Organisation for Economic Co-operation and Development

DAF/COMP/M(2018)1/ANN8/FINAL

Unclassified **English - Or. English**

12 November 2019

DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS
COMPETITION COMMITTEE

Executive Summary of the hearing on Blockchain and Competition Policy

Annex to the Summary Record of the 129th Meeting of the Competition Committee held on 6-8 June 2018

7 June 2018

This Executive Summary by the OECD Secretariat contains the key findings from the discussion held during the 129th Meeting of the Competition Committee on 6-8 June 2018.

More documents related to this discussion can be found at
http://www.oecd.org/daf/competition/blockchain-and-competition-policy.htm

Please contact Mr Chris PIKE if you have questions about this document.
[Email: chris.pike@oecd.org]

JT03454460

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Executive Summary of the Hearing on Blockchain and Competition Policy

By The Secretariat[*]

From the discussion at the hearing, the secretariat paper, and experts' written submissions, several key points emerged:

1. Blockchain or Distributed ledger Technology (DLT) is a shared ledger of transactions between parties in a network that is not controlled by a single central authority. It is a general purpose technology that crowd-sources verification services and therefore removes the need for a trusted third party to fulfil that role. It therefore has possible applications across a wide range of markets.

A blockchain is a shared ledger of transactions between parties in a network, not controlled by a single central authority. A ledger is like a record book: it records and stores all transactions between users in chronological order. Instead of one authority controlling this ledger (like a bank), an identical copy of the ledger is held by all users on the network, called nodes.

Blockchain, or Distributed Ledger Technology, as it is sometimes known, incentivises a pool of validators to assure users that a transaction has been completed. It creates trust by requiring a degree of consensus amongst these validators before a new block of transactions is added to the immutable ledger. The immutable nature of the ledger allows a product's history to be traced. There are two broad types of validator network that can verify an action:

- In a 'permissionless' blockchain, anyone with the right equipment can become a validator and so they can be numerous. The need for consensus incentivises individual validators to act honestly. Meanwhile the identity of users is pseudonymised so that validators cannot easily identify an individual user, though anybody can observe the actions that have been taken place on the blockchain between these pseudonymous parties. This removes the traditional need to hire a trusted third party (e.g. a notary), or to cover the transaction costs incurred by the parties agents (e.g. credit card firms) to verify an action.
- In a 'permissioned' blockchain, restrictions on who can be a validator are applied, leading to a smaller but perhaps more trustworthy pool of validators. The requirement on consensus across the pool of validators may also be relaxed, potentially leading to a single validator verifying the action of two pseudonymised users. In contrast to its permissionless variation where access to the blockchain's history was open to anybody (public), in a permissioned blockchain this may also be restricted to defined users.

While the most popular applications of blockchain have thus far been in the financial sector, the technology may become relevant to numerous other sectors, including legal services, notaries, data storage, energy and transport. Indeed it is already being used to improve

[*] This Executive Summary does not necessarily represent the consensus view of the Competition Committee. It does, however, encapsulate key points from the discussion, the issues paper, and the panellists' presentations.

global supply chains, and pilots are underway on its ability to authenticate the ownership of intellectual property rights, land rights, identity data, health records, online votes, pollution certificates, search query data, stock, pensions, insurance schemes and many other assets.

2. Like many new technologies before it, blockchain creates an opportunity to reduce prices, improve quality, and disrupt the market power of incumbent firms. It may also offers competition agencies opportunities to innovate in their own ways of working. For example, new types of remedies or pro-competitive regulations may become possible in cases where markets are not working well for consumers.

Blockchains create an efficient marketplace of validators that cost a fraction of the price that trusted intermediaries are currently able to charge for their services. It is true that the issue of the energy required to power permission-less blockchains still needs to be solved (one existing blockchain currently absorbs the average daily power usage of Norway). However, if this is possible then the magnitude of the reductions in transaction costs will challenge both existing payment systems and existing intermediaries, creating opportunities for new entrants and early adopters to thrive. While regulation may well be required this will have to be carefully designed in order that it does not remove the potential for pro-competitive efficiencies that the technology offers.

There are also opportunities for competition agencies from blockchain technology. In particular the possibility of an agency having its own node on a private industry blockchain might allow them to improve the effectiveness and efficiency of their investigations. For instance, agencies could receive real-time information on the market at zero marginal cost to market participants, allowing them to overcome the asymmetry of information that exists in most markets. For example they might monitor market outcomes, adherence to commitments, collect data for cases, and screen for suspicious patterns. It may therefore be something that agencies want to ask for in the design protocols of private industry specific blockchains.

Another possibility is that blockchain technology might offer agencies new options when they are looking for remedies in markets that they have studied. For example, like the drive for Open API standards in banking that followed a market study into banking in the UK, blockchain might help to stimulate competition in malfunctioning markets. In the case of blockchain this might involve removing regulatory barriers to the use of blockchains to set-up trusted automatic switching services, or to give users better control of their data, and in particular the ability to be paid for providing access to it. There might also need to be standards and regulations to ensure that data is portable between blockchains, though it did not appear that this was likely to emerge spontaneously from the market and hence pro-competitive regulatory intervention might be required if such a goal were to be achieved.

3. Firms are increasingly turning to a consortia model to explore blockchain solutions, and such collaborative efforts can be pro-competitive. However there are the traditional risks that such cooperation can lead to sharing of competitively sensitive information. Other potential risks include the use of collective boycotts to prevent rivals joining a blockchain, or the use of the blockchain to store collusive agreements. Given the additional transparency and trustworthiness of transaction data on a blockchain it may also be the case that tacit coordination becomes easier to monitor and hence more stable.

Firms are increasingly turning to a consortium model to explore the possible efficiency of blockchain solutions. These are often, but not always, industry-based permissioned blockchains and so often feature collaboration between competitors. In such cases there is often a pro-competitive rationale for efforts to cooperate to improve efficiency, for instance by creating industry standards that allow firms to reduce their costs and improve the efficiency of supply chains. However as in any joint R&D project there are the traditional risks that cooperation to develop the technology will spill-over into the sharing of competitively sensitive information. As such traditional compliance measures by firms participating in such projects will be necessary.

Beyond information sharing there is a potential risk that consortia members might engage in a collective boycott that prevents a rival from using or joining a blockchain that becomes essential to competing within a supplychain. While collective boycotts are often treated as hard-core infringements it is also the case that there is no general duty to admit a rival to a blockchain consortia. For instance such rivals might be developing competing technologies and thus admitting them to the consortia might undermine efforts to compete to innovate. Such boycotts would therefore only be a concern where the blockchain had become a de facto standard.

Finally while blockchains might be used to store collusive agreements, it is unclear why traditional tools such as dawn raids would not be able to deal with this in the same way that they have had to adapt to the use of whatsapp groups and private email addresses to coordinate cartels.

A distinct concern is that if all transactions move onto blockchains the information that is made visible on a blockchain might be such that it enables oligopolists in downstream markets to tacitly coordinate. This is a potential risk not only on those permissioned blockchains developed by consortia, but also public permissionless blockchains. The visibility of such information to agencies and regulators would mean firms are unlikely to make information on future strategies visible. However, the increased transparency on prices, and perhaps more importantly the increased confidence that those prices are the prices at which transactions occurred and not simply list prices, combined with the use of algorithms that use those transaction prices to optimise profits, might improve the ability to monitor prices and hence increase the stability of tacit coordination amongst downstream oligopolists.

4. There are a number of particular challenges in investigating abuse of dominance by a blockchain. For instance, it is at first sight not always clear who would be liable for any such conduct, and this could create practical difficulties for enforcement. In addition, identifying dominant positions would itself require careful consideration of the nature of the different competitive constraints upon a blockchain. However, the nature of the competitive concerns over exclusionary conduct are not particularly different from those that are found in other markets and hence the tools and analytical frameworks for examining them remain broadly the same.

In order to investigate an abuse of dominance involving a blockchain, an agency would need to consider who would be liable for the behaviour of a decentralised blockchain. For instance would it be the developers who originally created the blockchain and its protocols, or the users who, by validating entries on the blockchain according to their chosen set of protocols in effect control the evolution of those protocols and hence the ‘decision-making’ of the blockchain.

In the case of a private permissioned blockchain the answer might simply be the consortia who both created and continue to operate the blockchain. However in a public permissionless blockchain there is the additional issue that the users are numerous and pseudonymous. This creates a number of practical difficulties in enforcing against such a blockchain. Not least how to sanction it and how to put a stop to the harmful conduct if the perpetrators remain unknown.

To prove dominance agencies would need to consider the market in which a blockchain operates, once possibility is that this might be all the blockchains with applications which allow you to take a taxi in Paris. However, taxi users might substitute between these and non-blockchain-based taxi services, while blockchain validators might substitute between that blockchain and a similar one that provides the same service in London, or a blockchain that provides an electricity trading service in Madrid. Competitive constraints on both sides of the market would therefore need to be considered.

The types of conduct might then be those exclusionary strategies that are familiar from more traditional markets: tying, refusal to deal, loyalty rebates and discounts, predatory pricing and margin squeeze. The visibility of these strategies on public blockchains might make them less likely than on private permissioned blockchains, whose behaviour is also easier to control. Overall, it would not appear to be a question of finding new instruments, but rather of adapting existing instruments to reflect the realities of these new production technologies.