerce will be running on blockchain backed and enabled systems. - *World Economic Forum*

Top 5 Legal Issues Surrounding Blockchain Technology

1

Absence of a 'Customer Helpline'

- Lack of a centralized authority means an absence of a 'customer helpline' or intermediary in case of any user-errors eg. loss or misuse of a private key or other security issues.
- Protection cannot be sought under the Information Technology Act, 2000 or in any court of law.
- Loss of a private key could therefore mean loss of assets with no legal or quasi-legal recourse.

2

Jurisdiction

- Permissionless blockchain systems have the ability to permit transactions across borders. This combined with a lack of identity, could create cross-border jurisdictional issues.
- Given the anonymity of the participants, pinpointing the jurisdiction of a fraudulent or erroneous transaction participant could be challenging.
- Principles of contract and title differ across jurisdictions. Therefore for permissioned systems, identifying the appropriate governing law and dispute resolution mechanism is essential. **Arbitration is a good option as the New York Convention allows easy enforceability across different jursidictions**

3

Data Privacy and the Right to be Forgotten

- Data stored in a blockchain cannot be altered. This is one of the biggest strengths as it provides a digital ledger for record keeping. However, this has data privacy implications, particularly if data is sensitive personal data such as medical records etc.
- The 'right to be forgotten' is a right available to an individual to request deletion of personal data from the internet, recognized by the ECJ in 2014 and recently touched upon by Justice Kaul in *K.S. Puttaswamy* and recognized in a Karnataka high court judgment (*Sri Vasunathan* v. *Registrar*).
- If deemed enforceable, implications of this on

erasing personal records stored in blockchain systems raises interesting questions.

- Technology-based solutions will need to be found to protect privacy of blockchain users, including encrypting blockchain data. There is a need to implement solutions for migration & destruction of data without affecting system efficiencies.
- Development of Data Protection laws in India should therefore be forward thinking and take into account implications on disruptive technology like blockchain.

4

Attribution of Liability

- Can the company managing a private blockchain system be held responsible for any fraudulent or erroneous transaction? Who is responsible if laws are broken? What, if, any, is the liability of decentralized system and their creators? Can it be considered as a separate legal entity? Like with other disruptive technology, many such questions have not yet been tested in any court of law.
- So the allocation and attribution of risk and liability to all relevant parties must be thought through carefully.

5

Intellectual Property

- Given the amount of investment and the potential financial returns of blockchain technology, blockchain vendors will have to determine their IP monetization strategy: vendors will likely want to capitalize on any other commercial benefits to be generated from the Blockchain, including commercialization of the underlying data set.

GameChanger
Law Advisors

To learn more about Blockchain Technology, please contact us at shwetha@gamechangerlaw.com

Many thanks to our intern Srikanth Bhaskar, 5th Year Student from Gujarat National Law University, who helped with the research!