Working paper

The transparency explosion

Parallel behavior using blockchain and “algorithms” in light of market transparency

Nadine Rinderknecht

October 29, 2021

Competition law (EU), parallel behavior, quantitative and qualitative transparency explosion, general and blockchain algorithms, “transparency-based” parallel behavior

010001101100000111011110001110010
0100111000110001010011110100100101101011
0110001100110011001100000110000101101100
01100010001101000100100000110001100110010
001010000011101010110111001100100
0110011101100101011001110110010101101110
011001000110100101100101
0101010001110010011000010110111001110011
01110000001100001011100100110010101101110
0111101000101001

About the cover

The transparency explosion is shedding light on what is often a dark competitive environment. What will be its impact? Will it promote competition or restrict it? And what will be its effects on parallel behavior? As will be shown, this paper seeks to address the last question in particular.

Table of contents

List of figures

All sources used were last accessed on October 29, 2021.

1 Introduction

Transparency is, by far, the best regulator. It optimizes prices and the quality of goods and services, and it requires management to report its activities under the watchful eye of the public.[1]

1 Like everything else in this world, transparency has its sunny and dark sides. In some cases – as mentioned in the quote above – market transparency optimizes price and quality. In other cases, it optimizes nothing less than a collusive equilibrium that may lead to increased price levels and lower quality. Market transparency therefore requires a consideration which is as differentiated as it can itself produce the most diverse effects. In addition, the overall picture must not be forgotten, since market transparency should be placed in the larger context of competitive conditions. However, neither can be done in this short paper, as will be outlined in more detail.

2 At the same time, the above quote was not made in general, but in a very specific context: the blockchain. Interestingly, this technology has a dual role. Firstly, the blockchain creates transparency with regard to the transactions stored in it. This is especially true in the public blockchain that anyone is free to access, but also for the private blockchain, although the circle of authorized readers is limited there. Blockchain-based transparency (together with other competitive conditions) may induce companies to engage in parallel behavior. Second, blockchain can technically implement parallel behavior, for example, using smart contracts. As a result, the blockchain is both driver *and* means of parallel behavior. However, this paper does not comprehensively address either market transparency or blockchain. Rather, the following two research questions deserve more in-depth treatment:

- **What are the key elements that – combined with blockchain – may lead to increased market transparency in quantitative and qualitative terms?**
- **What are the main types of parallel behavior that can be technically implemented with blockchain?**

3 Indeed, increased market transparency – and with it the danger of increased and more aggressive parallel behavior by algorithms – has already been discussed countless times. So often that it can be considered a "publication bias".[2] Outside of algorithmic (tacit)

[1] Silver Charles, How The Transparency Of Blockchain Drives Value, Forbes Technology Council of February 14, 2020, available at <https://www.forbes.com/sites/forbestechcouncil/2020/02/14/how-the-transparency-of-blockchain-drives-value/?sh=4f0fd6a531a6>.

[2] Schrepel Thibault, The Fundamental Unimportance of Algorithmic Collusion for Antitrust Law, Harvard Journal of Law and Technology, February 7, 2020, available at <www.jolt.law.harvard.edu/digest/the-fundamental-unimportance-of-algorithmic-collusion-for-antitrust-law>.

collusion, however, there are largely unexplored areas – and not coincidentally, a subset of them corresponds to the two research questions listed above. First, as far as can be seen, the combination of blockchain (data[3]), big bata analytics and trust economy has not yet been discussed. This is surprising in that this "explosive mixture" favors a transparency explosion that could eclipse the currently thematized market transparency, especially in the realm of algorithmic collusion, in both quantitative and qualitative terms. Second, while collusion is increasingly being addressed in the context of blockchain, it is primarily on the basis of explicit collusion. Parallel behavior is only being addressed in limited instances in the context of blockchain-based increases in transparency as a driver of greater and more aggressive parallel behavior. As far as can be seen, blockchain as a *technological means* to implement parallel behavior has not yet been addressed. This paper aims to contribute to both of these areas.

4 To this end, the components of the "explosive mixture" are first described, followed by a description of the transparency explosion in quantitative and qualitative terms. However, the phenomenon of the transparency explosion must also be put into perspective (chapter 2). The next two chapters introduce the "classical" parallel behavior (chapter 3) and the "modern" parallel behavior by means of algorithms (chapter 4). Based on this, "modern" parallel behavior with blockchain is discussed in more detail. For this purpose, general algorithms are distinguished from blockchain algorithms. This is followed by a short description of parallel behavior in trust economy. Subsequently, blockchain-based parallel behavior is outlined in the different scenarios known from general algorithms. In addition, the question of whether parallel behavior using blockchain is coordinative and dynamic in nature is raised (chapter 5). This is followed with a conclusion (chapter 6).

2 The transparency explosion

2.1 Overview of market transparency

5 The transparency of a relevant market is measured by the market participants' knowledge of market-relevant information. In particular, information on competitive parameters such as prices, volumes and sales strategies is an important indicator that the market behavior of other competitors becomes more predictable.[4] As will be shown, this predictability has a central influence on parallel behavior.[5] Moreover, market transparency turns out to be higher or lower depending on the conditions of competition. A tight oligopoly, for example, is particularly suitable for increasing transparency, as the lack of a larger number of competitors makes market relations more

[3] The terms "data" and "information" are used synonymously in this paper.

[4] KERBER WOLFGANG/SCHWALBE ULRICH, Säcker Franz Jürgen et al. (eds.), Münchener Kommentar zum Wettbewerbsrecht, 3rd ed., Munich 2020, 1st part fundamentals n 318.

[5] *Infra* para. 53 f.

manageable.[6] In addition, product homogeneity, high interaction frequency and barriers to market entry tend to lead to higher market transparency.[7] Finally, a distinction can be made between horizontal (supplier-side) and vertical (demand-side) market transparency where supplier-side market transparency tends to increase the stability of parallel behavior, whereas demand-side market transparency tends to weaken it.[8]

2.2 Explosive mixture

2.2.1 Blockchain

2.2.1.1 How the blockchain works

6 One component of the transparency explosion is the blockchain. However, as this is a rapidly evolving technology,[9] the following will only address the fundamental aspects of blockchain focusing on the public blockchain. If the term "blockchain" is understood broadly, three layers can be distinguished: database, protocol and cryptocurrency or asset.[10] However, the explanations in this paper will primarily deal with the blockchain in the sense of the first layer.[11] In essence, the blockchain is a database with information stored in "blocks" that are interconnected and form a "chain". The blocks contain transaction data, a timestamp and a cryptographically secure hash of the block that

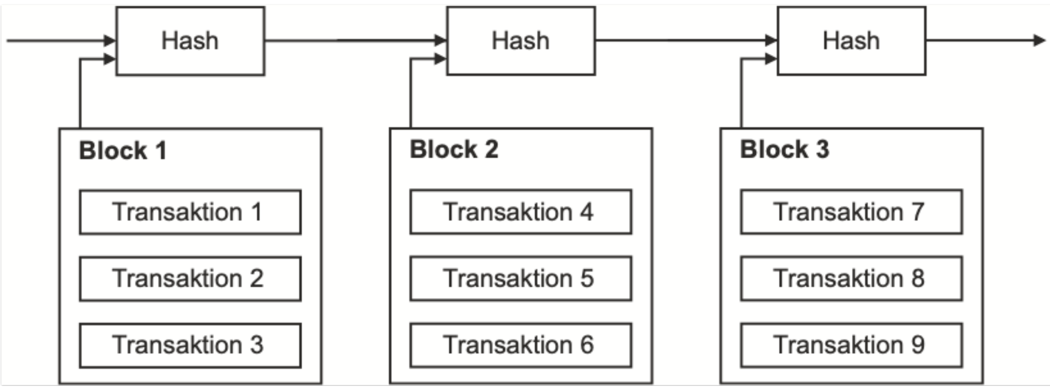

Figure 1: Simplified representation of the blockchain (1st layer).

[6] Riesenkampff Alexander/Steinbarth Sebastian, Loewenheim Ulrich et al. (eds.), Kartellrecht, Kommentar, 4th ed., Munich 2020, art. 2 n 149.

[7] Ezrachi Ariel/Stucke Maurice E., Sustainable and Unchallenged Algorithmic Tacit Collusion, Northwestern Journal of Technology and Intellectual Property, 17(2) (2020), 217–260, 226; Riesenkampff/Steinbarth, art. 2 n 149.

[8] Kerber/Schwalbe, 1st part fundamentals n 319.

[9] Schrepel Thibault, Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox, Georgetown Law Technology Review, 3(2) (2019), 281–338, 286.

[10] Swan Melanie, Blockchain: Blueprint for a new economy, Sebastopol 2015, 1; see also Naraine Michael, The Blockchain Phenomenon: Conceptualizing Decentralized Networks and the Value Proposition to the Sport Industry, International Journal of Sport Communication, 12 (2019), 313–335, 318.

[11] The Protocol consists of software programs and clients with which users conduct transactions; for cryptocurrency, see Garrick/Rauchs, 1 ff. with further references.

precedes it in time (digital fingerprint). The hash of the new block then becomes part of the following block and so on, resulting in a chronological chain of blocks linked by hash values. If a new transaction is made between computers (peer-to-peer), a new block is created according to a certain consensus procedure (e.g., proof of work or stake) and added to the chain using cryptographic procedures.[12]

7 The public blockchain has the following main characteristics: decentralized, pseudonymous, encrypted and immutable.[13] In fact, the records are stored in a decentralized manner so that basically each network participant has a copy of the entire blockchain. The identity of these participants is pseudonymous as their plain names are not showed in their addresses. In addition, transactions are often encrypted especially in the context of transparency. This will be discussed separately.[14] Lastly, the information stored in the blocks is basically unchangeable without the consent of the majority of network participants, since modifying it would change its hash. These properties ultimately result in a code that can establish trust technically between its participants without a central authority.[15]

2.2.1.2 Market transparency via blockchain

8 Blockchain does not create perfect market transparency for everyone. Indeed, the blockchain architecture leads to a limitation of transparency, primarily in terms of access to the blockchain and its content. First, depending on the type of blockchain, transaction data is accessible to everyone (public blockchain) or only to a selected group of authorized individuals or companies (private blockchain). While in public blockchains such as the Bitcoin or Ethereum blockchain no access controls are in place, the architecture of the private blockchain – including the granting of write and read rights – is centrally determined by a single person or group.[16] Since they can rule over the technical design of "their" blockchain, they can also decide that certain information is not visible to all users or that certain people cannot become users in the first place.[17] Depending on the reading rights that the market participant has, he can benefit from the transparency of public blockchains and possibly also from a private blockchain.

9 The second limitation relates to the content. It is true that in a public blockchain market transparency refers to the entire history of transaction data. This includes anything that

[12] Cf. on the whole URBAN NICKLAS T., Blockchain for Business: Erfolgreiche Anwendungen und Mehrwerte für Netzwerkteilnehmer identifizieren, Wiesbaden 2020, 15 ff.

[13] However, it must be taken into account that there is no agreement (yet) on the main features of the public blockchain.

[14] *Infra* para. 10.

[15] Cf. on the whole URBAN, 20 f.

[16] SCHREPEL THIBAULT, Collusion by Blockchain and Smart Contracts, Harvard Journal of Law & Technology, 33(1) (2019), 117–166, 149.

[17] SCHREPEL, Collusion, 147, 150.

can be described in digital form (e.g., transactions, contracts, assets, identities), which potentially includes all possible market-relevant information.[18] However, the data stored in the blocks is often encrypted (hashed).[19] In this context, two types of transparency can be distinguished: while the respective transaction participants understand the content or meaning of the transaction ("content transparency"), transparency from the perspective of non-transaction participants exists only with regard to metadata or other types of administrative information ("protocol transparency").[20] This includes, for example, the information that a pseudonymized person sends a certain amount of coins to another pseudonymized person.[21] In other words, there is – with regard to the content layer – a "visibility effect" for the transaction partners, while there is an "opacity effect" for third parties.[22]

10 A special type of content restriction exists due to the pseudonymized identity of the transaction participants: "[I]ts' possible to hide the 'meaning' of a transaction (to the extent that its' connected to peoples' identities) from everyone except the two parties to it."[23] This is true because the identity of the transaction parties is generally encrypted and represented by a so-called public key, which is comparable to a bank account number.[24] "We have seen that blockchain is indeed a fortress – immutable and pseudonymous. Blockchain will therefore prevent the collection of useful information, a point that is often overlooked when tech-optimists describe the new tools available to authorities."[25] However, this view must be put into perspective, because there is discussion about the possibility that transaction partners can be identified by

[18] DENG AI, Smart Contracts and Blockchains: Steroid for Collusion?, September 11, 2018, 3; PISCINI ERIC/HYMAN GYS/HENRY WENDY, Tech Trends 2017, Blockchain: Trust economy, in: Deloitte Insights of February 7, 2017, available at <https://documents.deloitte.com/insights/TechTrends2017>, 95.

[19] This is the assignment of a unique value to any string.

[20] DE FILIPPI PRIMAVERA, The interplay between decentralization and privacy: the case of blockchain technologies, Journal of Peer Production, 7 (2016), 5; see also BARSAN IRIS M., Public Blockchains: The Privacy-Transparency Conundrum, Revue Trimestrielle de Droit Financier, 2 (2019), 44–53, 45; protocol transparency is of great importance for a decentralized infrastructure like the blockchain. In the absence of a central authority, the network itself must ensure that no participant cheats. This requires protocol transparency so that nodes can verify and validate transactions.

[21] NAKAMOTO SATOSHI, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, available at <https://bitcoin.org/bitcoin.pdf>, 6.

[22] SCHREPEL, Collusion, 150; see, however, *infra* para. 57.

[23] BARTA SILAS/MURPHY ROBERT P., Understanding Bitcoin: The Liberty Lover's Guide to the Mechanics & Economics of Crypto-Currencies, Version 1.11, December 2017, 52; see SCHREPEL, Collusion, 150; see also NAKAMOTO, 6: "[...] privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone."

[24] MARTINI MARIO/WEINZIERL QUIRIN, Die Blockchain-Technologie und das Recht auf Vergessenwerden, Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen, NVwZ 2017, 1251–1259, 1251; SCHREPEL, Paradox, 287; the so-called private key (password) is to be distinguished from the public key.

[25] SCHREPEL, Collusion, 153.

proportionate means especially in the context of data protection law.[26] This is possible, for example, if the partners deliberately disclose themselves by signing up for services such as Bitcoin marketplaces. In addition, a blockchain participant can also be identified based on big data analytics. In private blockchains, it is added that the managing entity can identify a participant because it has already assigned the user ID to him.[27] As a result, the identity – and thus the information linked to it – can also be made transparent with (relative) effort.[28]

2.2.2 Big data analytics

11 Another "substance" which, according to the opinion expressed here, is part of the "explosive mixture" is big data analytics. However, the terms "big data" and "big data analytics" are often used as synonyms. In the following, however, a distinction must be made between specific data (big data) and its analysis (big data analytics). As will be shown in more detail below, this differentiation is of utmost importance in the context of blockchain.[29] Since there is currently no uniform definition of these two terms, their meaning is based on the following definitions.

12 The term "big data" describes in this paper a large amount and variety of data that is generated at high speed ("3V": "Volume, Variety and Velocity"). In contrast, the term "big data analytics" describes the analysis of big data, i.e., data processing that is neither carried out manually nor by conventional data processing methods and is therefore used to find patterns and trends in the data. The possible areas of application for big data analytics are extremely diverse. For example, Big Tech can determine and predict the behavior and preferences of its users by analyzing the data relating to them – making consumers transparent. In this respect, *Shoshana Zuboff* speaks of "surveillance capitalism", as consumers are monitored so that companies can increase their capital as a result of the transparent buyer (e.g., through personalized advertising and products).[30]

---

[26] The name of the transaction partners are personal data in the sense of art. 4 para. 1 GDPR, Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive) of April 14, 2016.

[27] Cf. MARTINI/WEINZIERL, 1253; see also BRUDNA ERNST, Tacit collusion and the blockchain: a theoretical approach, Graz 2019, 27, available at <www.unipub.uni-graz.at/obvugrhs/download/pdf/4590833?originalFilename=true> stating, however, that companies using the blockchain would have to be just as recognizable as in the traditional world.

[28] However, see SCHREPEL, Collusion, footnote no. 196 on quantum cryptography.

[29] *Infra* para. 16.

[30] See generally ZUBOFF SHOSHANA, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York 2019, 1 ff.

2.2.3 Trust economy

13 The third "explosive material" can be seen in the so-called trust economy. This is "[t]he next evolution of the digital economy"[31] in which trust plays a central role. A key driver for the emergence of the trust economy is the sharing economy, in which the use of resources such as unused living space or car seats is shared (e.g., Airbnb, Uber). "As we get into cars with complete strangers, sleep in the beds of people we've never met and lend money to others on the other side of the world, a powerful new currency is emerging – and its' based on trust."[32]

14 In recent years, there has been a shift in power and trust from vertical trust in institutions such as the state to horizontal trust between people (decentralized trust).[33] For example, an Uber driver is chosen by the passenger primarily on the basis of his or her score. In addition to passenger ratings, the analysis of individual identity and reputation data will increasingly flow into the score. This will probably lead to an expansion of credit scoring, which is already common today, into a more general "life scoring". The resulting "trust score" can then be used as a basis for decision-making in all kinds of transactions.[34] However, not only individuals are assigned such a score, but also companies, which is why the "trust score" could become the new standard of trustworthiness in macroeconomic terms.[35] "[T]rust is rapidly becoming the global – and most-valued – currency of modern time."[36]

> "The core of the sharing economy is trust. While platforms such as Airbnb and Uber have functioned as the vanguard of the collaborative economic revolution, the centralized manner in which they operate forces consumer trust to rely on third-party arbitrage. The next evolution of the digital economy, however, allows for the creation of a truly decentralized trust paradigm through a new immutable, transparent tool - blockchain technology. The fourth industrial revolution, driven by blockchain technology, is underpinned by a new economy: the Trust Economy."[37]

---

[31]VALON MATHIAS, Trust Economy – The 21st Century Main Market, Medium of February 25, 2019, available at <https://medium.com/@Chaineum/trust-economy-the-21st-century-main-market-21afdb69bb4e>.

[32] STAN ADRIANA, The future is the trust economy, Tech Crunch of April 25, 2016, available at: <https://techcrunch.com/2016/04/24/the-future-is-the-trust-economy>.

[33] STURM MIKE, Rachel Botsman: An Economy of Trust, Nordic Business Report of February 4, 2018, available at: <https://www.nbforum.com/nbreport/rachel-botsman-economy-trust/>; PISCINI/HYMAN/HENRY, 95; VALON, Trust Economy.

[34] VALON, Trust Economy; an interesting convergence can be observed with the social credit system in China. On the social credit system, see, for example, GENZSCH MADELEINE, Harmonie durch Kontrolle? Chinas Sozialkreditsystem, Loitsch Tobias (ed.), China im Blickpunkt des 21. Jahrhunderts, Impulsgeber für Wirtschaft, Wissenschaft und Gesellschaft, Berlin/Heidelberg 2019, 129 ff.

[35] STAN, Trust Economy; VALON, Trust Economy; on the changing meaning of the brand, see also STAN, Trust Economy.

[36] STAN, Trust Economy.

[37] VALON, Trust Economy.

15 However, as this excerpt also shows, trust does not necessarily have to emanate (only) from today's platforms and their scores. In this respect, a distinction must be made between "centralized" trust economy, on which the current sharing economy in particular is based, and the emerging phenomenon of "decentralized" trust economy. In the latter, the blockchain and its transparency, immutability and digital identity form important building blocks that can create trust without the involvement of a central authority.[38] First, transparency can create trust especially if it is qualitative in nature. As will be shown in more detail, the properties of the blockchain have a significant influence on the quality – and thus the trustworthiness – of the data stored in it.[39] And second, the blockchain is a tool of trustworthy identity management, since customers can use it to clearly prove that they are who they claim to be. Thus, the trust economy provides significant incentives to use the blockchain, whereby "[i]n a blockchain world, companies would compete to be more and more transparent. The more transparency, the more investors and other constituents will trust the security or utility token."[40] As a result, the blockchain forms an important foundation of the (decentralized) trust economy.[41]

2.3 Types of transparency explosion

2.3.1 Quantitative transparency explosion

16 The elements mentioned individually above, which according to the view represented here form a highly explosive mixture, are the following:

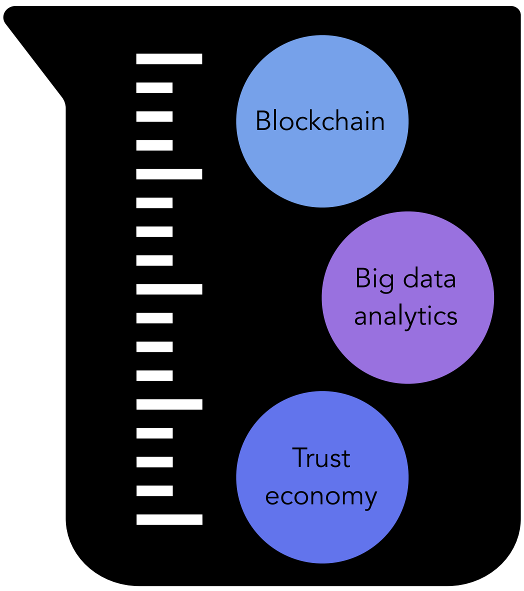

Figure 2: The three main components of the transparency explosion.

[38] STURM, Economy of Trust; VALON, Trust Economy.

[39] *Infra* para. 20.

[40] SILVER, Blockchain Drives Value.

[41] PISCINI/HYMAN/HENRY, 95.

- Blockchain (data): the object of data analysis.
- Big data analytics: the tool for data analysis.
- Trust economy: the economic incentive for both the increased disclosure of data using blockchain and its processing through big data analytics.

17 In this transparency mix, there is a growing amount of data stored in the distributed ledger of the (public) blockchain. As this is a foundational technology, it can potentially form the foundation of the economic system as the Internet once did. As a result, the (public) blockchain is likely to grow significantly in importance in the future,[42] which may lead to an ever increasing number of transactions – and thus of data – across all markets.

18 This immense amount of data is then analyzed by big data analytics, so that even more information can be derived from it (e.g., identification of blockchain participants). In addition, according to the view represented here, it is conceivable that the "opacity effect" acting in relation to third parties can be considerably weakened as a result of the analysis of (meta) data and the resulting additional information. On the other hand, it is also important to bear in mind that the relationship between big data analytics and blockchain data is still largely unexplored. However, it is already becoming apparent that the data stored in the blockchain will be able to solve some of the problems of big data analytics, making the analysis results more accurate (e.g., as a result of immutable and structured data in the blockchain).[43]

19 Next, big data analytics and blockchain meet the trust economy. Since trust is of central importance in this new form of economy and can be established and increased by means of transparency, this results in a considerable economic incentive for companies and individuals to use the blockchain to increase their trustworthiness.[44] This increases the number of blockchain participants and the data they create, which in turn are analyzed through big data analytics, creating even more data. As a result, the blockchain is a catalyst that drives trust economy, which in turn accelerates the use of blockchain and big data analytics. These three main components result in the **"quantitative transparency explosion"** introduced in this paper, which could ultimately lead to increased market transparency, potentially in all markets.

[42] SCHREPEL, Paradox, 286.

[43] DE MEIJER CARLO R.W., Blockchain and big Data: A great mariage, Finextra of January 29, 2019, Blockchain and Big Data, available at <https://www.finextra.com/blogposting/16596/blockchain-and-big-data-a-great-mariage>.

[44] VALON, Trust Economy.

2.3.2 Qualitative transparency explosion

20 The quantitative explosion in transparency may lead to increased market transparency. But the sheer increase in information must be distinguished from its trustworthiness or qualitative nature: “If Big Data is the quantity, blockchain is the quality”.[45] But what is the special quality of this new, blockchain-based transparency?[46]

21 Thibault Schrepel has noted that the characteristics of blockchain affect the nature of collusion based on it. For example, he speaks of pseudonymized and unstoppable collusion.[47] Similarly, the properties of the blockchain have an impact on the nature of *transparency*. Accordingly, it mainly results in validated, immutable, historical, and pseudonymous transparency.

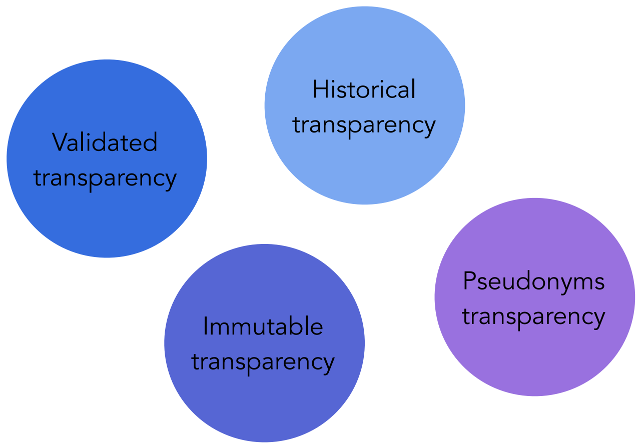

Figure 3: The main types of qualitative transparency.

22 The here so-called “validated transparency” refers to transparency that has been verified according to a certain consensus mechanism such as proof of work and thus creates more trust.[48] This particularly concerns the origin of the data and interactions.[49] For example, the risk of the same asset being transferred more than once (double spending) can be significantly reduced.[50] In addition, information about transaction prices stored in the blockchain is more trustworthy than listed prices.[51]

---

[45] DE MEIJER, Blockchain and Big Data.

[46] Big data analytics and the trust economy could also contribute to the quality of the transparency explosion. However, the following comments focus on the quality emanating from the blockchain.

[47] SCHREPEL, Unimportance.

[48] Cf. SCHREPEL, Collusion, 141.

[49] DE MEIJER, Blockchain and Big Data.

[50] BATUBARA F. RIZAL/UBACHT JOLIEN/JANSSEN MARIJN, Unraveling Transparency and Accountability in Blockchain, Proceedings of the 20th Annual International Conference on Digital Government Research (dg.o 2019), Association for Computing Machinery, New York, USA, 204–213, 205.

[51] OECD, Antitrust and the trust machine, November 2020, available at <https://www.oecd.org/daf/competition/antitrust-and-the-trust-machine-2020.pdf>, 12.

23 In contrast, "immutable transparency" is characterized by the fact that data is basically static from a time perspective. This fundamental immutability is particularly valuable from the point of view of big data analytics: if the data set under investigation is changed, the resulting analysis loses its value.[52]

24 Next, "historical transparency" is closely related to immutable transparency. Indeed, the history of transaction data is intended to create trust, which is why it should be immutable. In this respect, this type of transparency is a chronological and complete picture of the past in relation to the blockchain transactions that have taken place. However, traditionally (i.e., outside of the Blockchain) such a gapless picture is often only available because the data has been collected over a longer period of time by the company itself.[53] An exceptional case is, for example, the "Wayback Machine Scraper", which can be used to evaluate previous versions of websites. However, not all changes to websites are visible in the Wayback Machine and archived versions can also be deleted.[54] Historical transparency, which is based on the blockchain, therefore has a considerably greater qualitative value.

25 Finally, "pseudonymous transparency" must also be mentioned. Upon closer examination, however, it actually reduces transparency. In the area of traditional transparency based on the analysis of blockchain-external data, for example, the owner of a website, which shows also sales prices, is typically not pseudonymized. Accordingly, pseudonymous transparency is not a special quality feature. This illustrates that blockchain data can also contribute to *lower* quality transparency. On the other hand, identification of the blockchain participants is possible in some cases.[55] Depending on whether de-pseudonymization succeeds, the mere pseudonymous transparency loses importance, so that there can still exist an increased qualitative transparency.

26 As a result, especially these types of qualitative transparency mix with the transparency explosion, creating a **"qualitative transparency explosion".**

2.4 Relativizing view

27 However, the process of the transparency explosion needs to be relativized in several respects. First, the concrete form of the three components is not yet clearly contoured and is subject to constant change. Second, the relationship among the components is still unclear (especially in relation to the trust economy). And third, the three components are not the only ones that could lead to an increase in market transparency. In particular,

---

[52] DE MEIJER, Blockchain and Big Data.

[53] In this respect, blockchain data could lower barriers to entry, as the data does not have to be collected by the companies themselves over several weeks or months but can already be accessed in the blockchain.

[54] See, for example, <https://github.com/sangaline/wayback-machine-scraper>.

[55] *Supra* para. 10.

data that is analyzed by big data analytics is also stored "outside" the blockchain. For example, they can result from the analysis of user behavior on apps[56] or the website content of competitors (so-called web scraping). In this respect, data has already been of great importance for a long time ("The worlds' most valuable resource is no longer oil, but data").[57]

28 In addition to the components themselves, their anti-competitive effects must also be put into perspective. First, all three components may increase market transparency on the supplier side, which can have anti-competitive effects. At the same time, however, they may intensify competition and lead, for example, to (disruptive) product and process innovations or even business model innovations. This is especially true in the case of trust economy.[58] The multifaceted effects of these components on competitive conditions should not be underestimated, especially if they can have pro-competitive effects and thus reduce the harmful effects of supplier-side transparency. Second, the transparency explosion leads to an increase in demand-side market transparency, so that demanders or consumers can also benefit from it (e.g., similar to today's comparison websites).[59] From an overall perspective, however, it is questionable whether the increased transparency will not ultimately benefit providers. In case of doubt, it can be assumed that providers benefit more from the increased transparency.[60]

2.5 Interim conclusion

29 This chapter introduced the phenomenon of the transparency explosion. It is primarily based on big data analytics, blockchain and trust economy. Despite all relativizations regarding the components and their impact on competition, this explosive mixture may lead to a transparency explosion of a quantitative and qualitative nature.

[56] However, see also the Decentralized Apps (DApps).

[57] Author unknown, The world's most valuable resource is no longer oil, but data, in: The Economist Online of May 6, 2017, available at <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

[58] Cf. HEINEMANN ANDREAS, Algorithmen als Anlass für einen neuen Absprachebegriff?, SZW 2019, 18–30, 19.

[59] YLINEN JOHANNES, Digital Pricing und Kartellrecht, NZKart 2018, 19–22, 19.

[60] WECHE JOHN/WECK THOMAS, Neue Möglichkeiten impliziter Kollusion und die Grenzen des Kartellrechts, EuZW 2020, 923–929, 924; more optimistically DÜCK HERMANN/MÄUSEZAHL STEFFEN/SYMNICK INGA, Kartell der Algorithmen – das Verbot wettbewerbsbeschränkenden Zusammenwirkens im Lichte fortschreitender Digitalisierung bei der Preissetzung, ZWeR 1/2019, 94–132, 106.

3 "Classic" parallel behavior

3.1 Economic view

30 First of all, this chapter will look at the competitive fundamentals of "classic" parallel behavior. This is understood to mean parallel behavior that is not algorithm- or blockchain-based.[61] If players, who are both aiming to maximize profits, are in competition with each other, it may happen that both ultimately fail to achieve their goal (e.g., as a result of price wars).[62] It is therefore advantageous for market players to eliminate competition between themselves and replace it with coordination.[63] The stability of collusion is measured by the monitoring possibilities by means of which deviations can be detected. In addition, tough and credible punitive measures must exist as deterrent mechanisms (e.g., short-term price wars) so that there is no deviation from the coordination modalities. Finally, stability must not be jeopardized by outsiders such as other competitors or competition authorities.[64]

31 Such behavior can be based on an explicit agreement such as a written document (so-called explicit collusion) as well as on a merely implicit behavior (so-called tacit collusion).[65] From an economic point of view, however, both types of behavior can have highly damaging effects on competition.[66] Together with tacit concerted practice, parallel behavior is a subtype of tacit collusion. In this regard, a competitor generally behaves with restraint to maintain oligopolistic peace or he aligns its behavior with that of another competitor by analyzing its market movements (e.g., price leadership).[67] From these behaviors it becomes apparent that parallel behavior is traditionally found in oligopoly markets and thus primarily represents an oligopoly problem.[68] Whether this also applies to the modern context of algorithms and blockchain remains to be elaborated below.[69] However, oligopolistic markets in particular are prone to parallel behavior, with market transparency being only one of the facilitating factors.[70] On the

---

61 For the term "algorithm" see *infra* para. 36.

62 HEAD, 29.

63 KOPF JONATHAN, Evolution von Kollusion: Experimentelle Evidenz in Kontraktmärkten, Wiesbaden 2017, 28 f.; see also KÜNSTNER KIM MANUEL, Preissetzung durch Algorithmen als Herausforderung des Kartellrechts, GRUR 2019, 36–42, 37.

64 Cf. on the whole KOPF, 29 ff.; WECHE/WECK, 924.

65 For more information see HEAD, 34 f.

66 REES RAY, Tacit Collusion, Oxford Review of Economic Policy, 9(2) (1993), 27–40, 27.

67 KOPF, 34; see also the example of New York in SCHELLING THOMAS C., The Strategy of Conflict, Harvard 1980, 56.

68 HEINEMANN, 20.

69 *Infra* para. 48.

70 BKartA, Algorithmen und Wettbewerb, January 2020, available at <www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_6.pdf?__blob=publicationFile&v=3>, 4.

other hand, it is precisely this factor that significantly increases the probability of collusion. It is especially the case when the flow of information is frequent and the information is of good quality.[71]

32 From an economics perspective, the distinction between parallel behavior and (tacit) concerted practice is primarily made on the basis of the profit development of the competitors. While a price increase due to parallel behavior leads to an increase in profits for the price-increasing company, a price increase in the realm of a concerted practice is followed by an increase in profits for the competitor.[72] Moreover, the price stabilizes over time in the case of parallel behavior, since any further increase would lead to a loss of profits. In the case of the concerted practice, this is precisely not the case.[73]

3.2 Legal view

33 Since this paper is primarily legal in nature and there is already ample literature on parallel behavior from a legal perspective, this chapter provides only a brief overview. With parallel behavior, companies do not cooperate, but unilaterally adapt their behavior to the market conditions (e.g., price adjustment to the market leader).[74] In the end, however, this uniform behavior may look like the result of a coordination of wills.[75] However, the conduct lacks the essential feature of communication required for coordination to be legally problematic. Since such independent behavior is based on the so-called postulate of independence, it is unobjectionable under competition law – even if it leads to significant restraints of competition.[76]

34 A distinction must then be made between (lawful) parallel behavior and (unlawful) collusion within the meaning of art. 101 (1) TFEU.[77] However, this distinction has not yet been conclusively clarified by courts and the doctrine in all details.[78] Generally, the latter occurs when "practical cooperation [has] consciously taken the place of competition involving risks."[79] Since this also covers tacit cooperation, the distinction from parallel

---

[71] WECHE/WECK, 924.

[72] WEBER HANS-JÜRGEN, Abgestimmtes Verhalten und Parallelverhalten auf dem oligopolistischen Markt, Zeitschrift für die gesamte Staatswissenschaft, 133(2) (1977), 245–256, 255.

[73] WEBER, 255.

[74] THOMAS STEFAN, Harmful signals: Cartel prohibition and oligopoly theory in the age of machine learning, Journal of competition law & economics, 15(2-3) (2019), 159–203, 171.

[75] Cf. WEBER, 253.

[76] KÜNSTNER, 38; admittedly, it can be problematic in the context of abuse of market power or merger control.

[77] Cf. KÜNSTNER, 38 with further references; however, see art. 101 para. 3 TFEU, Treaty on the Functioning of the European Union of March 25, 1957.

[78] See THOMAS, 172 ff. for delimitation theories.

[79] ECJ, 26.1.2017, C-609/13 P – *Duravit*, para. 70; ECJ, 8.7.1999, C-49/92 P – *Anic Partecipazioni*, para. 115.

behavior, that is generally tacit, is further complicated.[80] However, a central criterion for differentiation is whether there was direct or indirect communication between the companies which limited their independence and had the effect or purpose of restricting competition.[81] Further explanations on parallel conduct are then provided in the context of blockchain.

3.3 Interim conclusion

35 This chapter has given a brief overview of "classic parallel behavior". This refers to the unilateral adaptation of a company's behavior to market conditions without this adaptation being algorithm- or blockchain-based. From a legal perspective, such behavior is permissible even if it leads to significant restraints of competition.

4 "Modern" parallel behavior by means of algorithms

4.1 Classification of the algorithms

36 The term "algorithm" has not yet been given a uniform definition.[82] In this work, however, it is understood as a finite number of clearly defined instructions which transform inputs into outputs and where the instructions are automated by software. Thus, they are not performed by human actions, as is typically the case with, for example, a cooking recipe that contains step-by-step instructions for processing ingredients into a meal.[83]

37 According to BKartA/ADLC, the categorization of algorithms with potentially anticompetitive effects can be made in particular on the basis of the task to be performed and the learning method.[84] Regarding the former, potentially anti-competitive algorithms can especially be found in the areas of dynamic pricing, personalization and ranking.[85] Firstly, in dynamic pricing, (online) prices are adapted to a company's own costs and capacities as well as to demand situations and prices of other competitors. The pricing company may collect and evaluate information about its own situation as well as that of other competitors, for example, using so-called scraping algorithms. Based on this, the company can set its own prices.[86] Secondly, personalization algorithms can be

[80] PASCHKE MARIAN, SÄCKER FRANZ JÜRGEN et al. (eds.), Münchener Kommentar zum Wettbewerbsrecht, 3rd ed., Munich 2020, art. 101 n 95.

[81] KÜNSTNER, 38; PASCHKE, art. 101 n 81.

[82] BKartA/ADLC, Algorithms and Competition, November 2019, available at <www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.pdf?__blob=publicationFile&v=5>, 3rd ed.

[83] BKartA/ADLC, Algorithmen, 3rd ed.

[84] BKartA/ADLC, Algorithms, 4 ff. for further differentiations.

[85] BKartA/ADLC, Algorithms, 4 ff. on other tasks.

[86] BKartA/ADLC, Algorithms, 5.

used to adapt advertising and goods to the interests of consumers. For this purpose, (personal) data is collected and analyzed using predictive models. Important areas of application for these algorithms are, for example, product recommendations or so-called personalized prices, which adapt to the respective customer (and his willingness to pay).[87] Thirdly, algorithm-based ranking can be used to select or sort elements, making it easier for consumers to find information and thus raising market transparency (e.g., through search engines, comparison portals).[88]

38 With regard to learning methods, BKartA/ADLC roughly differentiate between two basic types of algorithms: self-learning and static algorithms. While the algorithm of the first type can set its behavioral parameters with great automation from training data, adapt them and improve its performance with increasing experience (so-called machine learning, ML), the parameters of static algorithms are set by humans. However, they neither adapt (semi-)automatically to changing circumstances nor can they improve their performance independently.[89]

39 Finally, according to the view represented here, a distinction can also be made between general and special algorithms. The former are general in nature and are often discussed in the broad context of "algorithmic" collusion. As will be shown, blockchain-algorithms are tied to the typical nature of blockchain and are thus a specific subform of the general term "algorithms".[90]

4.2 Scenarios of algorithm-based parallel behavior

4.2.1 "Messenger"

40 The scenarios already developed by *Ezrachi/Stucke* in the (more general) context of algorithmic collusion can serve as a starting point for the categorization of algorithm-based parallel behavior. Indeed, the first scenario "messenger" also concerns agreements which are made by humans and then carried out, monitored and controlled by algorithms. [91]

41 In the context of algorithmic parallel behavior, this scenario relates to cases in which a company has independently decided to engage in parallel behavior and implements it by means of an algorithm. For example, price developments can be observed (price tracking), price changes of other companies such as the market leader can be monitored

[87] BKartA/ADLC, Algorithms, 6.

[88] BKartA, Algorithmen, 2.

[89] Cf. on the whole BKartA/ADLC, Algorithms, 9 f.

[90] *Infra* para. 52.

[91] EZRACHI ARIEL/STUCKE MAURICE E., Virtual Competition, The Promise and Perils of the Algorithm-Driven Economy, Cambridge MA/London 2016, 36.

(price monitoring), and the company's own prices can be adjusted accordingly (price setting).[92]

4.2.2 "Hub and spoke"

42 In the second scenario "hub and spoke", different competitors use the same algorithm and/or data pool, which can lead to an alignment of competitive parameters such as prices or quantities.[93] In this constellation, the competitors ("spokes") each have star-shaped agreements or other connections to the developer of the algorithm or the owner of the data pool ("hub"), but otherwise do not communicate directly with each other. Nevertheless, this scenario qualifies as a horizontal agreement between the competitors mediated by the third party if the star-shaped agreements or the resulting coordination were entered into knowingly and willingly by the competitors.[94]

43 However, if there is no such intent, there may be parallel conduct. In this case, a company uses an algorithm, for example, to align its prices with those of the market leader without knowing (and wanting) that it is still carrying out this alignment with other competitors via the developer. The company's intent therefore does not relate to coordination, but to the use of an algorithm for the *independently* chosen purpose of parallel conduct.[95]

4.2.3 "The predictable agent"

44 In the third scenario "the predictable agent", there is no communication between competitors. They use their own algorithms (with their own data pools) in the knowledge that the industry-wide use of algorithms that monitor and align with each other can ultimately lead to an increased emergence of parallel behavior ("tacit collusion on steroids").[96]

45 Since *Ezrachi/Stucke* themselves address parallel behavior, this scenario does not need to be further adapted to our constellation of parallel behavior. In fact, the only difference – if any – seems to be that in scenarios 1 and 2, the companies are arguably only considering their own parallel behavior and not placing the use of their algorithm in the larger context of industry-wide "tacit collusions on steroids". However, since this nuance is not primarily important to this paper, the focus of the following discussion will be on the scenarios 1, 2, and 4.

[92] HEINEMANN, 21.

[93] EZRACHI/STUCKE, Virtual Competition, 36.

[94] HEINEMANN, 21.

[95] Cf. HEINEMANN, 21.

[96] EZRACHI/STUCKE, Virtual Competition, 36 f., 56.

4.2.4 "Digital eye"

46 Finally, the fourth scenario "digital eye" consists of ML algorithms that lead to anticompetitive outcomes with increased market transparency – without the antitrust authorities being able to establish an anticompetitive agreement or intent. This could lead them to wrongly assume that markets are indeed competitive. However, consumers might not be able to benefit from this "virtual competition".[97]

47 This constellation is also conceivable for algorithm-based parallel behavior. A company could use an algorithm to implement a certain lawful or unlawful strategy. Nevertheless, the algorithm could independently take the "decision" that not the (unlawful) behavior intended by the company, but a parallel behavior could maximize its performance measure[98].[99] In contrast to unlawful agreements, parallel behavior is lawful. However, it can equally lead to "virtual competition" and ultimately to anti-competitive effects on competition.[100]

4.3 New forms of parallel behavior

48 Parallel behavior by means of algorithms has certain characteristics, which is why it diverges from "classic" parallel behavior. For example, the automation of algorithms means that they can monitor a high number of competitors and react immediately to certain events such as a change in prices. It has become less attractive for companies to lower their prices and engage in price wars. Indeed, the "meeting" of two algorithms, both trained to increase the price when a competitor increases its price, could lead to a spiral of price increases. As a result, algorithmic parallel behaviors not only occur more frequently, but also tend to be more stable.[101] Overall, these changed market characteristics lead to a trend from (unlawful) agreements to (lawful) parallel behavior even in non-oligopolistic markets, which can be just as harmful to competition as agreements.[102] This turns parallel behavior from an oligopoly problem into a polypoly problem.[103]

---

[97] EZRACHI/STUCKE, Virtual Competition, 37.

[98] The performance measure defines the degree of success of an algorithm.

[99] EZRACHI/STUCKE, Tacit Collusion, 251; HEINEMANN, 21.

[100] In this context, a change in the concept "agreement" is also being discussed, so that the increased and more aggressive parallel behavior (also due to increased market transparency) can be better captured. See, for example, KÜNSTNER KIM/FRANZ BENJAMIN, Preisalgorithmen und Dynamic Pricing: Eine neue Kategorie kartellrechtswidriger Abstimmungen?, K&R 2017, 688–693, 693.

[101] EBERS MARTIN, Dynamic Algorithmic Pricing: Abgestimmte Verhaltensweise oder rechtmäßiges Parallelverhalten?, NZKart 2016, 554–555, 555.

[102] EZRACHI/STUCKE, Tacit Collusion, 225.

[103] HEINEMANN, 27.

4.4 Interim conclusion

49 In this chapter, the algorithms, on which "modern" parallel behavior is based, were classified. Subsequently, the various scenarios that primarily deal with algorithm-based collusion were applied to algorithm-based parallel behavior. Lastly, it was pointed out that new forms of parallel behavior emerge due to the peculiarities of algorithms.

5 "Modern" parallel behavior by means of blockchain

5.1 General and blockchain algorithms

50 In the literature, some recent articles deal with both collusion by algorithms and by blockchain.[104] The authors are of the opinion that blockchain-based agreements are generally more problematic from the standpoint of competition law than algorithmic agreements due to certain properties of the blockchain (e.g., unstoppable code). First, it is claimed that there is a lack of conclusive empirical studies on algorithm-based agreements. Second, algorithmic collusion is considered "old wine in new bottles", because it does not chance the nature of anti-competitive collusion being merely a "more elegant way of implementing the same practices known for centuries".[105]

51 It is surprising, however, that no precise distinction is made between the two forms of agreement. In these papers, algorithmic agreements seem to be understood as agreements that are algorithm-based and thus either implement an agreement made by humans or – and this seems to be the focus of the literature – make agreements independently from humans. In contrast, blockchain-based agreements are based on the blockchain and therefore adopt its nature (e.g., unstoppable agreements).[106]

52 In the view expressed here, however, this (contourless) division into algorithmic and blockchain agreements must be critically questioned. The reader could fall prey to the misconception that blockchain-based agreements are not algorithm-based. In fact, however, they are based on algorithms such as smart contracts, consensus algorithms or the protocol. Smart contracts are computer protocols that can map or verify contracts or technically support the negotiation or settlement of a contract. Moreover, consensus algorithms are a process by which all participants in the blockchain network reach a common agreement on the state of the distributed ledger. And the protocol governs the blockchain network. Blockchain-based agreements do not stand alongside algorithm-based agreements. Rather, they are a specific subform of them, subject to the specific

[104] For example, SCHREPEL, Unimportance; COLANGELO GIUSEPPE/MEZZANOTTE FRANCESCO, Colluding through smart technologies: Understanding agreements in the age of algorithms, forthcoming in L. Di Matteo/C. Poncibò/M. Cannarsa (eds.), The Cambridge Handbook of Artificial Intelligence, Cambridge 2022, 4 ff.

[105] SCHREPEL, Unimportance.

[106] SCHREPEL, Unimportance.

nature of the blockchain. For this reason, this paper speaks of algorithm-based agreements or general algorithms in the sense of a generic term and blockchain-based agreements or specific blockchain algorithms in the sense of a sub-term.[107]

5.2 Parallel behavior in the trust economy

53 The longer it lasts, the more the trust economy may form the economic framework in which competition – and also parallel behavior – will take place. In it, market participants have an incentive to create trust through transparency. According to the current papers on the trust economy, however, it seems that the increased transparency primarily affects the vertical relationship, i.e., the relationship between market participants at different levels of the production or distribution chain (e.g., transparent car driver for the passenger). However, trust economy may also provide the incentive for increased use of blockchain and evaluation of (blockchain) data through big data analytics. The question therefore arises as to whether this transparency explosion will not also have an indirect effect on horizontal relationships between competitors and create trust there as well.

54 Ernst Brudna also assumes this when he states: "public ledger helps to distribute information between the firms, thus raising the transparency of an industry".[108] Regarding private blockchains, he adds: "in a permissioned blockchain, only firms of a specific industry could [...] have full access to the ledger. Thus, these firms could see all their competitors' transactions [...], which could help the firms coordinate tacitly on a collusive outcome, […]".[109] Accordingly, it is assumed in the following passages that not only the vertical but also the horizontal relationship will be affected by the transparency explosion.

5.3 Scenarios of blockchain-based parallel behavior

5.3.1 "Messenger"

5.3.1.1 Distinction from concerted practice

55 The first scenario ("messenger") concerns agreements that are made by humans and subsequently executed, monitored and controlled by algorithms. A coordinated behavior or agreement that was reached "outside" the blockchain can also be implemented in a blockchain, so that, for example, prices, production levels and innovation strategies are coordinated.[110]

[107] This nomenclature has also been reflected in the title of this thesis, which is why the term "algorithms" actually means general algorithms. For reasons of the better readability, however, only the term "algorithms" was used.

[108] BRUDNA, 36.

[109] BRUDNA, 26.

[110] SCHREPEL, Collusion, 128.

56 First, the blockchain can be used as a trusted database to ensure the visibility and traceability of agreed information such as the origin of raw materials.[111] Second, smart contracts can be used to automate the collusion, making it more predictable and transparent. For example, a smart contract could link to information published on the blockchain and – if conditions are met – trigger corresponding transactions between collusion participants or to third parties. In addition, smart contracts can also be used to find price equilibrium, allocate profits, and monitor and punish deviant behavior.[112]

57 Both approaches generate increasing trust among the collusion participants in both the public and private blockchain and thus tend to increase the stability of the collusion.[113] Admittedly, this does not mean that the collusion will be of infinite duration. It is true that the blockchain reduces both the risk of deviation from the coordinated behavior by collusion participants due to the higher transparency ("visibility effect") and the risk of detection by antitrust authorities ("opacity effect").[114] However, at least in the constellation of smart contracts on private blockchains, the exit from the collusion or even the blockchain can be automated under certain conditions. For example, the exclusion of a possible fraudster can be technically enforced, or a company can bring about its own exclusion.[115] As a result, "collusive agreements will be more robust during their lifetime […], but will die in more brutal ways."[116]

5.3.1.2 With and without smart contracts

58 Due to certain competitive conditions, which also include market transparency, a company could decide to engage in parallel behavior. Again, blockchain transparency on the one hand and smart contracts on the other must be taken into account.

59 The first constellation consists of parallel behavior that is stimulated by the increased transparency of blockchain (and the other components of the transparency explosion) – but that is not also technically implemented with blockchain. For example, more accurate oversight of competitors' market behavior may cause a company to engage in parallel behavior in a traditional manner (e.g., manual price changes) or with general algorithms. Even though increased parallel behavior as a result of higher blockchain transparency has

[111] SCHREPEL, Collusion, 130.

[112] SCHREPEL, Collusion, 145.

[113] SCHREPEL, Collusion, 141 ff.; however, the scope for action is usually greater in the private blockchain, which is why more sophisticated implementation options exist there.

[114] SCHREPEL, Collusion, 143; see also *supra* para. 9.

[115] SCHREPEL, Collusion, 154.

[116] SCHREPEL, Collusion, 163.

already been discussed in the literature, it has only received marginal attention.[117] Moreover, it has not been placed in the larger context of big data analytics and trust economy. However, it is this combination of transparency-enhancing components that allows companies to analyze and predict market behaviors of their competitors more accurately and adjust their behavior accordingly, more than might be expected from a focus on blockchain only. On the other hand, especially blockchain transparency is of higher quality compared to the one addressed in the context of algorithmic parallel behavior (e.g., transparency based on websites). Usually, however, it is *qualitative* data that is a key factor in (tacit) coordination, rather than the sheer quantity of data.[118] As a result, both the quantitative and the qualitative side of the transparency explosion play an important role in parallel behavior. However, since parallel behavior by means of blockchain can be more diverse and therefore needs to be evaluated in a more differentiated manner, the following discussion focuses on this type of parallel behavior.

60 The second constellation involves parallel behavior that is technically implemented by means of the blockchain respectively smart contracts. At first glance, however, an agreement based on a smart contract seems to contradict the definition of parallel conduct. In this regard, it should be noted that smart contracts can be used not only between competitors, but also between companies in a vertical relationship. For example, a smart contract could be unilaterally programmed by a company in such a way that it matches the price of another competitor that can be found inside or outside the blockchain ledger.[119] If the consumer fulfills the conditions in the smart contract (e.g., transfer of the respective purchase price), the transaction is executed and entered in the blockchain ledger. This reinforces the transparency explosion, which in turn can cause increased parallel behavior (via blockchain) by other companies. In addition, smart contracts can implement variables to detect and punish deviant behavior by a company (e.g., price war).[120] For example, a smart contract could unilaterally demand an x-fold lower price as soon as a competitor's price falls below a previously defined threshold in the smart contract. A smart contract between a company and its market counterpart can

---

[117] For example, CONG/HE, 1757: "However, as mentioned before, generating decentralized consensus also inevitably leads to greater knowledge of aggregate business condition on the blockchain, which we show can foster tacit collusion among sellers."; FAELLA GIANLUCA/ROMANO VALERIO COSIMO, Artificial intelligence and blockchain: an introduction to competition issues, Competition Law & Policy Debate, 5(3) (2019), 19–25, 23: "Furthermore, blockchain's potential to facilitate tacit collusion may have to be taken into account in the assessment of coordinated effects."; MASSAROTTO GIOVANNA, From digital to blockchain markets: What role for Antitrust and regulation, January 26, 2019, available at <https://ssrn.com/abstract=3323420>, 14: "In public blockchain transactions' data are distributed and stored in a vast number of computers (the decentralized blockchain ledger) which can make easier for competitors to tacitly collude despite the parties of transactions are kept secret."; see also COLANGELO/MEZZANOTTE, 8 and DENG, 5.

[118] Cf. HEINEMANN, 20.

[119] See the so-called blockchain oracles, which feed information from outside the blockchain into smart contracts. CALDARELLI GIULIO, Understanding the Blockchain Oracle Problem: A Call for Action, Information, 11(11) (2020), 1–19, 1 ff. for more information on the "oracle problem".

[120] Cf. EZRACHI/STUCKE, Tacit Collusion, 242.

thus have an indirect impact on the competitive relationship between two competitors by facilitating the alignment of competitive parameters and making deviation more difficult.

5.3.1.3 In public and private blockchains

61 A company can engage in parallel behavior using smart contracts on a public or private blockchain. In the public blockchain, the parallel behavior is potentially visible to everyone. This is especially true in the case of transparency explosion, where the "opacity effect" is reduced and even the company engaging in parallel behavior might be identified. However, since parallel behavior is lawful, visibility should not lead to parallel behavior hiding from competition authorities behind a private blockchain, as might be the case with unlawful agreements.[121] However, a similar deterrent effect as in the case of unlawful agreements could occur especially in the gray area between agreements and parallel conduct, where there is still a certain degree of legal uncertainty.[122] This uncertainty should urgently be reduced (also) in the context of blockchain. Otherwise the problem will – in case of doubt – shift to the private blockchain, which the antitrust authorities can penetrate and monitor less easily than the public blockchain.[123]

62 The second case concerns private blockchain. If a company intends to send its "communication over the market" only to a select group of market participants, it could process transactions over whichever private blockchain these participants are also members (e.g., blockchain with companies in the same industry). Compared to general algorithms, the scope of transparency can thus be limited to specific targets. However, this unilateral activity might constitute an inadmissible information "exchange". Data in a private blockchain is only accessible to the limited group of blockchain participants (with read rights) and is therefore not public as it is, for example, in a public blockchain. If the transaction has a competition-sensitive content, the unilateral disclosure of information in a private blockchain is to be treated as a concerted practice and not as mere parallel behavior.[124]

[121] Cf. SCHREPEL, Collusion, 150.

[122] Cf. THOMAS, 172.

[123] Cf. SCHREPEL, Collusion, 150.

[124] Cf. SCHREPEL, Collusion, 131 f.

5.3.2 "Hub and spoke"

5.3.2.1 Distinction from concerted practice

63 In the second scenario "hub and spoke" different competitors use the same algorithm and/or data pool, which can lead to an alignment of competitive parameters such as prices or quantities. Such a scenario is also conceivable in the context of blockchain, as the blockchain (in a broader sense) is nothing other than a combination of data and special algorithms governing the storage of that data.[125] The following explanations differentiate between public and private blockchain on the one hand and between data pools and algorithms on the other.

64 The public blockchain is a technology which, due to its decentralized nature, leads to a diffusion of responsibility and control among the individual nodes. At first glance, a centralized procedure, as is the case with the hub, is not conceivable due to the lack of centralized governance.[126] At second glance, however, coordination may take place on a logical-abstract level in that the blockchain participants – similar to platform participants – subject themselves to the same consensus algorithms, which can ultimately lead to an exchange of information.[127] However, on a third view, it is the blockchain participants themselves who decide on the consensus algorithms or the protocol within the self-governed nature of the public blockchain.[128] In contrast to platform participants,

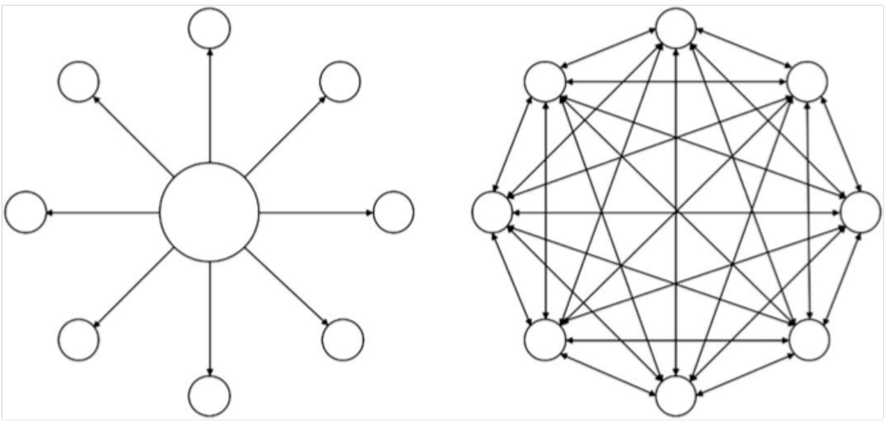

Figure 4: "Hub and spoke" (left) and "mesh" of the public blockchain (right).

[125] *Supra* para. 6.

[126] However, some of the public blockchains also attempt to establish a form of centralized governance. See, for example, SCHREPEL THIBAULT, Blockchain & competition: Thibault Schrepel on what authorities can do about eventual risks, OECD Competition Division of August 27, 2018, available at <https://www.youtube.com/watch?v=ptLDhYSEGpI>, from 2:09; whether a hub and spoke situation exists must especially then be assessed on a case-by-case basis.

[127] LOUVEN SEBASTIAN/SAIVE DAVID, Antitrust by Design – The prohibition of anti-competitive coordination and the consensus mechanism of the blockchain, GRUR Int. 2019, 537–543, 483; cf. GUPTA VINAY, The Promise of Blockchain Is a World Without Middlemen, Harvard Business Review of March 6, 2017, available at: <https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen>.

[128] Cf. NARAINE, 320 ff. about centrality and decentrality aspects of network paradigm in the sport industry.

blockchain participants govern the blockchain themselves, communicating *directly* with each other and not over a technological infrastructure of a third party like a platform provider ("mesh" according to figure 4). Therefore, blockchain participants are spokes and hubs at the same time. This, however, excludes the hub and spoke situation by definition. Rather, it is a classic case of *explicit* agreement by blockchain participants – should the blockchain algorithm have the effect or purpose of restricting competition. For these reasons, the hub and spoke scenario is of little significance in the public blockchain. The following explanations will thus be limited to the private blockchain.

65 Since private blockchains are generally based on centralized governance, a more differentiated distinction must be made between alignment by means of algorithms and data. With regard to algorithms, blockchain algorithms can be programmed so that, as in the *Eturas* case[129], they have anti-competitive effects if used by the spokes. Here again, a special distinction must be made between consensus algorithms and smart contracts. With regard to the consensus mechanism, the controlling actor of the private blockchain has the greatest possible freedom of design. Thus, a wide variety of types of mechanisms exist.[130] In addition, smart contracts may also be used to coordinate. In addition to the controlling actor, also blockchain participants may be considered "hubs" – depending on the design of the blockchain and their freedom to create and use smart contracts. For example, a smart contract could be programmed with the effect of fixing prices.[131] Since smart contracts might be increasingly used in the future, it will be of decisive importance that their collusive effects or purposes can be excluded or at least be reduced (e.g., through certification[132]) before they fundamentally become "unstoppable code".

66 With regard to data pools, the "ringleader [...] could choose to create a hub and spoke in which only he can access all information and manage the collusion".[133] The spokes consist of the blockchain participants, which are merely connected to each other via the ringleader or rather the private blockchain. They can only read the transactions to a limited extent and do not communicate directly with each other.[134] Accordingly, this is a "classical" sub and spoke-situation like that on platforms.

[129] ECJ, 21.01.2016, C-74/14 – *Eturas*, para. 44.

[130] Schrepel, Collusion, 136 ff. with more information on proof of work, stake, burn, authority, capacity, and storage.

[131] Cf. Schrepel, Collusion, 142; Hutchinson Christophe Samuel/Ruchkina Gulnara Fliurovna/Pavlikov Sergei Guerasimovich, Tacit Collusion on Steroids: The Potential Risks for Competition Resulting from the Use of Algorithm Technology by Companies, Sustainability, 13 (2021), 1–14, 10; Picht Peter Georg/Freund Benedikt, Competition (law) in the era of algorithms, E.C.L.R., 39(9) (2018), 403–410, 406.

[132] See Prinz Wolfgang/Schulte Axel T., Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen, Fraunhofer-Gesellschaft, November 2017, available at <https://www.iuk.fraunhofer.de/content/dam/iuk/de/documents/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf>, 12.

[133] Schrepel, Collusion, 149.

[134] See also BKartA/ADLC, Algorithms, 34.

5.3.2.2 Using blockchain algorithms

67 In the context of parallel behavior, it has already been indicated that the public blockchain is not of great importance due to its distributed governance. Indeed, a blockchain participant could intend to engage in parallel behavior using blockchain algorithms, since he himself contributed to their creation and communicated with the other blockchain participants in the process. Such direct communication rules out not only a hub and spoke situation, but also parallel behavior.

68 If a company does not program a smart contract itself, but uses an existing template on a marketplace for smart contracts,[135] it will often be difficult for it to assess, particularly in the case of complex smart contracts, whether or not it is entering into an unlawful agreement or mere parallel behavior. However, as mentioned above, certification and approval could help. If it were possible to "filter out" those smart contracts that have the purpose or effect of causing collusion,[136] the difficulties in proving intent, such as those that arose in the Eturas case, would become superfluous from the outset, at least in these instances.[137]

5.3.2.3 Using blockchain data

69 On the other hand, parallel behavior could take place at the blockchain data level. Here, too, it is of decisive importance whether a company has an intent to collude or "merely" behave in parallel. Similar to the Eturas case (which, however, only dealt with the algorithms scenario), certain circumstantial evidence may also speak in favor of an intent or tacit approval of the concerted conduct (e.g., anti-competitive statements by the "hub" which were received by the "spoke").[138] In addition, a blockchain participant may rebut the presumption of concerted practice if it has publicly distanced itself from the identified conduct that has the effect or purpose of restricting competition or has reported it to an authority.[139]

70 However, it is also important to bear in mind that in scenarios where the controlling actor decides on the storage and maintenance of the data in a private blockchain, it does not differ significantly from traditional databases. In this respect, there are no specific

---

[135] PRINZ/SCHULTE, 12.

[136] ECJ, 21.01.2016, C-74/14 – *Eturas*, para. 38 f.

[137] Cf. also the certification of AI algorithms: MANGELSDORF AXEL/GABRIEL PETER/WEIMER MARTIN, Die Zertifizierung von KI: Mehr Sicherheit für alle – oder unnötiger Ballast?, iit perspektive, Working Paper of the Institute for Innovation and Technology No. 58, available at: <https://www.iit-berlin.de/wp-content/uploads/2021/04/2021_04_30_iit-perspektive_Nr-58_Zertifizierung_von_KI.pdf>, 2 ff.

[138] ECJ, 21.01.2016, C-74/14 – *Eturas*, para. 36; LOUVEN, 482 f.

[139] Cf. ECJ, 21.01.2016, C-74/14 – *Eturas*, para. 46.

advantages worth mentioning for either the "hub" or the "spokes".[140] Thus, essentially no new blockchain-specific issues arise for competition law.

5.3.3 "Digital eye"

71 In the "digital eye" scenario the anti-competitive effects of algorithms based on AI are discussed. However, as this scenario is currently still largely futuristic and of no practical significance for either general or blockchain algorithms,[141] this chapter only addresses the central problems. Technically, it is possible that smart contracts implement aspects of AI so that the optimal collusive equilibrium can be established.[142] The interplay of blockchain and AI could thus lead to an even greater risk of collusion, as collusion is brought about even when it was not intended by the companies.[143]

72 This also applies with regard to parallel behavior: "Blockchain and AI have a symbiotic relationship. [...] Blockchain brings trust [...] to data. [...] On the other hand, AI brings intelligence to data. [...] With trust and intelligence, you have confidence. With confidence, you gain adoption, the result of authenticity, augmentation and automation."[144] As previously explained, increased and more aggressive parallel behavior may be brought about especially by trust – or rather by the qualitative transparency of blockchain. However, this is even more true when trust is combined with the "intelligence" of AI. The optimal collusive equilibrium is more likely to be calculated if the AI processes high-quality data. In contrast to general AI algorithms, which often also process incorrect, incomplete or outdated data, the calculations of AI-driven smart contracts may be closer to the optimal collusive equilibrium and thus have more harmful competitive effects.[145]

[140] Cf. Catalini Christian/Tucker Catherine, Antitrust and Costless Verification: An Optimistic and a Pessimistic View of the Implications of Blockchain Technology, MIT Sloan School Working Paper 5523-18, 4.

[141] Cf. Schrepel, Collusion, 142.

[142] Schrepel, Collusion, 142.

[143] Faella/Romano, 23.

[144] Cuomo Jerry, Integrating AI + Blockchain, IBM, available at <https://www.ibm.com/topics/blockchain-ai>, from 2:23.

[145] This, however, presupposes that the data that enters the blockchain "from outside" is also adequately examined for its quality. This concerns, for example, data that was not natively generated on-chain (and that is not publicly available) or that is provided through oracles.

5.4 New forms of parallel behavior?

5.4.1 Cooperative and dynamic explicit collusion

73 In view of the scenarios of blockchain-based parallel behavior just mentioned, the question arises whether they represent new forms of parallel behavior as a result of the peculiarities of the blockchain. According to Thibault Schrepel, agreements via smart contracts have two central peculiarities compared to general algorithms.

74 First, agreements in the world "outside" the blockchain are in principle non-cooperative games. The stability of the agreements depends on the respective interests of the participants and their actions, which are usually unpredictable or difficult to predict. In contrast, with blockchain-based collusion, the game transforms into a cooperative one, as the smart contract significantly increases the stability of the collusion.[146] In fact, its enforcement, including monitoring and possible penalties, no longer depends on the will of the colluding partners, but only on the principally immutable smart contract itself (or respectively the fulfillment of the conditions it contains). This considerably increases the trust of all partners in the continuation of the agreement (so-called cooperative collusion).[147]

75 Second, agreements via general algorithms are static in nature as they follow a linear and predictable learning curve. On the other hand, blockchain-based agreements are dynamic in nature when a clause of the smart contract refers to a decentralized app (DApp).[148] Thus, external forces of all possible natures can be implemented into the collusion, so that as a result of this flexibility, a variety of different cartel violations can be induced in a non-linear manner (so-called dynamic collusion).[149]

5.4.2 Cooperative and dynamic parallel behavior?

76 These explanations have shown that it is primarily the special nature of the smart contract that leads to cooperative (explicit) collusion. Therefore, a cooperative *parallel behavior* in which competitors communicate directly by means of a horizontal smart contract is ruled out by definition. However, parallel behavior can be stabilized other than by a horizontal smart contract.

77 In the case of cooperative explicit collusion, stability is directly based on the technological architecture of the smart contract: deviations are significantly technically impeded and automatically sanctioned. In contrast, in cooperative parallel behavior,

[146] SCHREPEL, Collusion, 125.

[147] On the whole, see SCHREPEL, Unimportance; see also BRUDNA, 17 ff.

[148] SCHREPEL, Collusion, 142.

[149] On the whole, see SCHREPEL, Unimportance.

stability may arise from other circumstances, and in this paper the stabilizing effect due to the quantitative and qualitative transparency of the blockchain will receive closer attention. Accordingly, the parallel behavior (also) based on blockchain transparency or the use of vertical smart contracts may reduce uncertainty about the future behavior of competitors and thus lead to increased stability of parallel behavior.

78 Moreover, just like explicit collusion, parallel behavior can be dynamic in nature. Again, the clauses of vertical smart contracts can reference DApps, leading to a large variety of non-linear behaviors (dynamic parallel behavior). This, however, leads to more unpredictable behavior for both competition authorities and other competitors. First, dynamic conduct may complicate its characterization as permissible parallel behavior or impermissible agreement by the competition authority. Depending on how the DApps function and whether there is communication among competitors, it is conceivable that the same smart contract could lead to a parallel behavior by company A and – at the same time – an agreement between company B and C. For example, the DApps could trigger a variable in the smart contract leading to communication between the competitors only in certain cases. In addition, it is conceivable that only the combination of DApp and smart contract leads to an impermissible agreement at all, while they are unproblematic when considered individually. In this respect, dynamic parallel behavior also raises competition law issues.

79 However, increased dynamism generally leads to lower predictability, which puts the cooperative character of parallel behavior into perspective.[150] While blockchain and smart contracts create increased quantitative and qualitative transparency, they also make predictability more difficult especially – but not only – as a result of the complex interactions between smart contracts and DApps. As a result, transparency primarily relates to the history of transaction data and less to future transactions (using smart contracts). Since especially transparency regarding *future* behavior may lead to increased and more aggressive parallel behavior (or even prohibited agreements), even an increased qualitative transparency is not to be assessed as fundamentally problematic from a competition law perspective. As the amount of blockchain data increases, so does complexity due to the more frequent use of blockchain, smart contracts and DApps. This in turn may reduce predictability.

80 However, it ultimately remains to be seen how companies will deal with this new type of transparency in practice and whether it can lead to more aggressive and stable parallel behavior. As in the area of "cooperative" and "dynamic" explicit collusion,[151] robust economic analyses are still lacking.

[150] Cf. SCHREPEL, Unimportance.

[151] SCHREPEL, Unimportance.

5.5 Interim conclusion

81 This chapter has focused on the scenarios of parallel behavior using blockchain. In the "messenger" scenario, the market behavior of competitors can be analyzed to align behavior. Transactions can also be triggered automatically by smart contracts. The types of parallel behavior vary depending on whether a public or private blockchain is used. In the "hub and spoke" scenario, only the private blockchain is of significant importance in terms of algorithms and data pools. Next, "digital eye" scenario does not yet exhibit practical relevance. Lastly, novel forms of parallel behavior may occur.

6 Conclusion and outlook

82 This final chapter briefly summarizes and critically examines the results of this paper. In response to the first research question, **"What are the key elements that – combined with blockchain – may lead to increased market transparency in quantitative and qualitative terms?"**, the second chapter introduced the phenomenon of transparency explosion. It is primarily based on big data analytics, blockchain and trust economy. Each of these components has the capacity in itself to (significantly) increase market transparency in potentially all markets. But when they are combined, the result is a highly explosive transparency mix consisting of efficient analytics tools, large amount of (high quality) data, and economic incentives to create and increase market transparency. This mixture may lead to both a quantitative and a qualitative transparency explosion. Despite all relativizations, this explosive mixture may lead to increased market transparency. Subsequently, the third chapter briefly dealt with "classical" parallel behavior from an economic and legal point of view. The fourth chapter addressed the "modern" parallel behavior by means of general algorithms. After the classification of general algorithms, the four scenarios "messenger", "hub and spoke", "the predictable agent" and "digital eye" were applied to algorithm-based parallel behavior and the new forms of parallel behavior were pointed out.

83 Building on this, the fifth chapter took an in-depth look at "modern" parallel behavior using blockchain to answer the second research question, **"What are the main types of parallel behavior that can be technically implemented with blockchain?"**. First, it was established that blockchain algorithms are a specific subform of general algorithms and that the trust economy also acts (indirectly) in the horizontal relationship. Due to certain competitive conditions, which include also market transparency, a company might decide to engage in parallel behavior and use the blockchain for this purpose: in the "messenger" scenario, it was shown that the market behavior of competitors can be analyzed and one's own behavior can be adjusted accordingly. Transactions can also be triggered automatically by smart contracts. The types of parallel behavior vary depending on whether a public or private blockchain is used. In the "hub and spoke"

scenario, only the private blockchain is of importance regarding algorithms and data pools. The "digital eye" scenario does not (yet) exhibit any practical relevance. Finally, the new forms of parallel behavior were discussed. However, they still have to withstand further economic analyses.

84 Ultimately, it is questionable whether there is any need for action in light of relativizations and uncertainties – as is already the case with general algorithms.[152] The blockchain transparency (or generally: the transparency explosion) and the possible emergence of greater and more aggressive parallel behavior by means of blockchain are both accompanied by numerous unknown variables. As a result, the uncertainty is even greater than in the context of general algorithm-based parallel behavior. From the standpoint of the author, the implementation of new solutions should therefore be restrained and premature solutions should be avoided – at least until economic analyses have proven an increased threat to competition.[153] Otherwise, there is a risk that competition law will prevent what it actually tries to achieve: "optimize[d] prices and the quality of goods and services, […]".[154]

[152] WECHE/WECK, 928.

[153] In the case of an increased risk, for example, the concept of agreement could be modified. See, for example, HEINEMANN, 25 ff. and PICHT/FREUND, 404 ff.

[154] See the quote in the introduction.