Kluwer Competition Law Blog

The Interaction Between Blockchain and Competition Law in the Indian Competition Regime

Vishal Rajvansh (The Competition & Commercial Law Review) and Saumya Sinha (Sarthak Advocates & Solicitors) · Wednesday, May 5th, 2021

While the skyrocketed technological advancements add immense comfort to human lives, they bring certain tied-up gifts for humans to ponder upon. One such technology which recently had an enormous outburst in the economic structures is that of blockchains. Blockchain is one of the most revolutionary consequences of the advancement of digital commerce which is arguably expected to store about 10% of the total gross domestic product by the year 2025-27.[1]

Blockchain precisely refers to a distributed ledger technology that stores information in blocks on several nodes without the control of a central authority or the interference of intermediaries.[2] The transactions in a blockchain take place with the consent of each node without the control of a central governing entity and such transactions are immutable, contributing to the trustworthiness of blockchains.[3] Indubitably, these characteristics of blockchains make them the preferred mode of transaction for numerous purposes including the spheres of finance, cryptocurrency, healthcare industry, supply chains, etc.,[4] thereby accounting for their interaction with various spheres of technology, law and economy.

While most of these interactions have been repeatedly discussed, the one between blockchain and competition law is relatively nascent with a dearth of judicial precedents.[5] The adoption of this technology raises several prominent concerns, relating to the application of various aspects of Competition law.

Applicability of the Indian Competition Framework to blockchains

First and foremost, the qualification of a blockchain as an 'enterprise' under the Competition Act, 2002 (**"Act"**) is crucial for the assessment of various anti-competitive practices. Notably, an enterprise is defined by the Act as "a person or a department of the government which is engaged in any activity…."[6] The CCI has interpreted the term to include any entity which is engaged in any specified economic and commercial activity.[7] In this context, a blockchain can be termed as an enterprise based on two grounds. Firstly, the definition of 'persons' which includes "*individuals, artificial juridical persons or an association of persons or a body of individuals, whether incorporated in India or outside India,*"[8] would naturally encompass blockchains and their participants. Secondly, a blockchain is involved in the *provision of services****[9]*** with the use of

distributed ledger system thereby falling within the ambit of the act as it encompasses services of any description provided to the user.[10]Conclusively, a blockchain can reasonably be termed as an enterprise and is amenable to several provisions of the Act.

Further, the question as to whether or not the participation in blockchain can be construed as an agreement is fundamental to the applicability of the Act to blockchains in light of Section 3. This provision purports to prohibit the conclusion of anti-competitive agreements between various entities.[11] The Act provides a rather wide definition of 'agreement' to include *any arrangement or understanding or action in concert* irrespective of it being formal or in writing; enforceable or not.[12] As the definition is wide enough to "*cover situations where the parties act on the basis of a nod or a wink*,"[13] it evidentially encompasses blockchain within its ambit. This is primarily because various participants of the blockchain in fact act in concert or agreement through the use of a consensus mechanism to maintain or modify the status of the ledger, which is instrumental to the functioning of a blockchain.[14] Consequentially, this modus operandi of blockchains enables the various nodes to facilitate anti-competitive practices by the use of mutual consent, thereby meeting the requirements of an 'agreement' under the Act.

Another pertinent question surrounding the applicability of the legal regime to blockchains is that of jurisdiction. Blockchains generally extend across various countries and work in a global network, while the participants maintain an anonymous nature of their identity.[15] This comes off as a setback for regulatory authorities as it would be onerous to ascertain which authority would exercise jurisdiction and more importantly, over whom. Although the CCI is empowered to exercise jurisdiction over global blockchains in cases where an appreciable adverse effect is cast on competition in the relevant market in India,[16] its application will be a practical impediment to say the least.

Blockchains: Pro or anti-competitive?

The highly complex nature of blockchains renders their interpretation as pro- or anti-competitive exceedingly debatable while raising a number of anti-competitive concerns on account of the various fundamental aspects involved in their use.[17] One of the core features of blockchain technology is its decentralised nature, where every participant is equally involved and has access to the same amount of information. An optimistic approach would suggest that the decentralisation and consequent transparency can be effective in promoting competition as consumers are provided with greater information resulting in effective transactions.[18] However, it is more likely that the availability of such an impactful amount of information would result in the adoption of anti-competitive practices as it would abet the exchange of commercially sensitive information and consequential unlawful concert between various parties.[19] The decentralised nature of the technology would also prove to be an enforcement challenge for the regulatory authorities as there is no single definite entity to be held accountable.[20]

Additionally, certain prominent concerns also result from the pseudonymous nature of participants of a blockchain. On a high note, the formation of anti-competitive agreements in cases of permission-less blockchains is less likely due to the high number of pseudonymous participants involved which makes entering into agreements rather improbable.[21] However, if such agreements were formed, pseudonymity would pose a substantial challenge for the regulatory authorities as the identification and accountability is not practically plausible in vast permission-

less blockchains.[22] Permissioned blockchains, on the contrary, would not raise these enforcement concerns[23] as they are generally governed by a centralised entity and the participants thereof are scrutinised and listed.

Sensitive information exchange: A catalyst for collusion?

As blockchains use a distributed ledger system, every node can have access to commercially sensitive information including prices, discounts, production, sales, cost, turnover, price and management-related plans and strategies, investments amongst other strategic information.[24] Notably, the CCI in its ***Compliance Manual****[25]*categorically discourages enterprises from even discussing such matters concerning prices, quantities and conditions of goods and marks it to be an anti-competitive practice prohibited by the Act.[26] Further, the CCI in ***Builders Association of India v.Cement Association of India and ors****[27]* held that the availability of commercially sensitive information could result in anti-competitive outcomes in light of Section 3 of the Act. Astonishingly, this position was altered in the ***Flashlights case****[28]* wherein the Commission ruled that the mere exchange of sensitive information was not enough as its effect on the determination of prices by the enterprises involved could not be established.

Conspicuously, in the recent judgment of ***In Re: Cartelisation in Industrial and Automotive Bearings****[29]* the CCI restored the previous position of law enunciating that Section 3 not only prohibits agreements that cause an appreciable adverse effect on competition but also those which are likely to cause such effect. The case reiterated that the exchange of commercially sensitive information is an anti-competitive practice. Such a strict stance of the CCI vis-à-vis the exchange of information does not favour the operation of blockchains and is opposed to the basic principle on which such blockchains are based.

Smart Contracts: oil in the fire?

The CCI not only prohibits sharing of sensitive information but also any activity or collusion that can adversely affect competition. In light of the same, the use of smart contracts in blockchains can prove to be effective tools of collusion and thereby raise significant anti-competitive concerns. Smart contracts, simply put, are self-executed digital contracts which are automatically executed based on the fulfilment of given contingencies, without the element of human intervention.[30] Such contracts are used in a blockchain for carrying on various transactions. Interestingly, smart contracts can be devised to automatically specify punitive measures against collusions thereby adding to the transparency advantage of blockchains and promoting competition.[31] However, they are also capable of facilitating collusions and making them dynamic in nature[32] as such contracts can easily be devised by parties to a blockchain to automatically form agreements upon automatic satisfaction of conditions based on the shared information.[33]

Essentially, smart contracts are computerised programs that function on algorithmic principles.[34] The CCI in its recent decision in the case of ***Hyundai Motor Company and Kia Motors Corporation****[35]* ruled that the mere use of algorithms is not discriminatory in nature, however, such algorithmic means should not be used to promote anti-competitive behaviour in the relevant market.[36] The complex nature of algorithms used in smart contracts and the inescapable issues

attached with the identification of the entity involved in the anti-competitive use of such contracts present significant potential legal anomalies for the regulatory authority. One of the prominent anomalies relates to the regulation of data use. Being one of the substantial components of blockchain, they might render certain competitive advantages and disadvantages.

Blockchain and data – A smoking gun for anti-competitive concerns

Interestingly, data is considered to be the new oil[37] in the age of technology and an information-oriented economy.[38] In the near future, blockchains might become the largest reservoir of such oil which will have several impacts on the economy as well as competition. Notably, every block in the chains contains data that can provide the consumers with greater information and help them make better choices for market purchases and investments thus creating better-functioning markets.[39] The emergence of such comprehensive markets can prudentially enhance competitiveness and reduce the risk of foreclosure.[40] While several aspects of blockchain possess the potential to bring pro-competitive effects and help market players grow more efficiently thereby promoting competition in a market[41] but a substantial possibility of sharing sensitive information in form of data and resorting to concerted practices exhibits the potential to raise anti-competitive concerns.

Data-driven developments

The collection of data generates huge datasets commonly known as “big data.” Big Data is produced at high speed from multiple sources which are subsequently subjected to powerful processors and algorithms for its handling and analysis.[42] If such data is fed and processed through systems that use artificial intelligence, machine learning and automated decision-making, it results in comprehensive upgrades in such systems[43] giving them certain competitive advantages. Blockchains, as they store and analyse data to provide better services, might become the undefeated enemy of competition law due to their data storage.

Additionally, according to the Organisation for Economic Co-operation and Development (**“OECD”**), big data is a core economic asset having the potential to create a significant competitive advantage for companies and drive innovation and growth.[44] Further in this context, the CCI, in the case of ***Matrimony v. Google***[45] has noted that data can be turned into any number of revenues generating artificial-intelligence-based innovations.[46] A majority of the data-driven businesses incorporate multi-sided platforms where one or more sides of the platform are designed to attract user presence and the other sides are used for monetising the data relating to user behaviour.[47] The OECD further points out that data-driven markets can lead to a “winner takes all” situation where extreme market success leads to concentration in the market.[48] Concerns arising from the use of such data extend to the privacy of the consumers.

Concerted Practices and Privacy Concerns

Recently, the CCI released a report on ***Market Study on Telecom Sector***[49](**“Telecom Study”**)

wherein it discussed data privacy and competition and recognised privacy as a competitive factor. The use of such data without the prior consent of the users undermines consumers' privacy.[50] Privacy concerns arising in competition law have also been recognised in the European Union. Article 20 of the General Data Protection Regulation (**"GDPR"**) ensures data protection by limiting the processing of data without consent.[51]

Blockchains are both public and private, anti-competitive concerns may arise from both types. Firstly, public blockchains which are anonymously hosted allow everyone to read and validate data, such open data access evidently raises privacy concerns for the owners of those data. Privacy being a competitive factor makes the arising concern anti-competitive in nature. Secondly, private blockchains which are hosted by private servers and give access to only authorised participants raise the suspicion of exchange of sensitive information and concerted practices. These authorised participants have access to both public and private blockchains which provide them with an opportunity to cherry-pick the useful information for their use and bring data-driven modifications or developments. Additionally, private blockchains act as secure medium run by algorithms which prevent detection of activities undergoing through that medium. Having an access to such huge and diverse data and an undetectable medium implies having a mechanism to avoid competition regulation. Thus, the risks arising from blockchains might not seem as paramount and dangerous as they are. The Competition authorities will have significant difficulties in identifying the anti-competitive conducts undertaken through blockchains.

CCI or blockchain: Who is dominant?

The pseudonymous nature and opacity effect of a blockchain will pose significant challenges before the CCI. First, such aspects of a blockchain will deprive the competition authority of taking *suo moto* actions because the information about any actual or potential anti-competitive conduct might not reach the CCI and its inability to extract such information will add to its incompetency. Second, blockchain does not involve human-element for its functioning, it rather uses algorithmic mechanisms for all its progressions. As much as the authorities would wish to resolve the disputes arising herein, the Indian competition framework does not include any provision to shoot dead the automated riders.

The Act requires the involvement of human element to provide any relief in such cases. As it is prominent from the case of ***Samir Agarwal v. ANI Technologies,***[52] wherein the CCI has held that algorithmically determined prices do not lead to collusion or cartelisation within the meaning of Competition law. Notably, every process involved in the functioning of a blockchain is algorithm based which will certainly create a quandary for the Indian competition watchdog.

Additionally, a lack of a provisional mechanism to assert and recognise potential anti-competitive concerns will be yet another barrier in noticing and resolving concerns emanating from the use of blockchain. A pertinent decision of the CCI in this context is the case of ***Plasser India v. Harbour Sales Pvt. Ltd.,***[53] wherein CCI decided that a mere possibility of potential collusion does not show anti-competitive conduct, hence cannot be dealt with under the realm of Section 3 of the Act. The decisional practice of the CCI demonstrates a lack of pro-activeness. However, even if we consider CCI to be extremely diligent and proactive, it does not seem that it is equipped to deal with the varieties of difficulties that might arise from the use of blockchain applications.

The way forward

The efforts of CCI in recognising the potential concerns emanating from the utilisation of blockchain technology stay extremely commendable. However, the mere acknowledgement of anti-competitive concerns will not ensure a resolution of such concerns. Consequently, there exists a dire need for a provisional mechanism to incapacitate and deter the emergence of such concerns. Although it becomes evident that blockchain falls under the ambit of the Act yet the existing provision under Section 3 might not suffice to resolve the disputes arising therein.

Remarkably, the CCI does not consider the use of algorithms to raise competitive concerns whereas blockchain technology uses algorithms for almost every transaction. More so, the pseudonymous nature of such transactions will be the requisite escape for such algorithms to avoid competitive regulation. Consequently, the CCI should widen the ambit of Section 3 of the Act to regulate the use of algorithms and do away with the requirement of human-element while determining and rendering conducts and activities as anti-competitive in nature.

---

[1]Ernesto Rengifo Garcia, 'Blockchain and Competition law', *GRUR International*, Vol. 70(2), (February 2021), https://academic.oup.com/grurint/article-abstract/70/2/113/6032580?redirectedFrom=fulltext.

[2] OECD, 'Blockchain Primer', *Organisation for Economic Cooperation and Development*, (2018) https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf.

[3] *Id.*

[4] Almudena Arcelus, Mihran Yenikomshian and Noemi Nocera, 'Commentary, Mitigating Antitrust Concerns When Competitors Share Data Using Blockchain Technology', *Harv. J.L. & Tech. Dig.*, (2021), http://jolt.law.harvard.edu/digest/mitigating-antitrust-concerns-when-competitors-share-data-using-blockchain-technology.

[5] United American Corp. v. Bitmain Inc. et al, Case no. 1:2018cv25106; *Gallagher v. Bitcointalk.org,* Case no. 3:18-cv-05892.

[6] Section 2(h), Competition Act, 2002.

[7] *In Re: Dilip Modwil and Insurance Regulatory and Development Authority, Case No. 39 of 2014; In re: Shri Shubham Srivastava and Department of Industrial Policy and Promotion, Case No. 39 of 2013.*

[8] Section 2 (l), Competition Act, 2002.

[9] Section 2(h), Competition Act, 2002.

[10] Section 2(u), Competition Act, 2002.

[11] Section 3, Competition Act, 2002.

[12] Section 2(b), Competition Act, 2002.

[13] Builders Association of India v. Cement Association of India and Ors., Case No. 29 of 2010.

[14] *Id* at 2.

[15] *Id* at 1.

[16] Section 32, Competition Act, 2002.

[17] OECD, 'Antitrust and the Trust Machine', *Organisation for Economic Cooperation and Development*, (2020), https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf.

[18] OECD, 'Blockchain Technology and Competition Policy-Issues paper by the Secretariat', *Organisation for Economic Cooperation and Development*,(2018), https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf.

[19] *Id* at 4.

[20] *Id* at 17.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] Jacques Derenne, Michael Hofmann and Ciara Barbu- O'Connor, 'Blockchain and EU Competition Law', *Sheppard Mullin Richter and Hampton* (11 January 2021), https://www.jdsupra.com/legalnews/blockchain-and-eu-competition-law-9904251/.

[25]Compliance Manual for Enterprises, *Competition Commission ofIndia*, (2017), https://www.cci.gov.in/sites/default/files/manual_compliance/manual_booklet.pdf.

[26] Section 3, Competition Act, 2002.

[27] *Id* at 13.

[28] In Re: Alleged Cartelisation in Flashlights Market in India, Suo Motu Case No. 01 of 2017.

[29] In Re: Cartelisation in Industrial and Automotive Bearings, Suo Motu Case No. 05 of 2017.

[30] Lin William Cong and Zhiguo He, 'Blockchain Disruption and Smart Contracts', *NBER Working Paper No. 24399*, (2018).

[31] *Id* at 13.

[32] Thibault Schrepel, 'Collusion by blockchain and smart contracts', *Harvard Journal of Law and Technology*, Vol. 33 (1), (2019).

[33] I. Lianos, 'Blockchain Competition – Gaining Competitive Advantage in the Digital Economy: Competition Law Implications', *Ph. Hacker, I. Lianos, G. Dimitropoulos& S. Eich, Regulating Blockchain: Political and Legal Challenges*,Oxford University Press, (2019), https://www.ucl.ac.uk/cles/sites/cles/files/cles_8-2018.pdf.

[34] Eliza MIK, 'Smart contracts: Terminology, technical limitations and real-world complexity', *Law, Innovation and Technology*, Vol. 9(2),Research Collection School Of Law, (2017), https://ink.library.smu.edu.sg/sol_research/2341.

[35] Hyundai Motor Company and Kia Motors Corporation, Combination Registration No. C-2019/09/682.

[36] *Id.*

[37] Matrimony.com Ltd. v. Google LLC, Case No. 7 & 30 of 2012, ¶ 86.

[38] Patrick Moorhead, 'Why your Personal Data is the New Oil', *AdAge*, (10 November 2011), http://adage.com/article/digitalnext/personal-data-oil/230932/.

[39] *Id.*

[40] Morten Nissen and Martin von Haller Grønbæk, 'Blockchain technology and competition law – issues to be considered', *Bird & Bird* (2018), https://www.twobirds.com/en/news/articles/2018/global/blockchain-technology-and-competition-law-issues-to-be-considered.

[41] *Id* at 18.

[42] P. Hustinx, 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition law and Consumer Protection in the Digital Economy', *European Data Protection Supervisor*, (March 2014), https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf.

[43] UNCTAD Secretariat 'The value and role of data in electronic commerce and the digital economy and its implications for inclusive trade and development', *United Nations Conference on Trade and Development*, (23 January 2019), https://unctad.org/meetings/en/SessionalDocuments/tdb_ede3d2_en.pdf.

[44] OECD, 'Data Driven Innovation: Big Data for Growth and Well-Being', *Organisation for Economic Cooperation and Development*,(2015), Data-driven innovation for growth and well-being – OECD.

[45] *Id* at 38.

[46] *Id*, ¶86.

[47] Jaadhu-Facebook/Jio Platforms Ltd-Reliance Industries Limited, Combination Registration No. C-2020/06/747, ¶11.

[48] Pedro Gonzaga and Ania Thiemann, 'Big Data: Bringing Competition Policy to the Digital Era', *Organisation for Economic Cooperation and Development*, (27 October 2016), https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf, ¶50.

[49] Market Study on the Telecom Sector in India, *Competition Commission of India*, (22 January 2021), Market-Study-on-the-Telecom-Sector-In-India.pdf (cci.gov.in).

[50] Dina Srinivasan, 'The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy', *Berkeley Business Law Journal*, (2019), 16 BERKELEY BUS. L.J. 39, 70.

[51] Art. 18, 20, General Data Protection Regulation, 2016.

[52] Samir Agrawal v. ANI Technologies, Case No 37 of 2018.

[53] Plasser India v. Harbour Sales Private Limited, Case No 45 of 2019.

This entry was posted on Wednesday, May 5th, 2021 at 10:40 am and is filed under Algorithms, Blockchain, India
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.