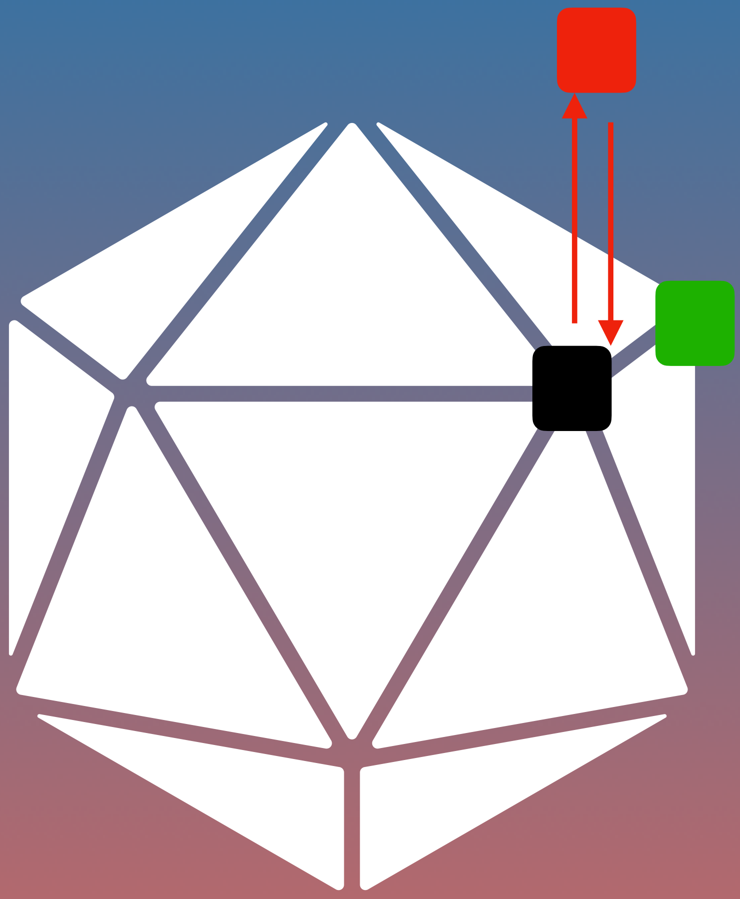
Antitrust in case of a 'Blockchain Denial of Service': Tackling a new form of collusion



Ardi Kaars
5777631
05 March 2021
Course: Blockchain Antitrust
Seminar-lecturer: Dr. Thibault Schrepel
1996 words

Table of contents

I. Introduction

The usage of public permissionless blockchains for the trade of cryptocurrencies have become increasingly popular in the last few years. As recent as 2021, Bitcoin was trading $60,000 per coin, followed by a drop to around $50,000[1]. This sudden drop of price is another sign of Bitcoin's volatility, besides a previous major crash that took place in the winter of 2017 to 2018, in which the coin's value dropped from around $19,000 to $6,500 in May 2018.[2] In a permissionless ledger, anyone may enter the blockchain as a user or miner.[3] In principle, that means it is publicly available. But there are circumstances in which a level playing field ceases to exist, and recent study by Cornell Tech and Technion Israel has shown something previously deemed impossible within blockchains: Blockchain Denial of Services.[4] This attempt to take over a blockchain and cause a full shutdown, or decrease in value, differs from previous attacks on blockchains in the following respect: Whereas previously a majority of mining power was required to force a shutdown, in this case only a fraction is needed. And the principle behind it differs, as the former requires forceful use of a dominant position, whereas the latter rests on incentivising rational miners to obtain a shutdown. With this method, a coin can be devalued or shut down to attract users for a different coin of higher value, thereby capturing market share at the expense of the shutdown coin.[5] In light of antitrust law, the question is: How should liability be assigned in case of a Blockchain Denial of Service?

Our hypothesis is that new forks should be designed that detect and sanction an initiator of a BDoS within the blockchain. In addition, existing antitrust law should be used to establish whether a BDoS serves anticompetitive behaviour between competing blockchains.

This paper explores the implications BDoS has for competition between blockchains. We use cryptocurrencies as a reference point and argue that the initiator of a BDoS should be treated according to competition law on cartels, that is, in light of article TFEU 101 in the EU, and the Sherman Act in the US. At the same time, a blockchain itself should address the anticompetitive practice, to the extent that actors within the blockchain are affected. This is even more relevant when cryptocurrencies become an accepted method of payment on markets for goods and services. For example, Elon Musk on behalf of Tesla recently announced that Bitcoin would become an accepted currency for purchasing Tesla cars.[6]

[1] Billy Bambrough, Bitcoin Price Prediction: How Far Could The Bitcoin Bull Run Go?, Forbes, Feb 25, 2021, 03:40am EST, https://www.forbes.com/sites/billybambrough/2021/02/25/bitcoin-price-prediction-how-far-could-the-bitcoin-bull-run-could-go/

[2] Author unknown, *Bitcoin BTC, Coinmarketcap,* https://coinmarketcap.com/currencies/bitcoin/

[3] Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers, 25 RICH. J.L. & TECH., no. 1, 2018, 21

[4] Michael Mirkin et. al., 2019, *BDOS: Blockchain-Denial-of-Service.* https://arxiv.org/pdf/1912.07497.pdf

[5] Id, at §8.1

[6] Matt Ott, *Tesla Buys $1.5 B in Bitcoin, will accept as payment soon,* AP News, Feb 25, 2021. https://apnews.com/article/tesla-buys-billion-bitcoin-061817c6795e75d1c3c9e9d6cfc4a911

II. The definition and discovery of a Blockchain Denial of Service

In October 2020, Mirkin et. al., on behalf of Cornell in collaboration with Technion Israel, brought forward a research into the ability to shut down a blockchain by altering its reward mechanism.[7] In the first place, classic Denial of Service attacks were found to be unlikely, as the decentralised nature of blockchains require at least 51% of mining power for a shutdown.[8] Such an attack may occur on smaller coins, yet for larger cryptocurrencies such as Bitcoin, that is much harder to achieve due to the continued costs of upholding such mining power.[9]

However, their newly discovered Blockchain Denial of Services was found to use a fraction of the mining power: 21% on 13 March 2020[10]. And instead of overloading the blockchain, this DoS incentivised other miners to quit by creating a new block, perceived to be faster.[11]

The creation of new blocks occurs in rounds, whereby the scheduler of the rounds randomly appoints a miner to generate a new block. The probability to be chosen is proportional to mining power. Each round can be won either by one of the rational miners, or, and adversary, of which there is only one. If a rational miner wins, the scheduler contacts the adversary first. Otherwise, it simply communicates the new block to the other miners. This gives the adversary an advantage, and a probability to provide a header with a Proof of Work showing more power than any of the other miners in the block. This way the system can be cheated. If the adversary wins, the adversary decides whether to publish the block or just its header. Accordingly, the profitability of mining decreases for the other miners when i) the adversary can prove itself faster, or ii) has received information about the winning rational miner, so that it has the option to respond with an even faster block.[12] In a worst case scenario, the command *stop* is the most profitable option left for the miners. That leads to a full shutdown of the blockchain.[13] Although synthetic thus far, a BDoS proves public blockchains with Nakamoto consensus to be vulnerable.

III. Two traitors in our midst

Firstly, within the given setup, miners inside the blockchain cannot determine the adversary, neither collusive behaviour between scheduler and adversary. The communication between the adversary miner and the scheduler constitutes a coordinated action aimed at reducing the profits of all other competitors. Hence, it is a necessity to make software adjustments that enable detection.

[7] The Block, *A newly-described blockchain denial of service' attack could convince miners to stop mining,* CoinMarketCap, Dec 8, 2020, 08:18 GMT+1, https://coinmarketcap.com/nl/headlines/news/blockchain-denial-of-service-attack-miners/

[8] Id. 5 §2

[9] Id.

[10] Id. §8.5

[11] Id. §3.1

[12] Id.

[13] Id. §5

IV. Market definition and the theory of granularity: symbiosis between law and code

Secondly, in general, public permissionless blockchains are found to be less susceptible to anticompetitive behaviour than private ones, due to the visibility effect.[14] The newly discovered possibility of a BDOS violates that assumption. This BDoS attack was said to be possible on blockchains that are based on a 'Nakamoto'-like consensus mechanism[15], which is by definition a public blockchain.[16]

The miners that respond to the BDoS initiator cannot meaningfully prove the validity of the transactions on which the BDoS attacker bases its Proof of Work, and hence the visibility effect does not apply. Therefore, detecting and sanctioning this abuse within the blockchain requires incorporating the theory of granularity. This theory approaches a blockchain as a market whose boundaries are set by developers, and in which core players, who have an incentive to collude rather than compete, can affect the blockchain as a whole. This group is called the nucleus.[17] Such an approach justifies a detect and sanction mechanism within the blockchain.

Yet on top of that, the shutdown puts the blockchain (with its corresponding coin) at a competitive disadvantage. In other words, the market on which this event can be used illegitimately to the benefit of competitors, includes competing blockchains. This part of the anticompetitive practice falls outside the scope of the granularity concept, and extends the issue into the sphere of existing antitrust legislation as well. Such a symbiosis is in line with the findings of Dr. Schrepel on granularity.

V. Proper classification: where antitrust law comes into play

Thirdly, collusive nature of a BDoS brings us into the realm of antitrust law on cartel behaviour. Both Section 1 of the Sherman Act[18] and Article 101 TFEU[19] outlaw any form of collusive behaviour that restrains trade within their respective geographic areas. The market for cryptocurrencies will be affected in case of a shutdown as mentioned. Based on the EU's definition on cartel behaviour, a BDoS should be considered an application of dissimilar conditions to equivalent transactions. After all, the adversary and scheduler communicate to outperform the most powerful block, whereas the other way around is not the case, despite the random probability assigned to both of them.

Yet the anti-competitive object can only be established outside of the blockchain, as the attack alone does not result in profits. Mirkin et. al. argue that the attack can be used by a

[14] Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox.* 3 GEO. L. TECH. REV. 281 (2019) , at 308

[15] Id. 13 §2

[16] Id. §1

[17] Thibault Schrepel, THE THEORY OF GRANULARITY A Path for Antitrust in Blockchain Ecosystems, Jan 29, 2020. https://ssrn.com/abstract=3519032 at. 37

[18] Djordje Petoski, *United States Cartels Comparative Guide,* Mondaq, Feb 17, 2021. https://www.mondaq.com/unitedstates/anti-trustcompetition-law/890398/cartels-comparative-guide

[19] 2009 O.J. (L 115) 88

user from a competing coin that gains attractiveness after the attack, or a shortseller who can profit from a shutdown.[20]

Hence the illegal, anti-competitive nature of a BDoS becomes clear. But harder to establish is a solid precedent of blockchain in antitrust law. In the US, so far there have been two cases: *United American Corp. v. Bitmain* and *Gallagher v. Bitcointalk.org.* What these cases have in common is a lack of substantial evidence of anti-competitive behaviour.[21] A detection of a BDoS in conjunction with behaviours mentioned above, could break that trend and create precedent.

VI. Absence of fiduciary relationships: blame the others, but do it right

Additionally, it is nearly impossible if not undesirable to hold miners, nodes and exchanges to account for losses resulting out of a BDOS. If these parties were to be held responsible, a fiduciary duty should be established in the first place.[22] This would be contrary to the entire nature of a decentralised blockchain, where each user establishes trust on an individual basis, in interaction with its peers.[23] On those grounds, liability should exclusively rest with the scheduler and the adversary.

VII. Cryptocurrencies and their increasing market share: do not ignore

Fifthly, cryptocurrencies are an expanding market. As of 15 February 2021, cryptocurrencies have reached a market capitalisation of $1.5 trillion.[24] Of that amount, 600 billion USD is occupied by bitcoin, one of the coins on which a BDoS would work. When a substantial part of the market for cryptocurrencies is subjected to coordinated devaluation of coin value, the systemic risks are unforeseen. As Nassim Taleb points out, "It’s more effective to focus on the consequences—that is, to evaluate the possible impact of extreme events. Realizing this, energy companies have finally shifted from predicting when accidents in nuclear plants might happen to preparing for the eventualities."[25] In that light, preparing the cryptocurrency market against anticompetitive behaviour makes sense, hence antitrust matters.

VIII. Pseudonimity and burden of proof: not so fast

The potential targets of a BDoS are publicly accessible blockchains. Anyone may enter through a Public Key Identication, and access shall be granted. User and miners can

[20] Id. 5

[21] Thibault Schrepel, *The first case of "blockchain antitrust": Gallagher v Bitcointalk.org,* Concurrentialiste Journal of Antitrust Law, May 28, 2020. https://leconcurrentialiste.com/first-case-blockchain-antitrust/

[22] https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1468&=&context=ripl&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Den%2526as_sdt%253D0%25252C5%2526q%253Dbitcoin%252Bantitrust%2526btnG%253D#search=%22bitcoin%20antitrust%22

[23] Chelsea D. Button, The Forking Phenomenon and The Future of Cryptocurrency in the Law, 19 UIC REV. INTELL. PROP. L. 1 (2019), at. 27-31

[24] Zack Voell, *Market Wrap: Crypto Market Cap Breaks $1.5T as Buyers Show Up for the Dip*, Yahoo! Finance, Feb 15, 2021, 21:03 UTC. https://finance.yahoo.com/news/market-wrap-crypto-market-cap-211704223.html

[25] Nassim N. Taleb et. al., *The Six Mistakes Executives Make in Risk Management,* Harvard Business Review, October 2009. www.hbr.org, at. 1

hence operate in relative secrecy. It is therefore questionable whether blockchains in their current form can meaningfully detect the perpetrators of a BDoS, let alone sanction them.

If we assume that pseudonimity, one of the five core principles of blockchain[26], will prevail, it should be borne in mind that detection software has gained ground. Furthermore, it is very well possible that compliance with official rules require abandonment of pseudonimity. Creation of new, non-pseudonymous forks, could hence ensure government compliance and detection/deterrence of BDoS, and incentivise tracking software to decode potential fraudsters when pseudonimity is upheld.

IX. Lurking legal arbitrage opportunities

Imposing antitrust law from the geographical area on which the scheduler operates poses a threat as well. It is inherent to the difficulty of establishing a geographical area, that a scheduler has incentive to operate from a jurisdiction with little restrictions on cartel behaviour. A 2013 study by Ivaldi et. al. indicates that developing countries on average have 19% penalty in excess of profits, versus 26% in the EU. For Pakistan, this amount was only 3%.[27] This adds to the difficulty of establishing a BDoS cartel case in the first place.

However, this can be solved for by including the regimes of the most highly affected geographical markets in establishing an antitrust case. The 'Brussels effect' has enabled the EU to set global standards on antitrust[28], and hence a significant geographical area covered by the cryptocurrencies market has antitrust safeguards similar to that of the EU (and US).

X. Conclusion

As apparent from the analysis, the scheduler and adversary in a BDoS should be treated as a cartel. However, harder to establish is the geographical area and the jurisdictions to be used for enforcement. Given the fact that cryptocurrencies are being traded worldwide, so is the systemic impact a BDoS can have. Therefore we propose that new forks be made to cope with this issue, and experimentation with forks that abandon pseudonimity. Once successful, its creation and release will improve the resilience of a coin against BDOS in two ways: through the new fork's improved algorithm and by splitting up the coin into more forks, thereby making the systemic risk of one BDOS on one fork smaller (provided the coin value has not changed). The development of new software was largely outside the scope of this paper, and hence further research is required.

[26] Id. 14 at. 330-332

[27] Mark Ivaldi et. al., *Cartel Damages to the Economy: An Assessment for Developing Countries.* Centre for Economic Policy Research. https://cepr.org/sites/default/files/Ivaldi%20-Cartel%20Damages%20061214.pdf , at. 7

[28] Anu Bradford, *The Brussels Effect,* 107 NW. U. L. REV. 1 (2012). https://scholarship.law.columbia.edu/faculty_scholarship/271

XI. Bibliography

[1] Billy Bambrough, Bitcoin Price Prediction: How Far Could The Bitcoin Bull Run Go?, Forbes, Feb 25, 2021, 03:40am EST, https://www.forbes.com/sites/billybambrough/2021/02/25/bitcoin-price-prediction-how-far-could-the-bitcoin-bull-run-could-go/

[2] Author unknown, *Bitcoin BTC, Coinmarketcap,* https://coinmarketcap.com/currencies/bitcoin/

[3] Jean Bacon, Johan David Michels, Christopher Millard & Jatinder Singh, Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers, 25 RICH. J.L. & TECH., no. 1, 2018, 21

[4] Michael Mirkin et. al., 2019, *BDOS: Blockchain-Denial-of-Service.* https://arxiv.org/pdf/1912.07497.pdf

[5] Id, at §8.1

[6] Matt Ott, *Tesla Buys $1.5 B in Bitcoin, will accept as payment soon,* AP News, Feb 25, 2021. https://apnews.com/article/tesla-buys-billion-bitcoin-061817c6795e75d1c3c9e9d6cfc4a911

[7] The Block, *A newly-described blockchain denial of service' attack could convince miners to stop mining,* CoinMarketCap, Dec 8, 2020, 08:18 GMT+1, https://coinmarketcap.com/nl/headlines/news/blockchain-denial-of-service-attack-miners/

[8] Id. 5 §2

[9] Id.

[10] Id. §8.5

[11] Id. §3.1

[12] Id.

[13] Id. §5

[14] Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox.* 3 GEO. L. TECH. REV. 281 (2019) , at 308

[15] Id. 13 §2

[16] Id. §1

[17] Thibault Schrepel, THE THEORY OF GRANULARITY A Path for Antitrust in Blockchain Ecosystems, Jan 29, 2020. https://ssrn.com/abstract=3519032 at. 37

[18] Djordje Petoski, *United States Cartels Comparative Guide,* Mondaq, Feb 17, 2021. https://www.mondaq.com/unitedstates/anti-trustcompetition-law/890398/cartels-comparative-guide

[19] 2009 O.J. (L 115) 88

[20] Id. 5

[21] Thibault Schrepel, *The first case of "blockchain antitrust": Gallagher v Bitcointalk.org,* Concurrentialiste Journal of Antitrust Law, May 28, 2020. https://leconcurrentialiste.com/first-case-blockchain-antitrust/

[22] https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1468&=&context=ripl&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Den%2526as_sdt%253D0%25252C5%2526q%253Dbitcoin%252Bantitrust%2526btnG%253D#search=%22bitcoin%20antitrust%22

[23] Chelsea D. Button, The Forking Phenomenon and The Future of Cryptocurrency in the Law, 19 UIC REV. INTELL. PROP. L. 1 (2019), at. 27-31

[24] Zack Voell, *Market Wrap: Crypto Market Cap Breaks $1.5T as Buyers Show Up for the Dip*, Yahoo! Finance, Feb 15, 2021, 21:03 UTC. https://finance.yahoo.com/news/market-wrap-crypto-market-cap-211704223.html

[25] Nassim N. Taleb et. al., *The Six Mistakes Executives Make in Risk Management,* Harvard Business Review, October 2009. www.hbr.org, at. 1

[26] Id. 14 at. 330-332

[27] Mark Ivaldi et. al., *Cartel Damages to the Economy: An Assessment for Developing Countries.* Centre for Economic Policy Research. https://cepr.org/sites/default/files/Ivaldi%20-Cartel%20Damages%20061214.pdf , at. 7

[28] Anu Bradford, *The Brussels Effect,* 107 NW. U. L. REV. 1 (2012). https://scholarship.law.columbia.edu/faculty_scholarship/271