January 6, 2020

BLOCKCHAIN TECHNOLOGY
- A REVIEW

argus partners
SOLICITORS AND ADVOCATES

TECHNOLOGY & DATA PRIVACY

MUMBAI I DELHI I BENGALURU I KOLKATA I AHMEDABAD

What is a Blockchain?

A blockchain, as its name suggests, is a virtual chain made of blocks, where each block contains information. Alternatively, it can be described as a digital ledger, where each block of data represents a distinct transaction on the ledger, with the transactions occurring across a decentralized peer-to-peer network. This peer-to-peer network consists of a network of computers (each called a "**node**") connected together, which allows the participants in the blockchain to transfer information across the internet without the need to involve any centralised third party. Each block in a blockchain comprises of (i) the transaction data (ii) a timestamp recording the creation of the block and (iii) a cryptographic hash which is unique to each block, akin to a "fingerprint". When a node initiates a transaction, it sends across a message to the other nodes in the network. Each transaction is verified by the nodes, without relying on any external party for authentication, before it is added to the blockchain. This verification process is as follows. Each node in the network has its own set of public and private cryptographic keys. Whenever a transaction is initiated by a node, it generates a digital signature with its private key. The digital signature is proof of the authenticity of the data present in the block. Once the transaction has been examined by every node, there is an electronic vote amongst them to decide the validity of the transaction. If a majority of the nodes hold the transaction to be valid then it is written into a block and the newly created block forms a part of the chain.

Each block includes the cryptographic hash of the previous block. Each newly formed block latches itself to the previous block and is available for public viewing. When a new node joins the network, the complete history of all the transactions is copied onto its system, pursuant to which it can undertake all the functions of a node in the network. Once a block is created, any change made to the information inside the block will cause the unique hash inside such block to change, which will have a cascading effect on all the blocks in the blockchain and will make all of them invalid. This gives blockchain its unique "immutable" feature and makes it resistant to hacking.

Decentralisation makes the Blockchain Stronger

A blockchain establishes a decentralized network that allows the participants in the blockchain to transfer information across the internet without the involvement of any centralised authority. The information that is transferred is not stored by the blockchain in any fixed location but is replicated multiple times across a network of nodes. When nodes communicate with each other, they become "peers" and form a peer-to-peer network. Thus, instead of having one central server, there exists several distributed and decentralized peers. Whenever any new block is added to the blockchain, this information is spread across all the nodes in the network which in turn simultaneously update their own blockchains. By spreading information across a network, rather than storing it in one central database, a blockchain becomes more difficult to tamper with.

Origins of Blockchain

Blockchain came into vogue in 2008 as the underlying technology for Bitcoins, which has been hailed as the world's first decentralized cryptocurrency. In the words of its creator (who used the pseudonym 'Satoshi Nakamoto'), Bitcoin was created since there was a need for "*an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party*"[1].

[1] https://bitcoin.org/bitcoin.pdf.

Bitcoin can be likened to a digital token having the nature of virtual cash, operating on a peer-to-peer network. Bitcoins can be bought, sold and traded on crypto-exchanges and can be used to pay for goods and services. Bitcoin holders use a decentralized peer-to-peer network based on blockchain technology to transfer their Bitcoins to each other or third parties. These transfers of Bitcoins are recorded by each node in the network, thereby creating an immutable ledger of such transactions. Bitcoins are stored in a 'digital wallet' on a smartphone or computer. A digital wallet includes a public key and a private key, which together permit the Bitcoin holder to authorize every Bitcoin transaction that such holder participates in. Each transaction is contained in a block, which after verification by the nodes, gets added to the blockchain, thereby recording each of such transactions permanently.

The Bitcoin network is sustained through “mining”. Bitcoin mining is the process of creating new Bitcoins which are then given to the nodes in the network. Since there is no single central server verifying the transactions which occur in a Bitcoin network, it falls upon every person on the network to verify the transaction. These people are called miners. The miners are given a complex math problem to solve and the miner who first solves the problem adds the verified ‘block’ to the blockchain. The fastest miner is given a chunk of Bitcoins as a reward for their efforts. Bitcoin mining, however lucrative it may sound, is an incredibly sophisticated process that requires specialized computers with advanced processing powers. Every Bitcoin which currently exists has been created through this method.

Types of Blockchains - Public and Private

A public blockchain is one in which anyone can join the blockchain network and participate within the blockchain. Public blockchains are decentralised, in the sense that no one has control over the network. Bitcoin and Ethereum are examples of public blockchains.

A private blockchain is one where only permitted participants can join. The following are examples of innovations which rely on private blockchains:

Smart Contracts

Smart contracts are more than mere agreements. They are a set of protocols embedded in computer codes and stored in a blockchain which provide for the negotiation, finalisation and enforcement (or implementation) of such contracts. Once committed, parties would be bound by the protocols wired into such contracts by the programmers. Thus, parties in different countries could enter into such agreements without worrying about bias or prejudice. There would be greater transparency and accountability. More importantly, transaction costs would be lower since there would be no middle-men involved.

Storing Land Records on a Blockchain

It is possible to store details of ownership of land and the underlying transactions on a blockchain. Since all underlying transactions would have been verified by users, the changes of fraud or forgery become minimal, if not non-existent. The verified block becomes an immutable record accessible to the public for viewing. These blockchains would ideally be over a private network, with only a few government entities, like the registrar’s office having the power to add information to the blockchain. The scope of such entities can be regulated by the guidelines embedded in the blockchain.

Currently, the infrastructure for recording and storing land records is plagued with corruption and other inefficiencies. Title certificates issued by the government do not come with title guarantees. If title certificates are verified by a blockchain, the credibility of such certificates would be vastly improved and challenges would be minimal.

However, the implementation of such a blockchain would face many practical difficulties. If the underlying land records are imperfect and subject to many disputes, it would not be possible to store them on a blockchain, since users would not be able to approve all records. However, when a new capital is being built, as is happening in Andhra Pradesh and a clean slate is available, blockchain can be used effectively.

Degree Certificates

Circulation of fake degree certificates is endemic in India. This is partly because verification of a degree certificate is difficult and many fake certificate holders get away with their crimes. Blockchain technology offers a solution to this problem by shifting the entire process of issuance and verification of the certificates on the blockchain. Digital certificates issued on a blockchain can be verified through an app. The app will be accessible by the issuing university and each of the graduating students and will allow verification by third parties. Moreover, the records cannot be tampered with, since blockchain technology does not allow for any modifications to be made to the information already stored in the chain.

Fighting Drug Counterfeiting

Counterfeiting of drugs is rampant in the pharmaceutical industry. There is a lack of transparency in the supply chain through which manufactured drugs reach consumers, due to which the authenticity of the drugs cannot be easily verified. Without transparency in the supply chain, it is nearly impossible to trace the source of any fraud, identify the perpetrators involved, or verify the authenticity of the drugs. Fake drugs may contain highly toxic substances which could be fatal to human life, hence there is a need for an efficient drug tracking system. The main feature of blockchain technology that can be utilized in drug traceability is its security, as each block added to a blockchain is immutable as well as timestamped. Pharmaceutical companies that manufacture drugs can register their drugs on to a blockchain before such drugs are shipped, to ensure their traceability. Every package shipped by such a manufacturer will have a unique ID that will be inserted in the block. Each block in the chain will be linked to the next one and as the drug moves along the supply chain among different entities, it can be traced easily at any given stage. End users can scan the unique ID stamped on the wrappers to verify the genuineness of the drugs they have purchased.

Security Threats to Blockchain Users

Since every node in a blockchain stores details of all transactions, which can be scrutinised by anyone in the network, malicious users may access and trace public keys and addresses to specific persons. If and when an individual user of a blockchain is traced, every transaction undertaken by such an individual through blockchain may be permanently exposed.

A person's private key is used by him/her to sign as well as verify every transaction that s/he makes on a blockchain. Each private key creates a unique digital signature for every transaction that the key-holder undertakes, thereby verifying that the key-holder has ownership of the assets which are being transacted and that s/he has the authority to undertake the transaction. Since private keys are crucial to accessing and safekeeping assets on a blockchain, users are required to store them safely. If the private key becomes available to a stranger, the assets stored on the blockchain could be compromised. Storing the private key on a computer, flash-drive or telephone can pose potential security risks if the device itself is lost, stolen or hacked. If such a device is lost, the user will cease to have access to his/her private key, and in turn, his/her assets, such as cryptocurrency. Storing it on a physical media, such as a piece of paper, also leaves the private key vulnerable to loss, theft or damage.

Blockchain Technology and Data Privacy Law – A Clash of Ideologies

The immutability of data and transparency are two important pillars on which blockchain technology rests. The immutability of data implies that data cannot be erased and transparency requires data to be exposed to public view. These two requirements conflict with data privacy laws across jurisdictions.

In India, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**IT Rules**") currently govern the collection, disclosure and processing of personal data and sensitive personal data. Sensitive personal data has been defined in the IT Rules to include, inter alia, passwords and financial information. While the IT Rules do not explicitly provide a person whose sensitive personal data is being collected ("**Data Principal**") the right to seek an erasure of their personal data, it does create an obligation on the body corporate or person holding such data to not retain it for longer than is required for the purposes for which the information may be lawfully used. Moreover, the IT Rules stipulate that any personal data, including sensitive personal data, can only be collected after obtaining the necessary consent from the Data Principal. Such consent can be withdrawn by the Data Principal, by a request in writing, at any point of time while availing the services of such body corporate/person. The IT Rules also give Data Principals the right to seek a review of his/her personal data and sensitive personal data, and if found inaccurate, the right to request that it be corrected or amended.

The Personal Data Protection Bill, 2019 ("**PDP Bill**") provides more detailed rights to Data Principals with respect to the privacy of their personal data and sensitive personal data.

Section 9 of the PDP Bill provides that a data fiduciary (defined to mean the person who determines the purpose and means of processing of personal data) should not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and should delete the personal data at the end of the processing. However, if the Data Principal consents or if required to comply with any law, the personal data may be retained for a longer period. Each data fiduciary is required to undertake periodic reviews to determine whether it is necessary to retain the personal data in its possession. Where it is not necessary for personal data to be retained by the data fiduciary, then, such personal data has to be deleted in the manner to be specified by regulations. Section 18(1)(d) of the PDP Bill gives each Data Principal the right to seek the erasure of his/her personal data if such personal data is no longer necessary for the purpose for which it was processed. Section 20 of the PDP Bill provides that every Data Principal has the right to restrict or prevent continuing disclosure of personal data (relating to such Data Principal) by any data fiduciary if such disclosure meets 1 (one) of the following 3 (three) conditions, namely the disclosure of personal data: (i) has served the purpose for which it was collected or is no longer necessary, or (ii) was made on the basis of the Data Principal's consent and such consent has since been withdrawn, or (iii) was made contrary to the provisions of the personal data protection act or any other law in force.

Penalties for Breach of Data Privacy Law by a Blockchain Operator

What happens if a data fiduciary who operates a blockchain breaches any of the provisions mentioned above?

Section 43A of the Information Technology Act, 2000 ("**IT Act**") holds accountable data fiduciaries (being body corporates), who are negligent in implementing and maintaining reasonable security practices and procedures (which are prescribed by the IT Rules) while possessing, dealing or handling any sensitive personal data or information in a computer resource which they own, control or operate and which has resulted in wrongful loss or gain to any person. The IT Act imposes an obligation on the data fiduciary to pay damages by way of compensation to the person so affected.

The IT Act empowers the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer to inquire into complaints of contraventions of any of the provisions of the IT Act or the IT Rules. The adjudicating officer exercises jurisdiction over matters in which the claim for injury or damage does not exceed Rs. 5,00,00,000 000 (Rupees Five Crore Only), whereas all claims above that threshold shall lie with the competent civil court. Every order made by such an adjudicating officer is appealable to a Cyber Appellate tribunal vested with appropriate jurisdiction.

Section 58 of the PDP Bill provides that if the data fiduciary fails to, *inter alia*, comply with a request for erasure made by a Data Principal, without providing any reasonable explanation to such Data Principal, the data fiduciary shall be liable to pay a penalty of up to Rs. 5,000 (Rupees Five Thousand Only) for each day during which such default continues, subject to a maximum of Rs. 10,00,000 (Rupees Ten Lakh Only) in case of significant data fiduciaries and Rs. 5,00,000 (Rupees Five Lakh Only) in other cases.

Section 53 of the 2019 Bill gives Data Principal's the right to file a complaint with the Data Protection Authority of India ("**Authority**") against any data fiduciary if inter alia, such data fiduciary has contravened the provisions of the personal data protection act. Pursuant to such a complaint, if the Authority has reasonable grounds to believe that the data fiduciary has violated any law, it shall appoint an inquiry officer to inquire into the affairs of the data fiduciary and prepare a report of its findings. Based on the report of such inquiry officer, the Authority shall, after hearing the data fiduciary in relation to the report, make a written order giving appropriate directions to the data fiduciary in accordance with Section 54. Through its order, the Authority can, *inter alia*, require the data fiduciary to take any such action in respect of any matter arising out of the report as the Authority may deem fit. If the Data Principal is aggrieved by the Authority's order, Section 72 of the 2019 Bill provides for an appeal to the Appellate Tribunal against such order.

Technological Solutions for Data Privacy Compliance by Blockchains

It is obvious that even under existing Indian data privacy law (that is, the IT Rules), blockchains tread on the privacy rights of Data Principals. Rights to erasure and to restrict or prevent continuing disclosure cannot co-exist with immutability or permanence of data that blockchain technology trumpets about. This issue will become even more acute in India once the PDP Bill comes into effect. The EU has been grappling with this conflict for some years now, which came into sharp focus after the General Data Protection Regulation ("**GDPR**") came into effect. Various technical solutions have been offered to this paradox, such as "forking" or using hashes. "Forking" attempts to rewrite the data held on a blockchain by getting most nodes on the network to agree to create a new version of the blockchain which includes the changes that the Data Principal wants to reflect and to then continue using that version rather than the original. Another solution which has gained prominence is that of hashing the personal data, where only "hashes" of personal data would be inserted into the blockchain, rather than the data itself. Hashes are mathematical derivations of data which cannot be reverse engineered to expose the data which is being represented. In a blockchain, hashes are used to verify the underlying data by repeating the hashing algorithm on that data and comparing the result with the stored hash. With a blockchain of hashes, rather than the underlying data, it might be possible to delete the data without having to alter the blockchain[2]. At the end of the day, it is accepted by all and sundry that it would be very difficult, for technical reasons, to remove personal data contained in a blockchain.

Possible Legal Innovations for Data Privacy Compliance by Blockchains

Consent from the Data Principal

If we assume, for argument's sake, that personal data contained in a blockchain cannot be erased, where does that leave those who either initiated the blockchain or are participants in the blockchain? One of the fundamental principles of data privacy law is that the Data Principal's consent is required for the processing of his/her personal data. It could be argued that by participating in a blockchain, a Data Principal is deemed to have given his/her consent for the permanent storage of his/her personal data in the blockchain, for the accessing of such data by all users of such blockchain and has permanently waived his/her right to seek erasure of such personal data. This argument might hold water under the IT Rules, but the PDP Bill requires express consent for such a waiver, especially if the data involves sensitive personal data. Therefore, before any user is given access to a blockchain, such user must be informed in clear and explicit terms that (i) it would be impossible to remove or erase his or her personal data from the blockchain, (ii) immutability of data and transparency are vital for the smooth functioning of the blockchain, and express consent obtained from such participant for permanent storage of his/her personal data in the blockchain.

Section 9(2) of the PDP Bill has a notwithstanding clause which provides that personal data may be retained for a longer period if explicitly consented to by the Data Principal. However, Section 18 of the PDP Bill which relates to the right to erasure of personal data, does not state that the

[2] https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/.

right of erasure disappears if the Data Principal has waived such right. It is a well-accepted legal principle that statutory rights cannot be waived unless the statute itself provides otherwise. However, Section 18 of the PDP Bill subjects the Data Principal's right to erasure to "having regard to the purposes for which personal data is being processed". Therefore, if the Data Principal has been informed of the near impossibility in erasing personal data from the blockchain and the importance of immutability of data and transparency, it may be argued that the right to seek the erasure of personal data from the blockchain does not subsist.

Withdrawal of Consent by the Data Principal

The arguments stated above for the harmonious co-existence of blockchain technology and data privacy rights come unstuck in the face of the Data Principal's right to withdraw consent for the processing of his/her personal data. As mentioned above, Section 20 of the PDP Bill provides that a Data Principal shall have the right to restrict or prevent the continuing disclosure of his/her personal data by a data fiduciary where such disclosure was made with the consent of the Data Principal and such consent has been withdrawn. The IT Rules give Data Principals an unequivocal right to withdraw consent with respect to any information provided, including sensitive personal data. Sections 7 and 11 of the PDP Bill also make it clear that a Data Principal has the right to withdraw his/her consent for the processing of his/her personal data. Prior to the processing of personal data on the basis of consent, the PDP Bill requires that the Data Principal be informed of his/her right to withdraw consent and of the procedure for communicating such withdrawal.

Section 11(6) of the PDP Bill states that where a Data Principal withdraws his or her consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such Data Principal. However, this provision will be of limited assistance in resolving the conflict between blockchain technology and data privacy rights, since it is possible that the Data Principal may have a valid reason for the withdrawal of consent.

Irrevocable Consent by the Data Principal

Having regard to the near impossibility of erasing data from a blockchain, would it be possible to obtain 'irrevocable' consent from the Data Principal before s/he is given access to the blockchain? Would such irrevocable consent be valid under law, given that the IT Rules and the PDP Bill place so much emphasis on the right to withdraw consent?

Unfortunately, the possibility of giving irrevocable consent is not even contemplated either by the IT Rules or by the PDP Bill. It is evident that the difficulty in erasing personal data from a blockchain has not been considered by those who drafted the PDP Bill.

Best Efforts Erasure or Restriction of further Disclosure

Another line of thought for resolution of this conflict is that, once consent is withdrawn, the data fiduciary who operates the blockchain only has to make the best efforts for the erasure of personal data or for the restriction or prevention of the continuing disclosure of his/her personal data. If any personal data remains un-erased or if disclosure continues unrestricted despite such best efforts, the data fiduciary shall not be liable for the penalties mentioned above, especially since the Data Principal was informed of the difficulty in erasing personal data from the blockchain.

Conclusion

Blockchain is the technology of the future and is here to stay, notwithstanding legislative impediments. Law is usually slow in keeping up with technological advancements. In our considered opinion, the PDP Bill ought to be amended (before it comes into force) to provide that data fiduciaries who operate a blockchain can obtain prior, 'irrevocable' consent from Data Principals for the processing of their personal data after providing Data Principals with sufficient information regarding the salient features of blockchain technology and the importance of immutability of data in the blockchain. The provisions of the PDP Bill dealing with the Data Principal's right to withdraw consent should be disapplied in cases where the personal data is stored in a blockchain.

Post the advent of GDPR, the European Union's European Parliamentary Research Service has published a paper[3] which discusses the conflict between blockchain technology and GDPR. Readers may access this paper via this link: http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

This paper has been written by Vinod Joseph (Partner) and Protiti Basu (Associate).

[3] Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law? A study by the Panel for the Future of Science and Technology, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA), PE 634.445 – July 2019

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata

www.argus-p.com