# SMART CONTRACTS AND BLOCKCHAINS: STEROID FOR COLLUSION?

*By Ai Deng*[1]

## I. WHAT IS A SMART CONTRACT?

It is late afternoon. Our stomachs are calling. We walk up to a vending machine. We stare at the selection for a minute, swipe a card or insert some cash, and make our choice. The machine (usually) gets us the snack we want and also figures out how much change to give back. It is such a routine part of life that most of us probably don't realize that we and the vendor just engaged in a transaction that is based essentially on a *smart* contract. Smart contracts are those that self-execute as soon as certain contractual terms are met.

The idea is not new. Every time we set up an automatic recurring bank transfer or payment, we effectively create a smart contract with the financial institution. Of course, a smart contract can do a lot more. For example, given the inevitability of smart vehicles in the not-so-distant future, it is easy to imagine a smart insurance contract where sensors on the vehicle detect who is at fault in an accident, insurance rates are adjusted accordingly, and an insurance payment is made automatically—all with minimal human involvement.[2]

The idea of "smart contracts" was conceptualized by computer scientist Nick Szabo in 1994:[3]

> A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.

As indicated by the quote from Szabo, in its simplest form, a smart contract is written as a machine-readable computer program. For example, on the popular smart contract

---

1 Ai Deng, PhD, is a Principal at Bates White Economic Consulting and a lecturer at the Advanced Academic Program, Johns Hopkins University. He has over a decade of consulting experience and has written extensively on the use of analytical tools in litigation. His current research interests include the interaction between technologies (artificial intelligence, machine learning, blockchains) and antitrust and other forms of market manipulation. His publications can be found at his LinkedIn page https://www.linkedin.com/in/aideng/. He can be reached at ai.deng@bateswhite.com. The views expressed in this paper are those of the author and do not necessarily reflect the opinions of Bates White or its clients, Johns Hopkins University, or its affiliates. The title is inspired by Professors Ariel Ezrachi and Maurice E. Stucke's popular book *Virtual Competition*. Heather Dittbrenner provided excellent editorial assistance. I thank Dr. Julian Chan and Dr. Paul A. Johnson for helpful discussions, Bob Freitas, Qianwei Fu, Anna Fabish for their help with the article.

2 Some have further generalized the concept of a smart contract to mean any computer program that can be executed on a blockchain.

3 Nick Szabo (1994), "Smart Contracts," available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

platform Ethereum, smart contracts are created using a particular programming language called Solidity.

## II. WHAT IS A BLOCKCHAIN, AND WHY DO WE NEED IT FOR A SMART CONTRACT?

We began by asking whether smart contracts and blockchains might be a catalyst for collusion. To answer that question, we must first understand blockchains. One can think of a blockchain as a particular type of information management system or, more specifically, a ledger system. It is also the technology that underpins the much-talked-about Bitcoin and other cryptocurrencies. A blockchain has three key characteristics: *distributed*, *trustless*, and *consensus*. Let's use a simple example to build an understanding of how a blockchain works.[4]

Imagine that you have just signed a contract to rent an apartment. As is typically done today, both you and the building management would keep an identical copy of the contract. The idea is that neither party can unilaterally modify any of the terms without revealing a discrepancy. You don't have to trust your landlord, nor does your landlord have to trust you. Obviously, both parties are free to make additional copies of the contract. You may decide to ask one or more friends or family members to keep a copy because you are concerned about theft or simply about the possibility of losing your copy. Your landlord may do the same. When a contract is "distributed" in this way, neither party has an incentive to manipulate the agreement. You have created an environment that works for both parties without necessarily trusting each other.[5] This is exactly what the blockchain enables us to do. One can think of a block in the blockchain as a collection of these contracts. The blocks are distributed in an analogous way.

There is, however, more to worry about. Suppose you have a pet dog that has a history of destroying your important documents, or that some of your friends may want to mess with you by changing terms (say, your monthly rent amount) in their copies. Your landlord may have a similar concern. At least one way to get around such a problem is to rely on *consensus*. That is, we are going to believe the version that is consistent with at least 51% of the copies. This is how blockchain works as well, that is, the "truth" on a blockchain is based on consensus.[6] For this reason, the so-called *decentralized consensus* is a fundamental feature of a blockchain.

Where does the "chain" part of the blockchain come from? Let's consider the perspective of the landlord for a moment. The landlord may want to track the property you are renting over time. He or she may have rented the same apartment to someone else before you. The "chain" simply refers to the sequence of transactions or blocks of

4 For a more rigorous discussion of blockchain and cryptocurrency, *see* Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton, NJ: Princeton University Press.

5 Of course, a conventional way to operate in a trustless world is to involve a trusted third party such as a bank or other financial institution. The use of a blockchain eliminates the need for such a trusted third party.

6 We are abstracting from the actual mechanism of reaching a consensus. The consensus mechanism is an active area of research and debate in the blockchain field. Some readers may have heard about "proof of work" or "proof of stake" as potential mechanisms.

transactions that are recorded in the system. The current block is always linked to the previous block. This allows one to track back all the way to the origin of a transaction, or the ownership history of a property. And thanks to the ingenuity of a design feature of the blockchain, people have little incentive, and for practical purposes are unable, to change the information in a block.[7] This is known as the "immutability" of the blockchain. And because the blockchain is immutable, the transactions are also "auditable." The relevance of this auditable feature will become clear when we discuss cartels and blockchains in the next section. Finally, it should be clear that although we use a rental contract as our example, any transaction or any information can be recorded on a blockchain.

Now that we have an understanding of what a blockchain is and some of its most important features, such as "distributed consensus" and "immutability," we can understand why a blockchain is an ideal platform for smart contracts. Most obviously, once a contract is written and "posted" in a block, parties have confidence that it won't be (easily) altered or manipulated, either inadvertently or maliciously (say, by a hacker). Of course, as still a relatively new technology, smart contracts on blockchains are not without their limitations.[8]

## III. IMPLICATIONS FOR COLLUSION

Companies can collaborate to form a so-called blockchain consortium. And these consortia are growing at a fast pace. According to a Deloitte report from August 2017, more than 40 consortia have been formed globally—most of them in the six months preceding that time.[9] Well-known business-focused blockchain consortia include **PTDL** (post-trade distributed ledger group), **DTC** (digital trade chain), **B3i** (blockchain insurance industry initiative), and **R3**. The blockchains in these consortia can be made private and require permission to join and use. To continue our rental contract example, a private blockchain is analogous to the situation in which you send the contract to only your five closest friends, instead of everyone you know. This is in contrast to a public blockchain, such as the one for cryptocurrency Bitcoin. On these private or permissioned blockchains, only members have access to the hosted information. Economists and courts recognize that

7 More technically, each block contains a unique identifier, known as the "hash," of the previous block. This identifier is a mathematical compression of all of the information in the block. If anything changes, the identifier also changes. Therefore, if someone tries to alter the information in the block, any change would reveal itself through the hash values. With the hash values, the system does not need to "remember" the entire history of the information or transactions on a blockchain to validate a transaction and ensure immutability. Of course, immutability is to some extent still relative. For an interesting perspective, *see* Gideon Greenspan (May 9, 2017), "The Blockchain Immutability Myth," *CoinDesk*, available at https://www.coindesk.com/blockchain-immutability-myth/.

8 For example, a smart contract would implement exactly what the computer program tells it to, regardless of whether there are any programming errors; software problems could also cause errors in the smart contract. *See* Mark Gates (2017), *Ethereum: Complete Guide to Understanding Ethereum, Blockchain, Smart Contracts, ICOs, and Decentralized Apps* (audiobook). Other recent research identified a number of security issues with the existing smart contracts. *See* Ivica Nikolíc, Aashish Kolluri, Ilya Sergey, Prateek Saxena, and Aquinas Hobor (2018), "Finding the Greedy, Prodigal, and Suicidal Contracts at Scale," available at https://arxiv.org/pdf/1802.06038.pdf.

9 Peter Gratzke, David Schatsky, and Eric Piscini (August 16, 2017), "Banding Together for Blockchain." *Deloitte Insights*, available at https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/ emergence-of-blockchain-consortia.html.

information sharing and transparency can facilitate collusion.[10] Let's take a closer look at the smart contracts on a blockchain and how they might do that.

Let's start with the case of explicit collusion. A cartel can take advantage of a private/permissioned blockchain's distributed system in two ways to efficiently implement a cartel agreement. The first is what I call the "traditional way," where cartel members engage in traditional "off-line" discussions to implement an agreement and use the blockchain solely to share competitively sensitive information (production, sales, prices, etc.) to enable monitoring of cartel member behavior and hence reduce the incentive to "cheat." Arguably, there is not much new here from the perspective of an antitrust authority.

The second way is much more sophisticated and largely blockchain and smart contract driven. In addition to using the private blockchain to share information, a cartel could codify its agreement into a smart contract. For example, a smart contract could automate interfirm transfer, *i.e.*, side payments (as a way to maintain the cartel agreement) when certain conditions are met, and punishment upon detection of cheating. Using the Internet of Things (IoT), firms in a cartel could even grant other cartel members access to artificial intelligence (AI)-based sensors to automatically monitor, say, a competitor's production activity. If the AI detects any deviation from the cartel agreement, it could trigger an automatic retaliatory response codified in the smart contract. Recall that because the smart contract is built on a blockchain, in theory, no party could modify the smart contract without the other cartel members knowing. This significantly increases the credibility of a punishment.

As we can see, smart contracts and blockchains give an explicit cartel a whole new and efficient way to implement an agreement. It may be tempting to think it is a "no-brainer" that an explicit cartel would seek to take full advantage of this ability. But is it? In most jurisdictions, an explicit cartel is illegal, which explains why in many price fixing cases, the cartel members have taken pains to avoid detection. They meet in private hotel rooms and strictly limit their discussions to a small circle of people. Seldom does a cartel have a formal agreement or contract. A smart contract, albeit being a set of computer codes, leaves a paper trail just like a traditional paper contract. This is related to the "auditable" feature of a blockchain we noted above. Of course, specific programming expertise (say, with Solidity on Ethereum) will be required to understand fully these computer code-scripted contracts.

Let's turn now to the more interesting case of tacit collusion. Certain types of information sharing and transparency can facilitate tacit collusion. There is some empirical evidence that increased transparency has indeed led to tacit collusion in real markets.[11] Firms should think carefully about the information they share on a blockchain

---

10 David C. Kully and Josias N. Dewey (March 2017), "Blockchain Collaborators Should Be Attuned to Potential Antitrust Issues." Corporate Counsel Connect article, Thompson Reuters, available at https://legalsolutions.thomsonreuters.com/law-products/news-views/corporate-counsel/blockchain-collaborators-attuned-to-potential-antitrust. *See also* Izabella Kaminsak (May 11, 2015), "Exposing the 'If We Call It a Blockchain, Perhaps It Won't Be Deemed a Cartel?' Tactic" *Financial Times*.

11 *See* Jorge Lemus and Luco Fernando (2017), "Pricing Dynamics, Leadership, and Misreporting: Evidence from a Mandatory Price-Disclosure Intervention" (Working paper).

and whether their information sharing may be construed as a tacit way to coordinate to harm competition.

In certain situations, (tacit) collusion could also be facilitated in a more subtle way. Suppose competitors form a blockchain consortium and intend to take full advantage of smart contracts in their business operations. For example, they plan to deploy a smart contract that automatically transfers funds from the customer to the seller if a shipment arrives at the designated port of delivery. To implement such a smart contract, external information (for example, the verification that the shipment has been delivered) is needed. Such external information is provided by what's known as an "oracle service."[12] Assuming that other firms in the blockchain consortium also have a presence at the customer's delivery location, the consortium members may choose to rely on each other as "record keepers" for the oracle service. That is, firm A could make requests to firms B, C, D, etc., to confirm whether a shipment has arrived.[13] The extent of a confirmation could range from a simple yes or no to estimating the quantity shipped using AI sensors and the IoT. Clearly, such oracle services are crucial to unlock fully the value of smart contracts for their intended use.

In such an environment, two economists from the University of Chicago's Booth School of Business have shown in a recent article that collusive outcomes can be more easily reached.[14] The intuition comes from the seminal paper of Green and Porter (1984).[15] Green and Porter show that imperfect monitoring of cartel members' behavior coupled with demand uncertainty could lead to price wars, disrupting the plan to raise or maintain the prices of a cartel. When a cartel member does not observe a competitor's behavior (say, production or sales), it does not know whether its own declining sales are caused by the cheating behavior of others or simply by an unlucky negative aggregate demand shock. The more volatile the aggregate demand is, the more difficult this inference becomes. To *internalize* the demand uncertainty, Green and Porter show that disruptive price wars can be a rational and disciplinary course of action by the cartel members. Going back to our new smart contract and blockchain environment in which competitors provide "oracle services" for each other, we notice that, as a byproduct, competitors now have an excellent

12 Lauslahti et al. describe the oracle service, also known as "API router," in the following way: in this type of smart contract, a program based on blockchain technology collects data from one or more third-party software interfaces or other sources and relays the collected information as a report to a pre-determined recipient. *See* Kristian Lauslahti, Juri Mattila, and Timo Seppala (2017),"Smart Contracts—How Will Blockchain Technology Affect Contractual Practices?" ETLA Report no. 68, Research Institute of the Finnish Economy.

13 In a trustless world, a customer's own verification will not be sufficient.

14 Lin William Cong and Zhiguo He (2018), "Blockchain Disruption and Smart Contacts" (Working paper). I focus on the intuitions. Readers interested in technical details are encouraged to read the article for more in-depth discussions.

15 E.J. Green and R.H. Porter (1984), "Noncooperative Collusion under Imperfect Price Information," *Econometrica*, 52 (1): 87–100.

opportunity to monitor the aggregated demand and even individual firm sales.[16] This could mitigate the destabilizing effects of aggregated demand uncertainty.[17]

How do we address this potential side effect of smart contracts on a blockchain consortium? An intuitively appealing approach is simply to keep the competitors and the record keepers separate. But in practice, doing so may present difficulties, especially when no alternative record keepers are available.[18] Another possibility is to institute independent third-party oracle service providers, funded by the competitors in the consortium. If complete separation is impossible or too costly, yet another possibility is to explore the feasibility of establishing firewalls within the firms to separate their record-keeping function from other business operations. This is an area worthy of further exploration. Lastly, we note that the oracle services provided by competitors may be viewed as a type of (collusion-) "facilitating practice" that antitrust authorities around the world have wrestled with for many years.[19]

## IV. CONCLUSION

In this article, we introduced the concepts of a smart contract, a blockchain, and a blockchain consortium. While there are other antitrust considerations with a blockchain consortium, such as standard setting and unfair competition, we focused on the implications these emerging technologies have on both explicit and tacit collusion. We argue that although smart contracts offer an efficient way to enforce any agreement, an explicit cartel may find it unpalatable to codify its illegal agreement in the form of a smart contract. Of course, this does not mean that cartels would never take advantage of smart contracts to carry out their operations. To uncover smart contract-based collusion, antitrust agencies will need readily accessible expertise in smart contract design and programming.

We also discussed how collusion may arise in more subtle ways, as highlighted by recent academic research. An open question is how to achieve the efficiency of distributed consensus made available by record keepers without increasing the antitrust risk of collusion.

It is encouraging that many antitrust practitioners have already advised corporations to exercise care when joining a blockchain consortium and deciding which information to share. While the directions of technologies are notoriously hard to predict, it is safe to assume that as more companies and governments continue to explore what blockchain technology has to offer, more subtle antitrust issues will arise for those of us in the antitrust and economics community to think about and debate. It is an exciting time.

---

16 The blockchain may be set up so that competitors do not know which firm is making the request. In that case, the consortium members would still be able to infer, possibly imperfectly, the aggregate demand. If the identity of the seller is also revealed in the consensus-generating process, competitors would have much more information about each other.

17 Note that blockchain technology per se does not give rise to the issue discussed here.

18 As noted by Cong and He, on some blockchains such as Symbiont, record keepers tend to be a separate group from the end users. *Supra* note 14, at 33.

19 For an international perspective, *see* 2007 OECD Roundtable on Facilitating Practices in Oligopolies, available at https://www.oecd.org/daf/competition/41472165.pdf.