BLOCK CHANGE: THE FALLACY OF BLOCKCHAIN IMMUTABILITY AND CARTEL GOVERNANCE[1]

Roberto D. Taufick[2]

Abstract: This article complements professor Schrepel's observations by shedding light on how consensus rules can be built to automatically erase or create a hard fork for sensitive information when immutability no longer interests the parties to a cartel.

By elaborating on how shifting from immutability to mutability and vice-versa is the most relevant feature to turn blockchain into an unprecedented threat to fight cartels, this paper complements professor Shrepel's observations on how blockchain can enhance opacity for outsiders and at the same time improve transparency for cartel members.

Keywords*:* blockchain, cartel, 51 percent attack, opacity, mutability

Palavras-chaves: blockchain, cartel, ataque por 51 por cento, opacidade, mutabilidade

Collusion and blockchain

The two most important works in blockchain and antitrust have been written by Utrecht Law School professor Thibault Schrepel, both published in 2019. Thibault's works explain in details how blockchain works and why blockchain's consensus rules can help create opportunities for both unilateral abuses and collusion. In this article I rely on professor Shrepel's

---

[1] Forthcoming publication of the work in : "1 NOTRE DAME J. EMERGING TECH. ([2020]). "© [2019] Roberto Taufick. Individuals and nonprofit institutions may reproduce and distribute copies of this article in any format, at or below cost, for educational purposes, so long as each copy identifies the author, provides a citation to the Notre Dame Journal on Emerging Technologies, and includes this provision and copyright notice."

[2] Invited Lecturer in Antitrust Law, Fundação Getulio Vargas. Master of in Law, Science and Technology, Stanford Law School. 2015 Gregory Terrill Cox Summer Research Fellow, John M. Olin Program in Law and Economics, Stanford University. Works recognized both nationally and internationally, including two nominations as best soft law in Concurrences' 2019 Antitrust Writing Awards.

conceptual explorations of blockchain so as to limit the discussion in this paper to the use of the technology in conspiracies in restraint of trade, particularly cartels. This article complements professor Schrepel's observations by shedding light on how consensus rules can be built to automatically erase sensitive information or create a hard fork when immutability no longer interests cartel members.

First and foremost, one must take into account that the economics of collusion is always concerned with technologies that handle anonymization and tracking. While cartel detection depends heavily on the ability of authorities and society together to identify conspiracies in restraint of trade, the length of cartels also relies on the level of compliance with its internal rules -- in other words, on the ability of cartel members to oversee one another and on the effectiveness of sanctions for cartel defection. Inasmuch as tracking, anonymization and coercion are the pillars of an effective collusion, experts tend to look with skepticism at the flip side of innovations that offer privacy and sophisticated anti-piracy solutions[3][4].

Such skepticism is magnified by trustbusters' historical inability to enforce the law against cartels, corroborated by the fact that it took quite long for cartel busters to develop and eventually apply leniency programs. In this regard, professor Thibault Schrepel[5] raises the question if authorities are not

---

[3] For the purpose of this article, anti-piracy solutions are those designed to prevent copying and preserve things in their original condition (immutability).

[4] Professor Schrepel claims that immutability of registries would also increase compliance with the cartel, marketing it less necessary to rely on punishment: "Moreover, to the extent that the technology allows for binding agreements, the need to rely on the threat of punishment strategies diminishes, which make collusive outcomes more stable compared to such outcomes in noncooperative games." (Shrepel, 2019(a)).

[5]"We shall therefore address whether the success of leniency applications is put into danger by blockchain. In other words, if the destabilization of game strategies is limited by the technology. If that is the case, we shall then discuss whether this would be problematic. After all, several studies estimate that the percentage of detected cartels is only between 10% and 33% in the post-World War II era, which proves that leniency procedures are not sufficient in themselves. Perhaps antitrust and competition agencies give them too much importance, which the blockchain will help to correct. And if only 12 % of cartels ended naturally, blockchain may change that too.

[...]By undermining the effectiveness of leniency, blockchain will force competition agencies to become proactive again in order to readjust the balance, failing which

relying too much in leniency, a tool has proved to be of low effectiveness. His concern is confirmed by extensive data. Studies from the European Commission, for instance, claim that detection tends to be lower in cartels[6]. Studies of Connor and publications from the OECD show that we detect circa 30% of the total number of cartels and that punishment is still quite low in most jurisdictions[7].

That notwithstanding, the high levels of deterrence in the US and in Canada and recent progress made by other jurisdictions -- also incentivized by the US, aware of cross-border effects of global cartels -- have, according Connor, been enough to raise concern from conspirators and increase deterrence. It is in this context of slow but persisting progress -- now powered by stimuli to private enforcement as a tool to complement public

companies will have a growing sense of immunity from antitrust and competition law. In addition, strengthening proactive detection will increase the risk of punishment, and thus will force companies to seek leniency again; it is a true virtual circle. We therefore recommend that agencies focus their best efforts in this direction while keeping in mind that their detection work will be complicated by the 'opacity effect' created by blockchain. But the screening of collusive agreements remains possible on certain aspects, notably on market behaviors, which must be put at the center of antitrust and competition agencies' attention." (2019, a)

[6] "Even in the most effective system of private enforcement, not all the harm to consumers and other victims reflected in the above estimates will be compensated: this is because, inter alia, a considerable number of antitrust infringements will remain undetected. For hardcore cartels, the detection rate is generally assumed to be no more than somewhere between 10% and 20%. For other infringements, the detection rate is higher, but the 'conviction' rate (i.e. the rate of successful damages actions) is likely to be much lower, since claimants often find it very difficult to produce proof that the contested conduct produced actual anti-competitive effects. It also has to be assumed that some victims do not come forward to claim compensation, for instance because they prefer not to disrupt an ongoing business relationship with the infringer. Moreover, in some instances, victims will find it rather difficult to convince courts of a sufficiently close causal link between any particular damage and the infringement." [EC, 2008(a)]

[7] Connor. John M (2007) (2011). See also OECD (2005) and EC (2008, a). According to Connor, "[l]ooking at data on only contemporary international cartels, price effects seem undiminished. A sample of 284 private international cartels discovered since 1990 results in median estimated overcharges of 26% (Connors and Helmers 2006). Combine this mean with projected sales results in global injuries of more than $500 billion (in real 2005 dollars). This study finds that the mean overcharges of global cartels were about 30%."

enforcement[8] -- that one must understand that the development and use of technologies that most authorities take time to master can obstruct the path to competition on the merits and contain the slow but progressive movement towards greater antitrust enforcement. At the same time, it is also in this context that we are nonetheless bound to look at Schumpeterian innovations that also raise welfare and try to fight what can be used to cause perfidious attacks on competition -- at the same time avoiding the risk of contaminating our ability to take advantage of what is special in them and can serve us well, even in the fight against cartels.

So far technologies have created efficient ways to protect privacy by encrypting messages or by anonymizing users, raising parallel concerns that perpetrators of illegal activities would be shielded from ordinary investigations. In any case, the existence of a central unit -- the ultimate parent entity -- compelled by law to store sufficient information to hold the perpetrator accountable for the illicit activity avoids perfect anonymization.

Yet no tool had proved to deserve enough trust when it comes to ensuring that shared or distributed information is true. Much of the historical distrust in digital technologies comes from the fact that digital products can be copied and distributed as duplicates. Correcting that flaw usually demanded the use of a clearinghouse whose task was building a reputation as an efficient ex post identifier of fraud and of credit bureaus that screened one's past commitment to honoring debts. As we all know, both intermediaries delivered poor performance due to incomplete and untimely information.

Blockchain promised to remedy both. First, public blockchains like bitcoin are created to have no central authority and allow that both the nature of the operations and the people behind them are anonymized by hashing. Second, every register in blockchain was supposed to be unique -- without digital copies -- and immutable -- not possible to edit. As we will see, governance of blockchain platforms can trigger either of them: be it by means of hard forks (that create copies), be it by 51 percent attacks (that can delete, or edit data).

The ability to operate against blockchains original purpose also makes it possible to design the characteristics that, as we discuss in this paper, seem to be blockchain's most relevant feature for the economics of

[8] EC (2009, a), EC (2009, b).

collusion: protecting the identity of the users and at the same time offering a solution to apparent conflicting purposes, that is, keeping an impeccable record of the members' relevant transactions during the cartel's regular operation and as a time bomb under signs of defection or threats of whistleblowing.

Anonymity

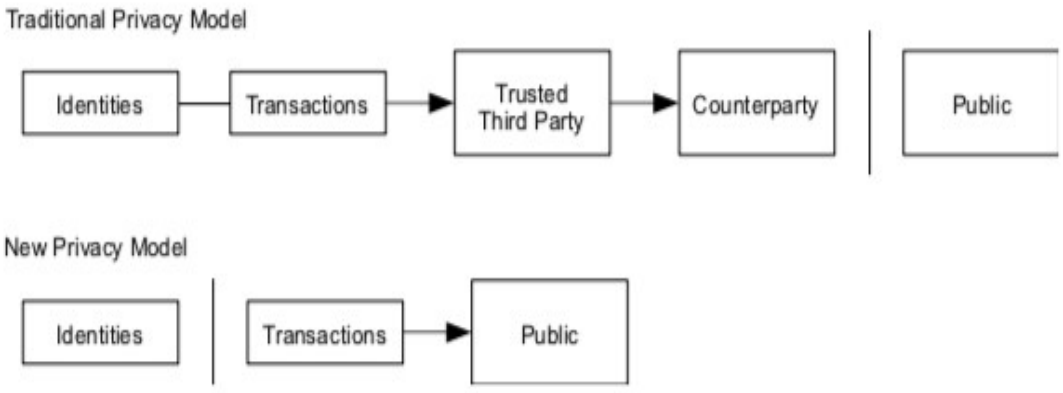
The financial system uses an intermediary -- the trusted central authority -- to check double spending in every single transaction[9]. The preservation of the intermediary is regarded as both costly and unreliable, as financial crises have taught us.

Instead of checking after each operation how dependable each business partner is, the most reliable system would be one where payees would know in advance the history of payments of each purchaser, choosing the partners according to the level of risk that the payee is open to take. Credit bureaus have been designed to accomplish said mission, but they too fall short of the quality information or information treatment that would offer complete and tailor-made data.

Because the solution to imperfect information is granting a complete and public record of the business operations, blockchain was created to allow that people check all information that the relevant partner shared on a platform built on top of it. In public blockchains, information is made available on public addresses created by hashing the public key. Even though it is not possible to reverse engineer a public key from the possession of public addresses, it is possible by design to get to public addresses by knowing someone's public key. The public key is the hashing or encrypted public interface of someone who has an account or a wallet in blockchain.

Blockchain was created under the belief that today's financial system's privacy model can be improved if transactions are made public but at the same time the identity of the involved parties is protected. Blockchain would not only increase transaction transparency, but also sustain the anonymity of the parties in each transaction.

[9] "After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent." (Nakamoto, 2008).



Nakamoto (2008)

Blockchain enhances anonymity by identifying each transaction party and each operation by means of cryptography -- the so called hashing functions. Blockchain creates hashing functions by means of asymmetric encryption using both the public and the private keys.

Each wallet has a private key -- that is supposed to be immutable and secret, accessible only by the wallet owner -- by means of which each transaction concerning one's wallet is authorized. Private keys generate public keys, that is how contracting and third parties can identify whom they are contracting with. Public keys are created by a derivation of the private keys and, unlike private keys, do not directly identify who is behind that wallet.

Public keys are made public in every transaction (transactions are identified by hashed public addresses): If, on the one hand, it protects the anonymity of those who need to supply or to be supplied without identification, it becomes possible for institutional players to offer more reliability over a transaction by publicly linking its name to a specific public account or public key. Nothing prevents that institution from keeping a separate shadow account with public keys that is not made public by the institution and that is used for other -- including illicit -- purposes.

Although it is possible to link all the operations to a public key -- that does not offer in itself clues as to who is behind those operations -, one can make it more difficult to track the history of transactions by linking each transaction to a unique address. In fact, for privacy purposes each blockchain transaction is by default linked to a unique address. Hence people whom one does business with can not see the other addresses that one owns.

In a sum, blockchain offers pairs of keys that do not identify who is on the other side of each operation and sequences of hashed public addresses that do not offer evidence of what is behind each specific transaction or fact of life. Blockchains anonymity is assured because neither is it possible to retrieve a public key from public addresses, nor derive the private key from public keys. In any case, the degree of anonymity can be attenuated by means of voluntary disclosure.

Traceability

Blockchain emerged as a technology that would improve our way to keep records of events by turning registers immutable. As a consequence, blockchain technology could be a source of either a perfect registry whereby cartelists would improve compliance and sanctioning inside a cartel or, conversely, of evidence that would provide public authorities with easier means to prove the existence of cartels and even helping them demand stronger evidence from defected firms on the line for leniency.

Bitcoin's introductory article[10] puts trust and traceability as a cornerstone to develop a new coin using a trustworthy technology that keeps records unchanged. According to the paper, the financial system suffers from "the inherent weaknesses of the trust based model." The answer to the imperfect system is to substitute "an electronic payment system based on cryptographic proof" for the unreliable financial intermediary.

At its very inception the technology aimed at providing an immutability solution to today's trust system. As argued by bitcoin's formulator, "[t]ransactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers." As a consequence, Satoshi Nakamoto built blockchain as a system that would deter reversibility not by designing a superior technology -- that would eventually and earlier than desirable be superseded by a new and more disruptive technology -, but by relying on the extreme deconcentration of the power to coin and act as a clearinghouse for financial operations. Quoting bitcoin's quasi-manifesto[11]:

[10] Nakamoto (2008).

[11] Nakamoto (2008).

> In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.
> [...] we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. [...] They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

To make it clearer, blockchain was never built as capable of delivering *per se* an immutable registry. Blockchain would only be a reliable means to prevent bitcoin double-spending if at the same time the incentives to become block miners or nodes were high enough to make the system be operational -- so that the operations would be validated in a timely manner -- and, despite the incentives, the nodes were atomized. If blockchain failed in any of those conditions, it would be either unoperational or unreliable. In the first case, it would fail because the means to achieve immutability were improper. In the latter, it would fail in its ends, insofar as concentration of power would still place us in the trust system that makes us all dependent upon the reputation of the financial intermediary or trusted central authority.

Due to its relationship with economic power, the second case is the one that matters for us in this paper.

Mutability

Blockchain is generally defined as a digital ledger. As such its main purpose is to serve as a more reliable register of facts of life. To serve that purpose, blockchain needs dependable immutability guarantees in such a way as to make fraud statistically meaningless.

Blockchain is not unitary, though. In other words, it is a technology on top of which diverse solutions apply. Because, as we saw, immutability in blockchain depends on both the existence of incentives to join the platforms as block validating nodes and the atomization of the power to validate the blocks, it is critical to understand how all the solutions developed

on top of blockchain can guarantee that both conditions are filled. The first step in that direction involves understanding the differences between public (or permissionless) and private (or permissioned) blockchains.

Public blockchain solutions rely on the atomization of miners to consolidate immutability. The atomizations is the natural consequence of open access.

> In most open blockchains, there is no guarding against bad actors and no access control, thanks in part to the original influence of the open source and cypherpunk movements. Applications may be added to the network without the approval or trust of others, allowing the blockchain to function as a platform layer. In practice, some public blockchains only permit a finite number of actions to be contained in a transaction, perhaps only allowing their users to send tokens among them. But most public blockchains do not impose such limitations. Transactions are generally secured by merely requiring new entries to include a proof of work.[12]

Conversely, private blockchains rely on the reputation of a central authority that has the power to restrict participation to a club of persons. Central to private blockchains' is the entity's ability to build a new governance that builds stronger reliance either on the immutability or on the resilience of the registries.

> Private blockchains are subdivided into two different categories. The first is called 'single entity blockchain.' As its name suggests, a single entity will set up the protocol and run the blockchain, while reading permission may be public or restricted to certain participants. The second is called 'consortium blockchain.' In such a blockchain, the consensus process is controlled by a pre-selected set of nodes.[13]

Last, there are semi-private blockchains. "Those blockchains are run by a single company that grants access to any qualified user."[14]

[12] Shrepel (2019 (b)).

[13] Shrepel (2019 (b)).

[14] Shrepel (2019 (b)).

Blockchain types	Public blockchain	Semi-Private blockchain	Private (single entitiy) Blockchain	Private (consortium) blockchain
Acess	No permission required	Qualified users via online approvals	Members only	Members only, who could b eco-founders
Typical implementation	As public blockchain application	One company launches and acquires users after	Via a private blockchain implementation	Via a private blockchain implementation
Innovation target	New business models	Supporting existing models or lauching new services	Supporting existing models or lauching new services	Supporting existing models or lauching new services
Blockchain governance	Public consensus	Controlled by a single owner	Controlled by a single owner	Equal weigt to all participants
Number of users	Millions (billions?)	Hundred of thousands	Dozen to few thousands	Dozens to few thousands

Shrepel 2019(b).

Regardless of its configuration, blockchain promises both unheard-of anonymity and traceability at the transaction level. Even though there has been no "big but" when it comes to protecting anonymity yet -- or else we would already know who Satoshi Nakamoto is by tracking his, her, or their account -, immutability has been a risk to be controlled from blockchain's inception. As we will see, although blockchain's immutability as a whole is not entirely dependable, the degree of mistrust grows reversely proportional to the levels of publicity[15].

The confirmation of blockchain's operations depends on different consensus rules. The most well known rule is the proof of work, whereby blocks are validated according to the ability of nodes' CPUs to do a specific

[15] "Second, the definition states that data on both private and public, permissioned and permissionless, ledgers is immutable. Despite the fact that it is unresolved whether different variations of blockchain technology give rise to immutable records, the statute explicitly treats public and private ledgers as if they have identical capabilities. Does the statute suggest that data on private blockchains should be treated as immutable, even if these ledgers have a much weaker claim to this property?" Walch (2017).

job: "incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits"[16]. The block can be changed, but it requires redoing the work. Again: Blocks are not immutable, but changing blocks requires higher CPU capacity to assure that competing nodes would not stand a chance in mining. The job becomes even more complicated as more blocks are chained in: "As later blocks are chained after it, the work to change the block would include redoing all the blocks after it."[17]

Poof of work was created as a means to avoid that economic power concentrated the decisions in the hands of a few. According to Nakamoto's article, "Proof-of-work is essentially one-CPU-one-vote." That notwithstanding, proof of work did not solve the market power issue. As claimed in Nakamoto's piece:

> [...] The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

In fact, the probability that an attack happens is not that low: It only depends on the concentration of the mining power. Clearly, the more blocks one needs to have changed, the harder it is to operate the change. Even dominant nodes would have a hard time trying to change two consecutive blocks before other nodes confirm one block only. But dynamics can change depending both on the unilateral dominance of a certain quasi-monopolist or in the existence of collusion between major nodes[18].

Mutability becomes a bigger threat as the nodes have incentives to collaborate with each other. As we better understand blockchain and how

[16] Nakamoto (2008).

[17] Nakamoto (2008).

[18] Professor Shrepel adds that: "Thanks to Bitcoin, this is currently the world's most used consensus mechanism. It has the advantage of allowing a relatively random distribution of block validation operations, which limits the risk of collusion, but suffers from the power it requires as well as scaling issues."

governance rules can be built to -- in a non transparent fashion and under specific conditions designed by the parties -- clear registries and hide past transactions, it becomes clearer that blockchain can become an effective ally to conspiracies in restraint of trade and lower the levels of cartel detection. It should be clear at this point that assured anonymity and malleable traceability altogether change the balance of blockchain in favor of cartel proliferation.

Governance

The way found by blockchain founder(s) to guarantee immutability was a governance rule. Nakamoto's instinct followed the logic that any corporate lawyer understands: Ultimately, the best way to keep a rule unaltered is by demanding unanimity. But because in an idealistically dispersed universe of block validators demanding unanimity was tantamount to blocking and insofar as some degree of flexibility is desirable from the perspective of market adaptability, majority quora or poison pills seemed more adequate to approve of changes that should happen only under exceptional circumstances.

In that sense, blockchain was originally formulated to work under a simple majority rule: Bitcoin -- the first use built over a blockchain platform -- demanded a 51 percent majority to confirm blocks of operations. Blockchain was also designed to an atomized market of miners. When votes are dispersed into a multitude of voters, reaching a majority demands large acceptance, which brings legitimacy to a decision that is no longer concentrated in those who have economic power. But, again, majority quora alone would not suffice: Validation, voting or mining power needed to be dispersed so as to guarantee the prevalence of honest nodes.

Blockchain was then built to work not only as a digital ledger, but as a distributed one, where new data is only added to the chain if it is approved by a majority of honest atomized miners. Votes in blockchain are not one-IP-one-vote[19], though. As mentioned earlier, the power to validate

[19] Professor Shrepel (2019(b) explains that "[...] some blockchains are already implementing new mechanisms on top of the consensus in order to create more sophisticated governances.For instance, Dash, a crypto-currency, uses a governance system that allows its users to vote if they hold tokens. Decred and Tezos are also crypto-currencies with more centralized governance systems. In fact, one of Tezos'

operations depends on computing power, a combination of the number of CPUs that one owns and the power of those machines used to mine. For professional miners, it is basically the number of CPUs that count[20].

Distribution of power aimed at diluting the chances of dishonest attacks to the system. Another key aspect of systems using blockchain lies in that miners or nodes -- or any other way that validators are called -- can vote to supersede existing blocks or even give birth to hard forks, where there are two, or more registries of the same timeline coexisting in different systems with different factfindinds. Hard forks can also be created to preserve information that would otherwise be deleted from the blockchain's registry.

The big "if" about bitcoin was precisely that is was built under the assumption that a proof of work consensus rule would survive under a dispersed basis of miners. As bitcoin and -- later on -- other over-the-top[21] services flourished under a more concentrated environment of miners, the real concern about bitcoin started being the precise problem blockchain was created to solve: The mutability of registries. As professor Shrepel[22] defines it, "[w]hoever controls the consensus — also known as the consensus mechanism — controls the governance of the blockchain". According to him23:

> As a result, fewer than 10 mining pools dominated Bitcoin in 2017. In fact, the 7 most powerful ones accounted for more than 85% of all transactions validated on the Bitcoin blockchain. This calls into question the proclaimed decentralized nature of Bitcoin because the owning of more than 51% of mining power is equivalent to a control of the blockchain.

main characteristics is its ability to amend its consensus when necessary. Further, more traditional systems such as "off-chain" and "sidechain" mechanisms are in development. The mechanism called BIP 9 already allows Bitcoin developers to probe miners about technical changes. By doing so, blockchains supplement the sole consensus mechanism (and create new opportunities for unilateral conduct)."

[20] "The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes." [Nakamoto, 2008]

[21] Running on top of blockchain.

[22] 2019(b).

[23] 2019(a).

As concentration of power takes place, registries can be altered, making it easier for the existence of hard forks and for the proliferation of 51 percent attacks[24].

Governance to conspire in restraint of trade

So far we have analyzed the odds of attacking public blockchains. That was a very important exercise to explain how blockchain consensus rule is actually frail and concentration exists both in public, quasi-public and private blockchains.

In the universe of collusion, however, mutability is an easier task that depicted in the preceding chapters. Mutability is facilitated because our main concern lies in the use of permissioned or private blockchains to share data and eventually conceal information if defection happens inside a conspiracy. In other words, collusion does not depend on the mutability of public blockchains: Instead, it can even be built on top of algorithms that rely on data coming from public blockchains, but the agreement will be better protected if data is shared and rules are set forth confined to private blockchains.

Intuitively, blockchain is used when parties do not trust each other and need evidence of a transaction or fact of time. It can also be used when the parties need evidence before third parties -- in which case blockchain is useful because the third party does not trust the members of the blockchain, regardless of how they feel between each other. The following table illustrates possible sets of options between public and private blockchains depending on the degree of trust:

[24] "As defined by Walch, "[a] 51 percent attack could occur if a party or colluding group controlled at least 51 percent of the computing power of the network, allowing them to determine what is recorded to the network's records, and potentially to revise the existing record."

Nodes v Nodes				
Users v Nodes		Know and trust	Know and do not trust	Do not know and do not trust
	Know and trust	Centralize (blockchain unnecessary)	Private	Public
	Know and do not trust	Public	Public/Private	Public
	Do not know and do not trust	Public	Public	Public

Arantes (2019). Free translation from Portuguese.

As one can identify from the board above, private blockchains can be recommended if the users know the nodes enough to be sure that they do not trust each other and will oversee each other's activities. Non-alignment is essential for third parties to believe that the nodes will not conspire to change the registries. That is true even if the users do not have reason to trust the nodes.

To better understand the statement, we pick up the example of a monopolist node. Because aligned nodes share common interests, they will work as if they were one entity or one economic group. And because whenever nodes behave as one sole entity or group they do not oversee and report misbehaviors of each other -- rather joining forces to deceive third parties -, they are not fit to be trusted as validators of private blockchains.

However, even when private blockchains are used to help transactions of nodes that do not trust each other, certain events can trigger alignment in the course of events between the nodes of small private

blockchains. When alignment happens, blockchain's pro-immutability argument does not apply[25].

Nakamoto's model was since its inception projected having in mind a possible attack of a corrupt against an honest chain of nodes. But according to him, "[n]odes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent."[26] Because Nakamoto was concerned with a public blockchain called bitcoin, he was not designing algorithms to prevent fraud inside private blockchains conceived of for dishonest purposes -- in which case all the nodes, or most of them (in the case of a cartel with a defected party) would be aligned to erase or adulterate the chain.

Immutability is not, then, an intrinsic characteristics of blockchain. Immutability, particularly in small permissioned networks, depends on the presence of miners -- voters, validators or nodes -- whose interests are not aligned. As mentioned by Gladstone Arantes[27], users or developers should only trust platforms whose nodes are not cooperative and therefore have no reason to be dishonest.

> Thus, it is to be expected that a large number of cases will fall into the Know/Do not trust column [....] (they know each other, but there is no mutual trust). At first, because the users do not trust the nodes, one would expect that the use of a public blockchain was necessary. But if users know that the nodes do not trust each other either, they may believe that a private blockchain is enough, since surveillance between nodes could guarantee their own trust. The best solution is only available on a case-by-case basis. [free translation from Portuguese]

When the nodes of private blockchains are aligned and cooperate in their self interest, then open platforms -- because we expect that they be

[25] One of the greatest problems lies in the diffused knowledge that blockchain cannot be altered. As Walch claims, "[t]he secret meaning of 'hard to change' does not seem to have reached the academics,consultants, thought leaders, and regulators who continue to state without qualification that blockchain technology creates immutable,permanent, unchangeable, indelible records."

[26] Nakamoto (2008).

[27] 2019.

less concentrated and that the chances that their nodes are cooperative be lower -- are the more appropriate environment to find trust.

Designing the cartel rules inside small private blockchains

In contracts between few entities, the immutability argument is stronger if all the involved need approve the changes in order to have them effective. That sounds like a good rule if the only purpose is to defend the parties against confidence attacks from outsiders or against each other.

Blockchain becomes complicated when people want transparency and immutability to be protected against fraud, but at the same time need opacity and mutability to be shielded against knowledge from third parties[28]. In other words, the contract must be immutable for the first group, but not in relation to the latter. Cartels can benefit from this design.

The use of blockchain's design to implement cartels strategy is not unheard-of. In fact, it has been reported by Nakamoto as cause to the 51 percent and the double spending attacks. The great difference here lies in the fact that, unlike public blockchains, the private ones can be built incorporating governance rules that aim at making it possible to do the block change that blockchain solutions usually regard as pernicious to their business models.

As claimed by professor Schrepel[29], "[a] blockchain's ability to implement anticompetitive strategies will vary depending on the governance system of the blockchain." In our understanding, cartels are prone to use private blockchains fundamentally as a hybrid tool that offers immutability and publicity to the nodes and at the same time supplies opacity and mutability as regards the outsider. For cartel purposes, the best rule is one designed to afford immutability as regards the operation of the cartel, but one than can also serve the purposes of the members of the cartel when one of them defects and collaborates with the authorities. Even though the OECD launched a paper a year before on blockchain[30] and challenges ahead,

---

[28] Professor Shrepel (2019 (a)) calls them " the '*visibility effect*' created by blockchain for the cartelist as well as the '*opacity effect*' created outside the collusive agreements."

[29] 2019 (b).

[30] OECD (2018).

Professor Shrepel (2019(a)) was the first to bring this possibility to our attention:

> As far as private blockchains are concerned, they may allow an on-demand exit from the agreement while ensuring the deletion of data. This is utterly attractive for potential colluders. More generally, considering the fact that the owner of a private blockchain retains the right to override, edit, and delete the entries on the blockchain, or even to modify the blockchain functioning itself, it cannot be used as intangible evidence to prove participation in collusion. [...] Nonetheless, by allowing the parties to delete their data and transactions, colluders may remain safe from detection. Only a copy of the data held by another colluder could potentially put them into great danger.

Usually, cartel members would not be able to detect defection before the dawn raid or -- even after they do -- easily detect who defected. That means that the anti-leniency rule in the smart contract would only apply in specific cases where a dawn raid starts and the parties must decide based on a pre established majority rule to erase the information. This is a very plausible scenario, as dawn raids take place in the premises of all the members of the cartel at the same time. The algorithms must then be designed to accommodate a smart rule giving more flexibility to erase the whole history in such cases.

There are many smart solutions that fit this context, including a specific quorum to change data when the cartel is working ordinarily -- unanimity would work in smaller groups, in order to assure immutability of the transactions and cartel surveillance -- and another to delete or to fork all data to another private blockchain where an independent third party elected by a quorum of the members of the cartel will be the only one to have access to the history of collusion. In the fork option, there must also be a specific command to erase all the data if defection is confirmed and the independent third party hears of cartel investigations regarding the members of that private blockchain.

Professor Shrepel[31] also brings to attention that smart contracts can automate sanctioning by automatically transferring tokens depending on the

[31] 2019 (a).

behavior of the cartelist. Smart contracts would also be able to automatically exclude those who infringe the law of the cartel[32].

Subverting the incentives to defect

Monetary sanctions can however be very detrimental to the opacity of the agreement. As can also be "printscreen", photo shooting and sharing of data from the defecting cartelist that precede the dawn raids. Because the dawn raid is usually the watershed that will trigger reaction from the members of the cartel, it is half correct to say that the cartel may only take the necessary measures when it is already too late and therefore blockchain may not increase underdeterrence as propagated.

That view is not correct because it fails to see half of the facts. Because with blockchain conspirators are subject to better enforcement of the cartel rules and because opacity of those rules is increased to the observer, the incentives to defect become minimal. In fact, the technology subverts today's incentives to blow the whistle.

Defection usually happens when there is fear that the cartel will be dismantled by public authorities (traditional leniency) or when someone has been caught for a cartel and wants to have the sanctions reduced by giving notice of another conspiracy (leniency plus). In any case, defection is either a consequence of fear that the cartel will be dismantled by public authorities -- which leads to a race to receive the lowest number in the marker system -- or the effect of past law enforcement. In both cases, the ultimate reason for defection is risk aversion to law enforcement.

As opacity escalates, the risk of law enforcement falls drastically. Lower risks of law enforcement and greater risks of sanctions inside the cartel shield the agreement against collaboration with authorities. At the same time, if law enforcement falls, the number of persons available to leniency plus agreements also drops.

[32] 2019 (a). "Smart contracts may be used to exit collusive agreements, whether it is to force the exclusion of a deviant colluder (**1**), or for a company to manage its own exit from it (**2**). These automated exits might be organized in accordance with several pre- established rules, ultimately leading to new challenges for antitrust and competition agencies."

That leads to the conclusion that even though blockchain and smart contracts build better solutions to preserve cartel member from the effects of defection and cartel settlements, that improvement is marginal as regards the amelioration of the governance of the cartel and a considerable fall in the risk of deterrence.

Final remarks

The findings of our work confirm professor Shrepel's[33] understanding that governance is the key aspect in designing cartels using blockchain technology. We confirm that the consensus rule can also be adjusted both to create trust in the information shared but also offer smart mechanisms to replace blocks of data or fork them in a way to protect the members against defection.

On top of that, we shed light on how a combination of mutability and immutability -- instead of immutability alone -- is the most relevant feature to turn blockchain into an unprecedented threat to fight cartels. In this sense, this paper complements professor Shrepel's observations on how blockchain can enhance opacity for outsiders and at the same time improve transparency for cartel members.

References

Connor. John M. Cartel Detection and Duration Worldwide. CPI Antitrust Chronicle. September 2011 (2).

Arantes, Gladstone (January 15, 2019). Entenda as Blockchains Públicas e Privadas. Infochain. Available on https://infochain.com.br/entenda-as-blockchains-publicas-e-privadas/. Accessed on July 16, 2019.

Connor, John. Global Price Fixing. Springer, 2007.

European Commission. Commission Staff Working Document accompanying the White Paper on Damages actions for breach of the

[33] 2019 (a) and 2019 (b).

EC antitrust rules. COM(2008) 165 final {SEC (2008) 404} {SEC (2008) 406}.

European Commission. Commission Staff Working Paper accompanying the White Paper on Damages actions for breach of the EC antitrust rules. COM(2008) 165 final {SEC (2008) 405} {SEC (2008) 406}.

Nakamoto. Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System (2008). Available on https://bitcoin.org/bitcoin.pdf.

OECD. Blockchain Technology and Competition Policy - Issues paper by the Secretariat. June 8, 2018.

OECD. Hard Core Cartels: Third report on the implementation of the 1998 Council Recommendation (2005). Available on https://www.oecd.org/daf/competition/cartels/35863307.pdf.

Østbye, Peder, Collusion Risk and Responsibility in Public Cryptocurrency Protocol Development (March 18, 2019). Available on https://ssrn.com/abstract=3354868 or http://dx.doi.org/10.2139/ssrn.3354868.

Shrepel, Thibault. Thibault Schrepel, Collusion by Blockchain and Smart Contracts, 33 HARV. J.L. & TECH. (2019).

Shrepel, Thibault. Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox. 3 GEO. L. TECH. REV. 281 (2019).

Understanding Bitcoin Traceability. Available on https://bitcoin.org/en/protect-your-privacy. Accessed on July 16, 2019.

Walch, Angela. The Path of the Blockchain Lexicon (and the Law), 36 REV. BANKING & FIN. L. 713, 713 (2017).