Re: Competition and Consumer Protection in the 21st Century Hearings, Project Number P18120

To the FTC:

I hereby wish to submit my comments to the topic #9 entitled “The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics,” although I will focus on blockchain and predatory innovation which seems to belong here.

I. To take blockchain into account

I believe that blockchain is the biggest challenge faced by antitrust law in the last 20 years. In fact, the very nature of this technology raises fundamental questions for antitrust as we have never seen since the advent of the Internet, considering the fact that the very nature of blockchain raises fundamental questions for antitrust law. Because blockchain is decentralized, anonymous and immutable, multiple questions do in fact arise regarding the detection of practices as well as the identification of perpetrators. We show that some practices are de facto more likely to be implemented, but they are yet to be identifiable.

Practices

Several monopolization practices are very likely to occur on blockchain. Here is our best estimate that the following practices will soon appear:

---

Remedies

One of the major issues faced by antitrust law in the face of blockchain is related to the identification of anti-competitive practices. This problem is new and twofold. First, algorithms are drastically accelerating the implementation of anti-competitive practices. They create issues on how to detect such practices, and incidentally, how to address evidence. But when practices implemented by algorithms are identified, the perpetrator is generally known concomitantly. The second issue faced by antitrust law is relative to blockchain. As we have previously explained, blockchain is a technology that ensures the anonymity - called pseudonymity - of its users. These anonymous nodes create obstacles in terms of enforcement, in fact, the distributed network architecture of blockchain constitutes a real barrier to antitrust enforcement. No one is in control of public blockchains, but everybody is at the same time. For that reason, although a practice is seen as being anti-competitive, the author may remain unidentified.

In addition to the issue raised by pseudonymity, other issues occur in relation to the effectiveness of sanctions and remedies because there are no “choke points” on blockchain.

---

2 Computational law is that branch of legal informatics concerned with the mechanization of legal analysis (whether done by humans or machines), see http://complaw.stanford.edu/ and https://law.stanford.edu/projects/computational-law/.  
3 Gur Huberman, Jacob D. Lesnho & Ciamac C. Moallemi, Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System 37 (2017): “Monopolies are often regulated to prevent or at least mitigate their abuse of power. Bitcoin is not regulated. It cannot be regulated. It need not be regulated because individually the miners are price takers.”  
4 This issue has been raised in the past, at a time when Internet wasn’t “designed to reveal who someone is, where they are, and what they’re doing,” see Lawrence Lessig, CODE: AND OTHER LAWS OF CYBERSPACE, Version 2, 38 (New York: Basic Books, 2006).  
5 Indeed, Primavera De Filippi & Aaron Wright, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 44 (2018): “Blockchains thus enable the creation of autonomous software programs run through the collaborative effort of
Blockchain creates issues related to emergency measures due to the fact that injunctions against a decentralized autonomous organization are nearly impossible to be taken. The only way around, once again, would be to encode these measures into the blockchain’s governance.

More broadly, it will be necessary to ensure a sufficiently effective deterrent effect, because practices are immutable and written on the blockchain forever. And many other procedural questions will arise, as dawn raids usefulness which will be called into question insofar as the seizure of a single computer will not make it possible to go back to the source, added to the fact that all the data - the amount of a transaction, its object, the identity of the parties - will be encrypted and tear-proof. Questions also arise as to the territoriality of the law. Antitrust authorities could lack the ability to seize the organization’s assets or enforce an injunction. Blockchain users located outside of the country in which the legal action is brought could indeed refuse to grant access to the blockchain.

In short, if competition is maintained as it is today, it will quickly become ineffective for technical reasons that will not be possible to compel. Because of the need for regulatory infiltration,

---

For instance, Augur - “a decentralized oracle & prediction market platform” - has no central party that can stop its operation. This platform will continue to work even if governments get tough — and even if penalties are imposed on the original parties who develop or promote the blockchain. No “technically skilled people of goodwill” are needed to keep the blockchain going, in fact. Daaps cannot be shut down because there is no server to take down. They can only be modified under specific and technical circumstances.

Blockchain creates issues related to emergency measures due to the fact that injunctions against a decentralized autonomous organization are nearly impossible to be taken. The only way around, once again, would be to encode these measures into the blockchain’s governance.

More broadly, it will be necessary to ensure a sufficiently effective deterrent effect, because practices are immutable and written on the blockchain forever. And many other procedural questions will arise, as dawn raids usefulness which will be called into question insofar as the seizure of a single computer will not make it possible to go back to the source, added to the fact that all the data - the amount of a transaction, its object, the identity of the parties - will be encrypted and tear-proof. Questions also arise as to the territoriality of the law. Antitrust authorities could lack the ability to seize the organization’s assets or enforce an injunction. Blockchain users located outside of the country in which the legal action is brought could indeed refuse to grant access to the blockchain.

In short, if competition is maintained as it is today, it will quickly become ineffective for technical reasons that will not be possible to compel. Because of the need for regulatory infiltration,
fascinating debates of public policies are ahead of us on how to proceed. And we need to get to the subject quickly, because as Lawrence Lessig already underlined in 2006, "we are at a stage in our history when we urgently need to make fundamental choices about values, but we should trust no institution of government to make such choices."¹⁶ The good news is that if governments take too restrictive measures against blockchain, developers will move away to different countries. It is what happened with the BitLicense¹⁷ which is issued by the New York State Department of Financial Services, causing many startups to leave the State.¹⁸ If they cannot vote with their computers, developers will vote with their feet when they change territory. Let us not forget that.

**Competition via blockchain**

Network effects are often used in the literature on digital sectors.¹⁹ They are twofold - direct or indirect - the idea being that the more a technology is used, the more new users are encouraged to join the group.²⁰ This is a fairly classic mass effect that is also described as the Metcalfe’s Law in the context of information technology according to which the value of a network is approximately proportional to the square of the number of users (people plus machines) that are connected to it. When reaching a certain number of users, “the value exceeds the cost for the majority of potential users, and they start multiplying rapidly, increasing the value in total, and to other individual users.”²¹ That number effect is also described by the “Aggregation Theory”²² based on which “consumers are attracted to an aggregator through the delivery of a superior experience.”²³ The idea of experience here is added to the simple mass effect. So does the blockchain, thanks to its intrinsic qualities, allow network effects to be limited in time?²⁴ Is blockchain the “most viable way out from the antitrust trap created by Aggregation Theory”?²⁵ That is very likely²⁶ and if that were to be the case, “New Googles” will soon be created. We will explain.

¹⁶ He further adds that “the government we now have is a failure. Nothing important should be trusted to its control, even though everything important is,” Lawrence Lessig, Code: And Other Laws of Cyberspace, Version 2, 8 (New York: Basic Books, 2006).
¹⁷ See https://en.wikipedia.org/wiki/BitLicense.
¹⁹ Showing how network effect can positively and negatively affect social welfare, see Michal S. Gal, The Power of the Crowd in the Sharing Economy, LAW AND ETHICS OF HUMAN RIGHTS (Forthcoming, 2018).
²⁰ Also, on blockchain, as on current platforms, “reputation has emerged as one of the most vital facets of competition in many modern markets,” for more on that see John M. Newman, Complex Antitrust Harm in Platform Markets, CPI (2017).
²³ See id.
²⁵ Rhys Lindmark, Macro Blockchain #1: The End of Aggregation Theory, TOKEN ECONOMY (June 6, 2017).
With blockchain, the data is public and shared by the distributed ledger system. This structure is opposite to the client-server platforms as we know it, whose results are an acceleration of the competitive process to the extent that it creates an incentive to share information about the blockchain in order (i) to make it effective against third parties and (ii) to encourage other users to share information (sense of community). In the words of Fred Ehrsam, “while some blockchain-based data will be encrypted and private, much of it will also be open out of necessity…this open data has the potential to commoditize the data silos most tech companies like Google, Facebook, Uber, LinkedIn, and Amazon are built on and extract rent from. This is great for society: it incentivizes the creation of a more open and connected world. And it creates an open data layer for AIs to train on.”

The incentive system of public blockchain also creates a strong incentive to join it as soon as possible, contrary to what happens on digital platforms as we know them today. It results in a weakening of these platforms against blockchains whose users have an interest in quickly joining the community — and not only once the network effect is created. This difference between “network effects” and “token effects” (network effects on blockchain) also lies in the fact that tokens help “overcome the bootstrap problem by adding financial utility when application utility is low,” as it is summarized in the following figure.

---

27 As underlined by Eric Posner, Marx and Weber have argued that market—or, capitalism—undermines community, see Eric A. Posner, LAW AND SOCIAL NORMS 221 (Cambridge, MA: Harvard University Press, 2009). Blockchain, which is driven by capitalism, proves this analysis to be incorrect.

28 Fred Ehrsam, Blockchains are a data buffet for AIs, MEDIUM (March 6, 2017).


30 Which is more than partially inspired by Chris Dixonn, see id.
In fact, token effects sort out the bootstrapping problem by creative different sorts of incentives. Initial Coin Offerings are one of them because they drive the buyers to make the blockchain prosper in order to make their tokens valuable. Other blockchains give away tokens, which is called an “airdrop.” We can imagine all kinds of conditions to get these tokens for free: the creation of an account via a social network in order to share some information as the contact list, proof of the possession of other tokens, for example, which may possibly create anti-competitive concerns.

As a result, interest in joining a new blockchain can be extremely high, potentially putting rapid and powerful competitive pressure on market leaders. It’s factors like these that antitrust authorities will have to take into account when deciding if a company is engaging in anti-competitive practices. We know the competitive environment tech giants are engaged in today, but it’s not clear yet how blockchain will challenge them tomorrow. This shouldn’t stop authorities from acting when there’s clear, established harm to consumers, but it raises at least two fundamental questions: how to evaluate whether a company is truly dominant and how competition authorities should be allocating their resources.

II. To recognize predatory innovation as such

Conventional wisdom assumes that antitrust law mechanisms are well suited to the study of practices in technology markets and that only adjustments should be made to these mechanisms, and sparingly at that. This is untrue. Several practices fall outside the scope of antitrust law because mechanisms for assessing the legality of practices are not adequate. In fact, no one can accurately identify a typical legal approach for non-price strategies, a truth

31 For instance, Steemit - a decentralized Reddit-like token network - makes payments to users who post and upvote articles.


34 But see Christian Catalini & Catherine Tucker, Seeding the S-Curve? The Role of Early Adopters in Diffusion 1 (2016): “We then show not only that natural early adopters are more likely to reject the technology if they are delayed, but that this rejection generates spillovers on adoption by their peers who are not natural early adopters.”

35 For instance, Mstoken, Bethereum, Sharelectric, Xriba, ConcertVR, Blockport, Wr, Articlex. For more details see What new ICOs are giving away free tokens right now?, QUORA. To track them, see https://airdropalert.com. See also Paul Vigna & Michael J. Casey, THE TRUTH MACHINE: THE BLOCKCHAIN AND THE FUTURE OF EVERYTHING 103 (St. Martin’s Press, 2018): “Brave’s model included a token-issuance strategy for dealing with that challenge. It set aside a 300 million-strong “user growth pool” to attract new users. There’s a plan, for example, to deliver a small amount of BATs to the integrated Brave wallet whenever there’s a unique new download of the browser. In this way, the token is designed as a tool to bootstrap adoption, to foster network effects.”

36 This is also called “coin drop,” see Melanie Swan, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 73 (O’Reilly Media, 2015).


which gives way for a chaotic jurisprudence to emerge from this lack of universal understanding.

There is, indeed, little published literature on the subject of the new anti-competitive strategies nestle in these markets. The process of competition generally encourages companies to lower their prices, which benefits the consumer. And yet, in certain specific cases, antitrust rules intend to sanction predatory prices because they eliminate the competitive process itself. A similar situation applies to innovation. Innovation is one of the main bases for competition between companies and it is beneficial to consumers who may enjoy new products which are also better suited to their needs. But certain “innovative” behaviors are considered as being predatory and are punished accordingly, despite the fact that no legal concept specifically addresses this issue.

This absence of a legal category specifically dedicated to anti-competitive practices disguised as “innovation” leads judges to create numerous type I and II errors. The jurisprudence didn’t yet generalize the etiquette of “predatory innovation,” which nevertheless answers some of the modern problems encountered by antitrust law with high-tech markets development. In fact, most predatory innovation practices are currently addressed under the label of “technological tying.” The creation of some legal rules dedicated to predatory innovation would lead to removing this legal concept and to create a more coherent legal regime.

We propose applying the “enhanced no economic sense” test to non-price strategies, including to predatory innovation. Without creating numerous type-I or II errors, this test results in the creation of a uniform rule of law, which will ultimately increase consumer welfare by encouraging companies to continue innovating.

III. The two combined: blockchain and predatory innovation

Blockchain (I.) and predatory innovation (II.) can be combined to cause great harm to the consumer, notably by ejecting competitors from the blockchain.

When the blockchain governance is modified, it could be seen as an innovative practice — being a new product. Such a situation is similar to the one of a software company uploading the new version of one of its products. And where there is innovation, there is a risk of “predatory innovation” which we define as “the alteration of one or more technical elements.

---

41 Peder Østbye, *The Case for a 21 Million Bitcoin Conspiracy* (March 2018): “certain stakeholders may have a more influential roles than others. As just explained, block-validators play such a role. There is a risk of concentration among such validators, which increases their influence. If changes in the protocols are to be implemented, it is ultimately the block-validators that must execute these changes.”
of a product to limit or eliminate competition.”

Predatory innovation takes the form of a real innovation - it’s a new version of a product/technology - but is not. In short, predatory innovation encompasses all anti-competitive strategies that, under the guise of being real innovations, aim at eliminating competition without benefiting consumers or users.

In the words of Vitalik Buterin — Ethereum creator, “the consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc.”

This is predatory innovation through blockchain. Such practices are expected to be more common on private blockchain where a change in the rules is easy and does not require any approval from the users. In fact, immutability is a characteristic that is shared only among open decentralized peer to peer blockchains and it does not apply to private blockchains. Accordingly, private blockchains can modify their governance design anytime as they do not need to convince any user to adopt the change. And predatory innovation could be made on public blockchains as well if the new governance design is adopted by a majority of the miners. But this seems unlikely at this time, first, because any change to the public blockchain governance design requires coordination and consensus among all of the stakeholders, and second, because it is impossible to “replace” the original blockchain. When it is done, a “hard fork” is created, a copy of the ledger is made and miners switch their hardware (hashing capacity) to the new governance design. If they do not, the software running under the old rules see the blocks produced according to the new rules as invalid, which creates a situation in which the original blockchain is split into multiple blockchains. Therefore, as the community grows on public blockchains, it becomes increasingly more difficult to reach a consensus on changing governance.

But let us already note that the future introduction of new governance models in public blockchain will reduce these difficulties and thus facilitate predatory innovation.

In addition, there are reasons to believe that predatory innovation may be particularly effective on blockchain, and therefore, a common practice. First of all, predatory innovation on blockchain is cheap as it can be implemented at no cost. Its implementation can also be very fast, in fact, interactions/validations via blockchain only take a few seconds or minutes at most.

---


43 Vitalik Buterin, *On Public and Private Blockchains*, Ethereum Blog (August 7, 2015) https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. In fact, this is a “godmode.” The blockchain owner can freeze any account or move the funds away; but chances are that people will eventually discover it and sell all the stocks/securities/tokens.

44 But still, no rule is set in stone, since they can all be modified with a broad consensus.

45 This subject is being discussed. The creation of an hard fork depends on the governance system. Some blockchains, according to the chosen governance, will thus allow a modification of governance without the creation of hard forks.


47 To read about the Ethereum “hard fork,” see Kevin D. Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, Berkeley Tech. L.J. Forthcoming: “Whether or not the Ethereum Foundation made the right call, the is that the controversy raised questions that could not be answered within the framework of the blockchain. They required appeal to some higher-level principles. The viability of trustless trust is ultimately a matter of governance.”

Although transactions and modification are not invisible on public blockchain, they can be on private blockchains — the access to information and the history of the blockchain can be limited to some users. And predatory innovation on blockchain can have a radical effect: it will produce immediate effects by excluding a targeted user which also is a competitor. Lastly, predatory innovation practices can take different forms with multiple effects, beyond the mere exclusion from the blockchain. A company that owns a private blockchain can indeed modify its governance design so that a user’s access is purely and simply denied, or, to a lesser extent, that the user can no longer read all the information on the blockchain, register transactions or take part in the block validation process. Of course, a badly designed blockchain operating rules to the detriment of some users would be unattractive, hence the interest to modify it once its adoption is generalized or to make some transactions not visible by all.

Here lies a similar problem to the one related to the platforms that we know today. The modification of blockchain governance may create issues while the initial choice of the type of blockchain - public, private… - should be exempt from antitrust scrutiny, although the type of governance that is chosen indicates the likelihood of anti-competitive practices being committed. But what is particularly worrying is that our legal concepts are blind to the full extent of this type of practice. Two concepts are generally used to analyze what is actually predatory innovation — tying and leveraging, but they are ineffective. Tying is inoperative to the extent that, with blockchain, only one product is involved. Moreover, it may not be sold - at least its access - and for this reason too, tying would be ineffective. Leveraging is unenforceable as well because, in the absence of two separate markets, it cannot be used. This concept is also ineffective when only one competitor is foreclosed but a wide competitive field remains active.

In short, predatory innovation is - for the time being - subject to several legal rules that are ill-adapted. And yet, it is one of the most anticipated and dangerous anti-competitive unilateral strategies that can be implemented on a blockchain. This should raise questions about the need to adapt our legal rules to a blockchain — and more broadly, about the role of the regulator.

**********

I remain at your disposal to talk about these subjects further,
Sincerely,

Prof. Thibault Schrepel

52 See Schrepel.