COMPETITION LAW IN THE DIGITAL WORLD

PART IV: BLOCKCHAIN

TABLE OF CONTENTS

INTRODUCTION

Blockchain is a general-purpose application of distributed ledger technology (DLT) that has the potential to disrupt traditional markets and institutions. Blockchain is touted to be the next revolution after the advent of the internet. Blockchain technology essentially allows every person who is part of the network to verify the details of a transaction (for instance, how much money was paid to whom at what time) since a common "ledger" where all the transactions are recorded are "distributed" to every participant in the system, who individually verify the veracity of the transactions. This removes the need for an intermediary or central authority (such as a bank) having to provide details of any particular transaction and acting as repositories of trust. Where the internet has greatly democratized information by enabling easy publication and transfer of information, blockchain attempts to decentralize the authentication of ownership over assets, by making them unique, traceable, and facilitating digital transfer and trading of assets by providing trust in the transaction and reducing uncertainty. Increasing consolidation of power in various sectors such as financial and digital markets had led to a growing distrust in our institutions. This was further exacerbated after the financial crisis in 2007, which led to many losing trust in the established banking systems. While Bitcoin was one of the first applications of blockchain technology and was the world's first "cryptocurrency", not requiring its users to trust in any central authorities, the underlying technology's fundamental features such as distributed consensus and reliability made more and more businesses take note of this emerging technology. Further, a fundamental risk with centralized systems is that they have a single (or a few) point of failure. A distributed system such as blockchain solves this problem by making it harder for hackers, or any bad actors to leverage the system to the detriment of its users.

In the first part of this trend, we will attempt to give a very rudimentary understanding of what a blockchain is and how it functions. Understanding how what blockchain is and the basic concept behind it is important and useful to appreciate the interface between competition law and this emerging technology. We will first explain try to understand the fundamental technology driving blockchain, i.e., distributed ledger technology in brief. Thereafter, we will try to understand what a blockchain is and the rules that are used to verify authenticity of transactions in a distributed system without a central authority to verify them (the consensus mechanisms). We will then point out the different types of blockchains that are implemented and how and to what extent can these different systems possibly determine the participants conduct within a blockchain.

The second part will attempt to outline the possible issues that competition regulators are likely to face in the future. However, at the outset, it is important to declare that businesses across industries are yet to warm up to the idea of implementing blockchain technology in their businesses. The mass adaptation of the technology is still awaited, and while there are a number of projects that have implemented blockchain successfully providing a proof-of-concept for increasing efficiencies and reducing costs, scaling the technology to the degree where it becomes a traditional mode of conducting business is still something that the industry is trying to solve. As a result, the evaluation of competitive risks in such a nascent industry would necessarily have to rely on conjecture. However, our assessment of competition law concerns is nevertheless derived from the fundamental concept behind a distributed system which may be implemented by stakeholders with varying degrees of openness of the system.

Part – I : BLOCKCHAIN – UNDERSTANDING THE BASICS

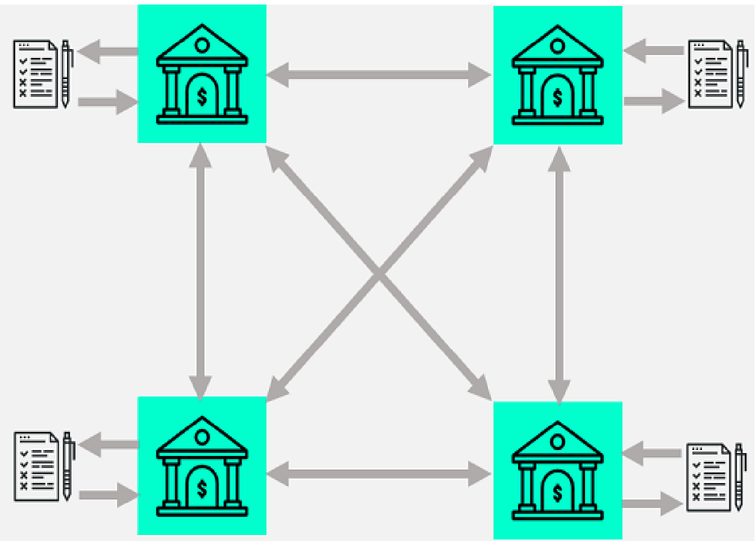
There are various levels at which the concept behind blockchain can be understood. We will try to explain what blockchain is, and the basic idea behind it without taking a deep dive into the technicalities and the computational processes that build and operate blockchain systems. However, in order to develop a meaningful understanding, we would have to understand, at a very basic level, how the system works.

Present literature defines blockchain as a decentralized, distributed ledger system wherein transactions are recorded and verified via a peer-to-peer consensus mechanism. To anyone not familiar with blockchain, there is a lot to unpack in this statement, so let us start from scratch.[1]

- **Distributed Ledger Technology**

[1] A basic, but excellent introduction to the concept is given by Lorne Lantz, “TED Talks: The Blockchain explained simply”, available at: https://www.youtube.com/watch?v=KP_hGPQVLpA

Blockchain is one application of distributed ledger technology (**DLT**). DLT is essentially used to maintain a decentralized database (i.e., the ledger). The important distinction between traditional technology used to create and maintain databases and DLT is that in the case of the latter, the database is decentralized, i.e., distributed across several users of the technology. In theory, this eliminates the need for a central authority or intermediary to process, validate or authenticate transactions.[2] This has important implications and is one of the idiosyncrasies that differentiate DLT from traditional technologies. Being a decentralized system, there is no central authority which approves and maintains a record of the database. These functions are, instead, delegated to the users of the DLT-based service.[3] Users of the DLT-based service are basically computer systems or what are referred to as 'nodes' in a distributed system. Typically, these records are only stored in the ledger when these users reach a consensus that a particular entry must be added to the record. The technology provides a verifiable and auditable history of all information stored on that particular dataset.[4]



- **How do transactions come to be recorded in this ledger?**

For a transaction to be recorded in the ledger, the users of the DLT-based service must agree to record the transaction on their copies of the ledger. Generally, in a DLT-based service, every node maintains the ledger. Therefore, if any data changes happen, the ledger is updated by all nodes synchronically and continuously, therefore making the process decentralized by not requiring any single authority or system to

[2] In this publication, we shall use the term transaction as a short hand for any information that may be stored in the database / ledger. This could, therefore, range from details of traditional transactions to medical records.

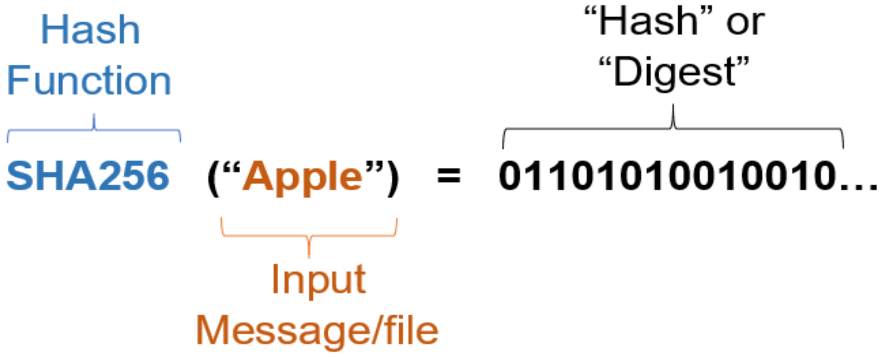
[3] Our common understanding of a user of a service remains the same. However, in a DLT-based service, the user is also one of the stakeholders in the system and in most cases plays an integral role in maintaining the system.

[4] https://tradeix.com/distributed-ledger-technology/

record these changes. The updating takes place independently at each node. These nodes can use various mechanisms to verify and reach a common conclusion regarding the veracity of transactions on the ledger. The process by which nodes can arrive at this "consensus" is called the "consensus mechanism". Each transaction recorded in the ledger is made secure by encrypting transactions using cryptographic hash functions.

- **How are these transactions secured in the absence of a central authority?**

Transactions in a DLT-based system are secured using Cryptographic Hash Functions. A cryptographic hash function is an algorithm that takes an arbitrary amount of data input – a message or a transaction, for instance – and produces a fixed-size output of enciphered text called a **hash** value, or just "**hash**."[5] A cryptographic hash function always gives the same output for a given input, but if you even slightly alter the input (the message), the corresponding hash changes completely.



For example, the SHA256 hash function gives the following hash for the word apple.[6] Notice how even simple changes in the spelling give completely different results, and a fixed output (32-byte output in case of SHA256) is given irrespective of the size of the input.

Input	Output or the Hash derived from SHA256
Apple	F223FAA96F22916294922B171A2696D868FD1F9129302EB41A45B2A2EA2EBBFD
apple	3A7BD3E2360A3D29EEA436FCFB7E44C735D117C42D1C1835420B6B9942DD4F1B
appl	58B06AC1DDD4448423E6C9A1C5640FF3866E1553489A5CD2362EB4E14954EE84

[5] Shai Halevi and Hugo Krawczyk, Randomized Hashing and Digital Signatures, available at: https://www.ee.technion.ac.il/~hugo/rhash/

[6] One can check the hash for any given input at http://onlinemd5.com/

The hash of this sentence	9357FB3ABA9532EAF96329C38CF13DE30696A59E1F27E6456A192D4356FA429D

A cryptographic hash function encrypts the message in a secure manner so that it becomes infeasible to compute the contents of the message in reverse direction, given the hash of the message.[7] We say *infeasible* and not *impossible*, because in theory, there is no hard proof that states that the input is hard to compute in the reverse direction. It is just that no one has developed a way to do so till date. This essentially means that one cannot guess the input "Apple" from its encrypted message digest without expending significant amounts of computing power that would in most cases render the enterprise of trying to decrypt the message futile.

- Reaching a Consensus and the Byzantine General's Problem

From our discussion so far, it can be observed in theory, it is extremely important for the functioning of a distributed ledger system that nodes agree upon whether a transaction is to be recorded in a ledger or not. However, distributed systems face a fundamental problem in reaching this consensus in a in a hierarchy-free and failure-prone network because of the possibility that a computer system or node may fail and there is imperfect information across the other nodes regarding whether a failure has in fact occurred at a node. It is difficult for the other nodes to declare if a particular node has failed and to therefore shut it out of the network, because they need to first be in agreement regarding which component has failed in the first place. In order for a particular system to continue functioning, computer systems must come up with mitigation strategies in order to ensure that the

[7] Decrypting a message which has been encrypted using the SHA256 hash function for instance, would require the computer to make 2^{256} guesses.

entire system does not stop functioning. This problem is commonly known as the "Byzantine Fault" or the Byzantine generals' problem.[8]

The mitigation strategy employed by a particular system to ensure that a byzantine fault does not lead to complete system failure, it must have a Byzantine Fault Tolerance (BFT). There are many cases of byzantine faults in distributed systems, ranging from simple faults such as one in which the node fails and stops operating to more complex ones where nodes may deliberately Respond with a misleading result or Respond with a different results to different nodes. It is important to note that byzantine faults are not necessarily caused by bad actors in a system and can be caused by purely physical latencies (for e.g. network congestions).

In distributed systems such as DLT-based systems, this central problem is how to decide and establish the agreed list, and correct order, of transactions. Since the technology is distributed, individual transactions are sent to the network through one particular node. This node is then required to pass the transactions on to other nodes. Because of physical latencies, not all nodes see the same transactions at the same time, so each node may build its own order of transactions based on which ones it receives first. All nodes being equal "citizens" in the DLT-based system, there is, as such, no authoritative order of transactions. However, a decision is required to be made as to which node's version, or any version, of the state of the ledger (that is to say the order of transactions) shall be the authoritative one that is shared by all the nodes.

The Byzantine General's problem is therefore stated as *how can a distributed network of computers / nodes agree on a decision if some of the nodes are likely to fail (or are acting dishonestly)?*

- **How are Systems Made Byzantine Fault Tolerant?**

A system is said to develop BFT when it is able to continue operating even if some of the nodes fail or act maliciously. That is to say, the nodes employ a method of arriving at a consensus on which transactions and in which order, to commit to the ledger in a distributed ledger system despite some nodes in the system malfunctioning. The mechanism through which these nodes reach this important consensus is called a

[8] The Byzantine General's Problem, LESLIE LAMPORT et al.

Consensus Mechanism or a Consensus Protocol. There are various methods that DLT-based systems may employ to ensure BFT, such as Proof of Work[9], practical Byzantine Fault Tolerance, etc.

- **Enter: Blockchain**

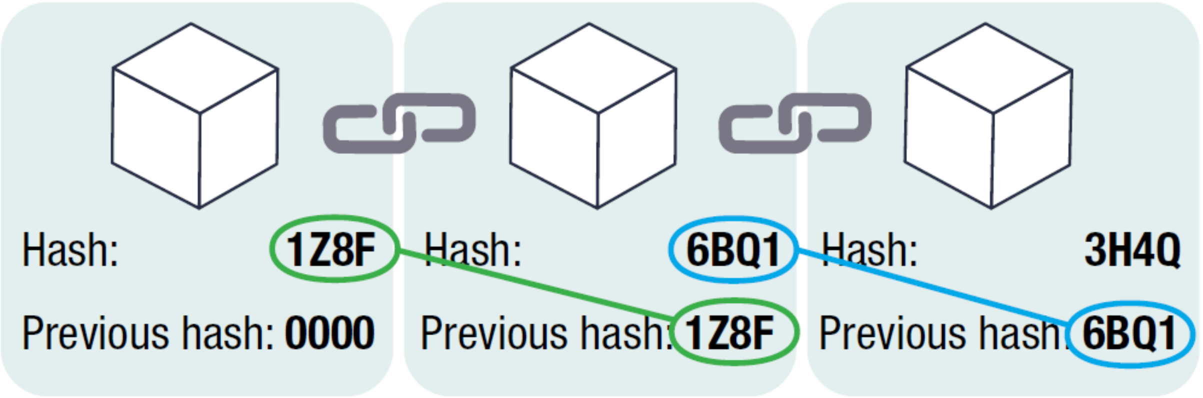
If one understands the broad working of a distributed ledger system as explained so far, it is sufficient to understand what Blockchain is. Blockchain is nothing but the application of DLT. DLT is the architecture employed for operating and maintaining a blockchain, which maintains a ledger of transactions distributed across nodes in the system. Characteristic of a DLT system, the ledger is not controlled by any single authority and is maintained between parties in the system with a focus on verifying the record of transactions using various consensus mechanisms and ensuring that the database is immutable, i.e., resistant to tampering by individuals.

Fundamentally, blockchain is a combination of already existing technologies that together can create networks that secure trust between people or parties who otherwise have no reason to trust one another.[10] Specifically, it utilises DLT to store information verified by cryptography among a group of users, which is agreed through a pre-defined consensus mechanism, often without the authorisation of a central authority. This combination allows users to transfer data and value across the blockchain system, without the need for trust in a central authority (in contrast to how traditional financial transactions are done with central banks acting as repositories of trust).

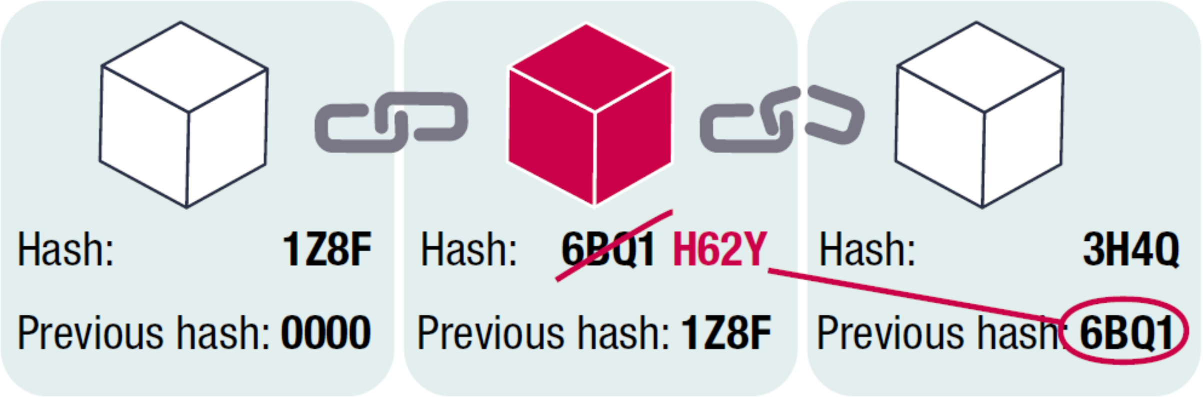
Each 'block' in a blockchain is akin to a page in the ledger, which contains the messages/transactions. Apart from the message/transaction data, the block is also secured by a hash, which acts as a unique fingerprint for the block, and the hash function for the block preceding it.

[9] Proof of work is one of the most popular and common consensus mechanisms deployed in public blockchain systems such as cryptocurrencies. The concept was developed by Satoshi Nakamoto, the pseudonymous creator(s) of Bitcoin.

[10] OECD Blockchain Primer.



Tampering any data in a block (for instance, to alter any recorded transaction fraudulently), completely changes the hash of that particular block, thereby not allowing the next block to recognize the tampered block as part of the chain. This altered block would therefore not be recognized in the blockchain, allowing anyone to identify the exact transaction that was sought to be altered and maintaining the integrity of the chain.



- ### Types of Blockchain

While Cryptocurrency such as Bitcoin, Ethereum and many more are the most common and public facing enterprises utilising blockchain technology, there are many different types of blockchains that are developed to suit different needs. While there are a number of variable features, two of the most important are the "openness" of the platform (public or private) and the level of permissions required to add information to the blockchain (permissioned or permissionless).[11] The following table lays down the different types of blockchains succinctly[12]:

[11] OECD Blockchain Primer.

[12] Ibid.

Blockchain Types		Read	Write	Commit	Example
Open	**Public Permissionless**	Anyone	Anyone	Anyone	Bitcoin
	Public Permissioned	Anyone	Authorized Participants	All or subset of Authorized Participants	Supply chain ledger for retail brand viewable by public
Closed	**Consortium**	Authorized Participants	Authorized Participants	All or subset of Authorized Participants	Multiple banks operating a shared ledger
	Private Permissioned	Fully private	Network Operator only	Network Operator only	External bank ledger shared between parent company and subsidiaries

While implementing blockchain technology remains an esoteric business decision and we do not know when it will start being adopted across industries, there are a number of pilot projects and proof-of-concepts that have showcased the immense potential for the technology to increase efficiencies and reduce administrative, back-end costs for businesses. For instance, HSBC successfully financed a consignment of soybeans from Argentina to Malaysia using the Corda blockchain platform. It has been suggested that putting all of Asia Pacific's trade-related paperwork into electronic form could slash the time it takes to export goods by up to 44 percent and cut costs by up to 31 percent.[13] Similarly, pharmaceutical companies, insurance as well as logistics sectors can greatly benefit from the use of this technology and there are various different projects being implemented or tried at different stages.

Part – II: BLOCKCHAIN AND COMPETITION LAW

Blockchain technology has a potential to bring a lot of benefits in the market at a large scale. Some of these benefits can also be shared with competition authorities. It has been argued that utility of blockchains can extend to merger controls, cartel

[13] HSBC says performs first trade finance deal using single blockchain system, https://www.reuters.com/article/us-hsbc-blockchain-idUSKCN1IF01X

investigations and monitoring of abuse of dominance.[14] For example, if all the evidence regarding company that is relevant for merger can be traced in a blockchain, it will be easier for authorities to assess correct economic evidences. This will increase transparency and reduce chances of getting misinformed by the parties. Further, in cases of commitments, the authorities can monitor whether the parties are adhering to the commitments imposed. Similarly, in cartel investigations it may assist in case of leniency applications, where the applicant can provide all the economic evidences and history of transactions effectively to the authorities. Therefore, there are several benefits that blockchain technology offers for effective implementation of competition law. However, it is also necessary to see some of the anticompetitive activities that may be conducted using this technology. Further, issue regarding regulation, as discussed below, is also pertinent to understand at this stage to keep in mind whether the authorities should adopt a light touch approach to ensure maximum innovation and minimal intervention.

Even though the blockchain technology is at comparatively nascent stage and it may be difficult to foresee all the competition concerns at this stage, but there is a general understanding that blockchain technology will not completely eliminate anti-competitive practices and competition authorities will examine these issues in future. Moreover, due to their inherent properties, competition issues are more likely to arise in permissioned or private blockchains rather than public blockchain. This is because the consensus mechanism on which a public-permissionless blockchain works is very difficult to capture, thereby making it difficult to amend the protocol or tamper any of the blocks. For example, in case of Bitcoin, it requires consensus of 51% nodes, which is very difficult for a particular ‘bad actor’ to achieve. It is completely different in the case of private-permissioned blockchain where consensus mechanism can be pre-coded by the entities engaged in its creation, which may also give themselves a room to engage in unilateral change in governance of such blockchains. However, this does not mean that a public-permissionless blockchain would be completely immune to anti-competitive conduct. Ultimately, a blockchain records and verifies transactions according to its consensus mechanism. If an enterprise or a group of enterprise can

[14] BY AJINKYA M. TULPULE, ENFORCEMENT AND COMPLIANCE IN A BLOCKCHAIN(ED) WORLD, CPI Antitrust Chronicle January 2017

control that, they can engage in such conducts in garb of a decentralised ledger system.

It has been argued that miners (who are validators of a new block) may also collude among themselves.[15] There are already mining pools forming, which are groups of miners cooperating in return of sharing block rewards in proportion of their contribution.[16] Mining pools concentrate the power to one of the person who is owner of the pool.[17] Therefore, it is easier to collude with several mining pool owners and engage in anti-competitive practices since the channel is already established. There are around 20 major mining pools for bitcoin, with more than 80% of hash power with mining pools in China.[18] This goes on to show how public blockchains may not be as immune to anti-competitive practices as they may appear to be.

As of now there are more private consortia rather than public.[19] Therefore, in any case there is are several potential competition concerns that needs to be discussed. However, it is pertinent to note that the categorisation of blockchain between public and private might be too simple and as the technology develops, there may be several sub-categories or hybrid categories. For example, a new type of blockchain 'public-permissioned' blockchain is being developed which seeks to fill the gap between public-permission less and private consortium networks.[20]

Even though there can be multiple types of blockchain, we argue that it is not immune to anti-competitive practices as long as the consensus mechanism of such blockchain is something that can be captured. This this argument, we proceed to see what actual conducts may be considered anti-competitive in blockchains.

[15] Dr. Thibault Schrepel, Collusion by Blockchain and smart contracts, Pg. 135, https://ssrn.com/abstract=3315182

[16] https://www.buybitcoinworldwide.com/mining/pools/

[17] https://www.buybitcoinworldwide.com/mining/pools/

[18] https://www.buybitcoinworldwide.com/mining/pools/

[19] Renato Nazzini, The Blockchain (R)evolution and the Role of Antitrust, King's College London Dickson Poon School of Law Legal Studies Research Paper Series: Paper No. 2019-20

[20] https://www.linkedin.com/pulse/public-permissioned-blockchains-common-pool-resources-jesus-ruiz/

- **Innovation and efficiencies**

As discussed above, there are several benefits that this technology brings with itself. One of the biggest advantages that we could be seeing in future may be the supply sector. If effectively implemented, blockchain can bring in automated and better integrated inventory management. It has been noted that supply chain blockchains will be in demand due to 'increased cost savings, enhanced traceability and greater transparency.[21] Companies around the world have already started deploying pilot projects and proof-of-concepts are already working to incorporate blockchain in their supply chains. Maersk and IBM, for instance, are working on cross-border, cross-party transactions that use blockchain technology to help improve process efficiency.[22] Similarly, Mastercard and Envisible have partnered together to create a blockchain-based supply chain platform to help supermarkets trace the origin of seafood.[23]

Further, HSBC successfully financed a consignment of soybeans from Argentina to Malaysia using the Corda blockchain platform. It has been suggested that putting all of Asia Pacific's trade-related paperwork into electronic form could slash the time it takes to export goods by up to 44 percent and cut costs by up to 31 percent.[24] Similarly, pharmaceutical companies, insurance as well as logistics sectors can greatly benefit from the use of this technology and there are various different projects being implemented or tried at different stages.

Companies are trying to scale and apply the technology so as to increase traceability of products in a supply chain, and decrease the time taken from days to seconds. If

[21] https://www.mckinsey.com/business-functions/operations/our-insights/blockchain-technology-for-supply-chainsa-must-or-a-maybe#:~:text=For%20supply%20chains%20where%20participants,a%20higher%20level%20of%20traceability.

[22] https://www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens#:~:text=The%20TradeLens%20platform%20has%20been,across%20the%20global%20shipping%20industry.

[23] https://www.computerworld.com/article/3448399/mastercard-partners-to-launch-blockchain-based-food-supply-chain.html

[24] HSBC says performs first trade finance deal using single blockchain system, https://www.reuters.com/article/us-hsbc-blockchain-idUSKCN1IF01X

successful, tracing potentially hazardous food substances to a particular source such as a particular city or farm within a short time period would be a reality, allowing authorities to take effective steps and stay ahead of the curve in terms of managing cases where a disease may be highly communicable.

Imagine the intended and effective application of this technology in the midst of our current crisis. Even as countries around the world are in a race to develop a vaccine or cure to COVID-19, ensuring smooth and efficient delivery of the vaccine to the most needed parts in the world is an entirely different challenge. A successfully deployed blockchain technology which streamlines supply chains in vaccine production and delivery across the globe can be very efficient. Blockchain technology in our current crisis would have reduced manual work and provided us a better automated system, saving crucial time and resources.

- **Relevant Market and Market power**

There can be several issues pertaining to horizontal agreements, vertical agreements or abuse of dominance. However, before delving deep into these issues, it is pertinent to assess how the market could be determined in future. It is also the first step to determine as to whether an enterprise under question would have market power under what circumstances. There are several questions which may need to be answered by competition authorities. Would blockchain technology based services compete with other existing technologies or would they come under a separate market? Will each blockchain be considered separate in its own and dominant in themselves? Or will it be dependent upon number of users or transactions?

We may not be able to give an answer with complete confidence as of now as the technology itself is still developing. However, we can take an approach by considering all the basics of the relevant product market as provided under section 19(7) of the Competition Act, 2002 (‘the Act’). There must be difference in characteristics of blockchain and its substitutability. Considering that CCI has considered online market different from offline[25], it can be presumed in a similar way that blockchain market may be considered different from existing technologies because of the facilities that blockchain technology can provide. It has been suggested that the market should

[25] All India Online Vendors Association v. Flipkart India Private Limited and Ors, https://www.cci.gov.in/sites/default/files/20-of-2018.pdf

depend on the type of blockchain and type of applications run of that blockchain.[26] For example, blockchain for bitcoin will be completely different from a blockchain engaged in providing streamlined services for pharmaceutical companies.

Once the issue of relevant market is resolved, competition authorities may put liability upon the person involved in anti-competitive practices, who could be developers, users or miners.

- **Anti-competitive Agreements**

a) Horizontal Agreements – There are generally three categories of players involved in a blockchain. These are developers, users and miners. In this case, collusion will mostly depend on the mechanism that a blockchain will follow. There can be collusion amongst all the miners, developers or users depending upon whether the blockchain is permissioned or permissionless. For example, in a private blockchain if the consensus mechanism is present in a manner that it provides maximum control to group of developers, there could be a case of collusion among the developers. Similarly, in a public blockchain such as bitcoin, all the pool owners can decide to collude for any anti-competitive practice.

Controlling the consensus mechanism

Since a blockchain works on consensus mechanism, issue of collusion remains the prime concern. Especially in a private blockchain, since the protocols and consensus mechanism can be made in a way that essentially, control would rest with a limited number of people and not to the public. Using the same, such group of participants can alter the protocols of the blockchain without notifying other members, and eventually engage in practice of alteration of any transactions or information stored in any block. Once there is required consent in the chain, there can be a case of cartelization in such blockchain. Similarly, as discussed above, the same can be case in public blockchain if there is enough consent. For example, even though it may be difficult, but if one manages to establish coordination among majority of the mining pool owners, there is a possibility of collusion in bitcoin also.

[26] Dr. Thibault Schrepel, Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox (Georgetown Law Technology Review / 3 Geo. L. Tech. Rev. 281 (2019), Pg. 304 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3193576 (Blockchain Antitrust Paradox)

Exchange of sensitive information

Exchange of sensitive business information is another aspect which may be achieved through blockchain. Such exchanges through blockchains can be used to collude and engage in anti competitive practices. Since the information is publicly available in a blockchain, it will be easier for enterprises to share information through which all the enterprises may collude easily. Considering the information on a blockchain can be updated on a real time basis, it can be used by colluding firms for their own advantages.

Additionally, because of anonymity that blockchain offers, it may be difficult for competition authorities to identify offenders and regulate conduct.

Enforcement of Cartel

Cartels usually enforce their anti-competitive agreements by ensuring that no cartel member deviates from their fixed price. For this, deviator is often punished by compelling it to compensate harmed firms.[27] For the same purpose, information such as prices, sales data etc. are monitored on a regular basis, and data collection is a regular exercise in the whole process. Usually, cartel rely on self-reporting by a member for all the data that is being provided.

Herein, blockchain may help cartel to ensure that none of the members are deviating from cartel objectives. It may help cartel members to effectively share the data at a large scale and subsequently monitor the prices. The cartel will no longer have to rely on self-reporting by member firms and a transparent database in form of blockchain can be readily available for their evaluation.

It is pertinent to note that members of a cartel always have an incentive to deviate from the anti-competitive agreement in quest of capturing big profits. Therefore, cartels are usually difficult to sustain in long run.[28] Herein, it is pertinent to note that better monitoring of cartel will give more credence to existence of a cartel. In case of

[27] Joseph E. Harrington, Jr., How is a Collusive Outcome Enforced? Pg. 43, Department of Economics, Johns Hopkins University, Baltimore, MD 21218, USA, https://joeharrington5201922.github.io/pdf/fnt06.pdf

[28] CUTS INTERNATIONAL and NATIONAL LAW UNIVERSITY, JODHPUR, Study of Cartel Case Laws in Select Jurisdictions – Learnings for the Competition Commission of India, pg. 45-46, https://www.cci.gov.in/sites/default/files/cartel_report1_20080812115152.pdf

blockchain, the information is updated in a real time basis and complete history of transaction is recorded. Since all the information will be publicly available, it will be easier for a cartel to detect any deviant behaviour of any cartelist.

b) Vertical Agreements-

It has been observed in EU competition law jurisprudence that even a unilateral conduct, if accepted by other enterprise, can fall foul of concerted practice.[29] That being the case, blockchain network may be used to prohibit enterprises to act independently of their own in a vertically integrated market. Since the information is available publicly, it would be easier to identify any deviation from the prescribed practice. Such transparency can force other players to tacitly accept the conditions imposed by vertically upward players. For example, it can be used to prohibit dealers/ retailers to provide discounts to consumers as the information regarding discount will be updated and visible to everyone on the chain.[30] This may, in turn, lead to issues of resale price maintenance.

Hub and spoke cartel-

In Hub and spokes arrangements are a horizontal restriction where a 'hub' facilitates coordination amongst two or more spokes, thereby facilitating a cartel without direct contact between two horizontal players.

In a private-permissionless blockchain: enterprises can engage in hub and spoke cartel by establishing a link between two blockchains. For example, a distributor can be a member of two rival supply networks based on blockchain. Such distributor can be a link for flow of information between two enterprises, thereby facilitating freely transfer of information. Therefore, two enterprises working through two distinct blockchains can also coordinate effectively to engage in anticompetitive activities.

<u>Refusal to deal</u>

Similarly, in a private blockchain created by one or more enterprises, it may be decided to not deal with any distributor or retailer. Private-Permissioned blockchains are

[29] CASE AT.40428 – GUESS.

[30] *Supra* note 16, Pg. 130-131.

distinguished from public blockchains in that the ability to write and commit transactions, and thus enjoy the facilities of the system, depend upon the permission granted to a user to access the blockchain. Such cases of refusal to deal are more critical in cases where access to any network is essential for the business. There may be a situation that certain players as well are prohibited from accessing the blockchain. This would be considered as a refusal to deal that may be violative of competition laws.

There may be a situation that such restrictive policies may be justified in the name of efficiency. Such as to ensure that protocols regarding security are complied with. However, members of the blockchain must ensure that protocols of such blockchains are reasonable and fair, especially once the technology has attained a position where it becomes a necessary or substantial factor for competing in the market.

Tying

Furthermore, there can be an issue of tying supplementary products/ services that are outside the blockchain as a precondition to become a member of any blockchain. In this way, an enterprise or a group can engage in a traditional tie-in practices that may create adverse effect on competition, especially in a blockchain which is essential for any business. For example, there may be a situation that distributors of certain medicines are engaged in sale of drugs of certain pharmaceutical company, for which joining the blockchain of the company is essential. Herein, if the company decides to impose certain supplementary services unrelated to the core business, that may amount to tie-in and subsequently, may attract scrutiny under section 3(4) read with Section 3(1) on the touchstones of Section 19(3) of the Act.

Exclusive dealing

Exclusive dealing is an effective way to foreclose competition. Similar to a traditional case of exclusive dealing, a blockchain may engage in such practices where it restricts its members from joining any other blockchain parallelly. For example, a distributor of multiple products may want to register itself on multiple blockchains. In such a case, restricting such distributor may be amount to imposition of an unfair condition since it may be considered as an attempt to foreclose the competition.

However, it is again emphasised that factors of section 19(3) of the Act will have to be taken into consideration since there may be a case where exclusive dealing may be beneficial for market and consumer. In some cases, exclusive dealing may be required to maintain quality of a product or services, such as the market of car dealership.

Predatory pricing

Usually in a blockchain, pricing is the transaction fee to add a block. For example, the amount is paid to the miners who verify the transaction in case of public blockchains such as Bitcoin. As the technology is developing, there may also be different pricing methods for a member to be added on certain blockchains. Since protocols can be changed easily in private blockchain, pricing can also be changed accordingly to the competition by other blockchain, which can also be used to engage in predatory pricing and consequently to foreclose the market. For example, we can take a market where several small businesses outsource their transaction to blockchain companies for certain fee. If there are multiple blockchains competing for users, any blockchain company may choose to take loss in transaction fee by burning out of their own pockets. Subsequently, once the competition is eliminated, transaction fees can be charged again at usual or perhaps higher amount. Therefore, issue of predatory pricing may be similar to what we encounter in traditional anti-competitive practices.

Abuse of data

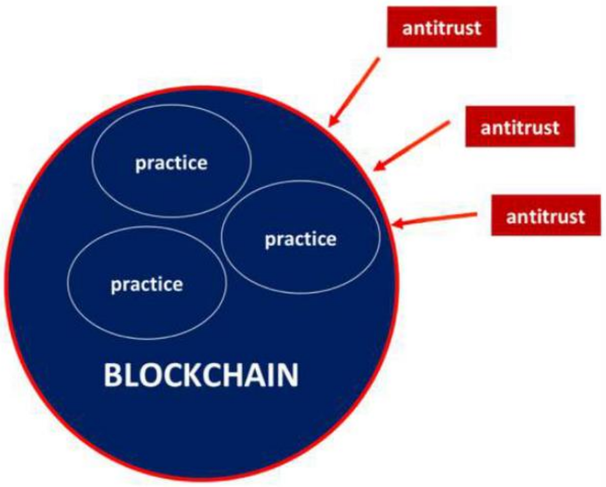
We argued in our previous trends that abuse of data can also be a competition issue and can invite investigation under the Act. Abuse of data would be more prevalent in private blockchains, mostly because of their nature of centralised control. It may be possible that an enterprise developing a blockchain may demand data from its users that are not required for the purpose of transaction. Such data can be used for other activities that developer is engaged into. Especially in cases where blockchain becomes an important service, mere collection of excessive data may be an anticompetitive practice. In this regard, we can see a recent decision by the Federal Cartel Office which fined Facebook for unfair collection of data, which was itself held to constitute an abuse of dominance and unfair terms of service.[31]

[31] 6th Decision Division B6-22/16, 06.02.2019

Further, data of users can be used without consent of members by those who control the 'consensus' mechanism of the chain. This is again most likely to happen in private blockchains. As discussed above, since developers can themselves hold the grip of consensus, they can change the protocols and collect the data within the transaction themselves. Concern will be greater in blockchains because data cannot be removed from the chain, unless it is decided by those who control the consensus mechanism.

- **Regulatory Issues**

One of the biggest concerns that come out are regarding regulation of blockchain. That because the blockchain is decentralised, immutable and anonymous, it might be difficult for competition authorities to regulate/ enforce competition law in blockchain regime.[32] Even though it would depend on the protocols on which a blockchain works, in many cases, for competition authorities to effectively regulate the blockchain, there has to be an intervention mechanism. However, at the same time, the core principles on which blockchain works must be respected in order to promote innovation.



The above chart shows that without having any intervention mechanism in place, competition authorities may not be able to take any action in certain blockchains. Source: Blockchain Antitrust Paradox

Once we decide that there has to be an intervention mechanism, the follow up question is that how can such an intervention mechanism be implemented? It has been pointed

[32] Blockchain Antitrust Paradox, Pg. 321.

out that for such implementation ‘law has to become code’.[33] This means that basic rules of governance must be implemented in the protocols of blockchain since from starting. However, for doing so, competition authorities must build trust that such an intervention measures would not be misused as that would kill the incentive to use the technology itself. It can be framed in a manner that identity of an individual would be only revealed in case of reasonable grounds that there has been any violation. It has also been that incentive to put in intervention mechanism may also include certain legal advantages such as tax incentives.[34]

The point that has to be taken into consideration while making such policy decisions is that the approach has to be a balanced so that it does not disrupt a new technology which is considered as revolutionary as internet. This can be achieved only by ensuring that core principles on which blockchain rests are not interfered with. Dr. Thibault Schrepel summarizes these principles into five points[35]-

a) Pseudonymity of members
b) Distributed ledger
c) Peer to peer transmission between members
d) Consensus mechanism
e) Data immutability, i.e. data cannot be altered or erased

There is no doubt that law always stays behind the technology. However, even though the technology of blockchain is yet to see a lot of development, if the concept of ‘law is code’ has to be included, it has to be done at early stage. This is more important in the case of public blockchain where it would be very difficult to change the protocols after a certain number of blocks in the chain.

Conclusion

Blockchain technology has the potential to be extremely beneficial and make markets function much more efficiently. There are many more advantages and issues that may be discovered as the technology matures and businesses try to meet the challenges of scaling blockchain technology. However, keeping this in mind, competition

[33] https://www.ellulschranz.com/blockchain-competition-law-compatible

[34] Blockchain Antitrust Paradox, Pg. 332

[35] Blockchain Antitrust Paradox, Pg. 330

authorities would have to be ready to not only evaluate the pro-competitive aspects of the technology and ensure that regulation of the technology doesn't lead to restriction of the technology, but at the same time to also scrutinize any anti-competitive practices that enterprises may engage in through this novel technology.

We have tried to put forth certain possible issues that may come up with greater implementation of blockchain technology in our day to day life. Giving a complete picture of the competitive landscape at this time would fall in the realm of speculation since mass-level adoption of blockchain is still some way into the future and the technology itself is developing and its adoption at enterprise levels is still at a very nascent stage. It is often said blockchain is as new to competition law as e-commerce was in 1990s. Therefore, there may still be sometime till we actually see any instance of anti-competitive case being dealt. However, we have attempted to highlight the various regulatory issues that authorities would have to address the moment we see the technology becoming mainstream. Even though the Competition Act is sufficient to deal with competition issues that may be posed by Blockchain, implementation of the same might be difficult considering the complex nature of the technology itself. It would be interesting to see how competition authorities across the globe deal the situation with development of technology in future.

CONTRIBUTORS

ABIR ROY

M: +91 7042101034
P: +91 11 48661126
E: abir@sarvada.co.in

Partner & Head, Competition Law, Sarvada Legal

Recognized as Leading Individual in Competition law by Legal 500 in 2017 and 2018, Future Leader by Whos Who Legal in 2019 and Recognized Practitioner by Chambers & Partners in 2019

Author of Competition law in India: A Practical Guide, Kluwer Law International, ISBN: 9041161392, 9789041161390

Author of Competition Law in India by Eastern Law House, ISBN: 9788171773442

ISHAAN CHAKRABARTI

M: +91 987 176 7687
P: +91 11 48661149
E: Ishaan.c@sarvada.co.in

Member -- Competition law team, Sarvada Legal

VIVEK PANDEY

M: +91 9810806250
E: vivek.p@sarvada.co.in

Member -- Competition law team, Sarvada Legal