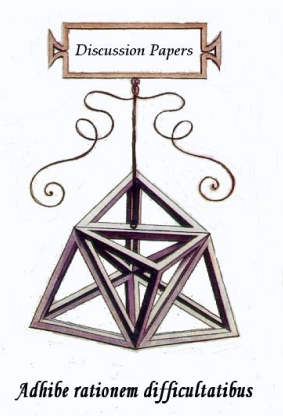
***Discussion Papers***
Collana di
E-papers del Dipartimento di Economia e Management – Università di Pisa




Massimiliano Vatiero

# Smart contracts and transaction costs

*Discussion Paper* n. 238
2018

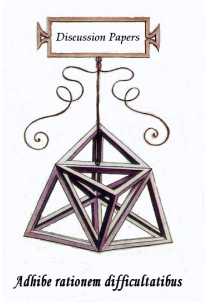
*Discussion Paper* n. 238, presentato: Ottobre **2018**

**Indirizzo dell'Autore**:
Massimiliano Vatiero
Dipartimento di Economia e Management, via Ridolfi 10, 56100 PISA – Italy
Email: massimiliano.vatiero@unipi.it



Si prega di citare così:
Vatiero M. (2018), "Smart contracts and transaction costs", Discussion Papers del Dipartimento di Economia e Management – Università di Pisa, n. 238 (http://www.ec.unipi.it/ricerca/discussion-papers.html).

*Discussion Paper*
n. 238




Massimiliano Vatiero

# Smart contracts and transaction costs

**Abstract**

Because of the enforcement based on the blockchain technology, smart contracts are supposed to allow contracting parties to conduct transactions more efficiently than traditional contracts. This paper challenges that claim. Because of the need for an efficiency-enhancing adaptation of institutions—a chief problem of transaction cost economics—traditional contracts may incur lower transaction costs than smart contracts.

**Keywords**: Blockchain, Smart contracts, Incomplete contracts, Transaction costs, Adaptation.

**JEL Codes**: D23, D86, L14, L86, O33.

I received exceptionally helpful comments from Alessandro De Chiara, Luca Enriques, Anne Lafarre, Maurizio Lisciandra, Ariel Porat, Marcello Puca, Hans-Bernd Schäfer, Jakub Szcserbowski as well as from participants at EALE 2018 (University of Milan-Bicocca), STILE 2018 (USI, Lugano), STOREP 2018 (University of Genoa) and the 2018 lecture series in "New Frontiers in Law and Economics" at Bucerius Law School (Hamburg). This paper benefitted from the generous financial support of the "Brenno Galli" Foundation. The usual disclaimers apply.

*We like all the things that we assume have no limits and, therefore, no end.*
*It's a way of escaping thoughts about death.*
*We like lists because we don't want to die.*
– Umberto Eco, Interview to Der Spiegel (11 November 2009)

*Lists range from simple checklists to complex databases,*
*but they all have one major drawback: we must trust their keepers. . . .*
*Now imagine a parallel universe in which lists have declared independence:*
*They maintain themselves.*
*This, broadly, is the promise of the "blockchain".*
– The Economist, "Disrupting the trust business" (15 July 2017)

## 1. Introduction

A somewhat neglected finding of Coase's (1937) pivotal work is that technology affects transaction costs.[1] It is no surprise, then, that some scholars have advanced the hypothesis that blockchain (hereinafter BC) technology, one of the most important innovations in today's world, could reshape the economic institutions of capitalism, to borrow the title of Oliver Williamson's (1985) celebrated book (cf. Davidson et al. 2016, 2018). In an BC each premise of transactions (e.g. the transfer of a certain amount of cryptocurrency from one party's digital wallet to another) is placed into a digital block, and once a consensus mechanism is applied, the block is placed into a perpetually growing chain of blocks—thus the term *block-chain*. Although scholarly interest in the subject is growing rapidly, however, to date an analysis of SCs from the perspective of transaction cost economics is severely lacking. This theoretical essay aims to fill that gap. In particular, this article addresses contractual agreements that exploit BC technology—namely, smart contracts (SCs)—through the lens of transaction cost economics.

For the threat of an *ex post* intervention of a third-party enforcer (e.g., court, arbiter), contracting parties are supposed to abide by their "traditional" contract. However, according to incomplete contract theory (e.g. Tirole 1999; Hart 2017), this external enforcement is costly and, therefore, there is a risk of *ex post* opportunistic renegotiation (the so-called "hold-up risk"), that diminishes contracting parties' incentives for specific investments and that can encourage them to abandon the contractual form and merge in order to conduct and enforce the transaction internally within a single firm. A further alternative is represented by the so-called relational contract. The enforcement in a relational contract is based on the fact that parties care about their reputation. The risk of losing their reputation and the threat of a stigma in a socio-economic "network" (for instance, in a given community) encourage parties to abide by agreements, even without the intervention of an external third party. For this reason, relational contracts are considered to be self-enforcing. The BC technology provides economic system with a fourth type of economic relationship, the SC (see the Table 1). An SC contains a series of promises made about some transaction, now and in the future, enforced by a BC. In an SC, the BC technology executes

[1] Coase (1937:397) contends that technological "[c]hanges like the telephone and the telegraph, which tend to reduce the cost of organising spatially, will tend to increase the size of the firm". To that, he adds that "most inventions will change both the cost of organising and the costs of using the price system. In such cases, whether the invention tends to make firms larger or smaller will depend on the relative effect of these two sets of costs. For instance, if the telephone reduces the costs of using the price mechanism more than it reduces the costs of organising, then it will have the effect of reducing the size of the firm" (Coase 1937:397, fn. 3).

automatically (i.e., without any external enforcing party) the transaction in line with what contracting parties have agreed upon *ex ante*. Because the BC protocol equates the enforcement with the execution, collapsing these two concepts, the BC technology begets SCs' hallmark ability to enforce themselves.

Hence, while traditional contract relies on the threat of an *ex post* intervention of a third-party enforcer, the main feature of relational contracts and SCs is that both are self-executing (namely, there is not the need for an external enforcement). The main difference between the self-enforcement in a relational contract and the one as conceived in an SC is that the former, but not the latter, relies on the identity of economic actors. Indeed, the reputation mechanism in a relational contract is based on the possibility that the socio-economic network penalises a certain identifiable economic actor for her or his deviating conducts. Instead, parties in an SC may and do use pseudonyms which are very hard to identify or associate with certain conducts. In addition, by construction, each actor in a BC can not deviate from the contracted agreement. Thus, a reputation-based mechanism of enforcement might not emerge or not work well in an SC scenario. Indeed, the BC network—and not the socio-economic network as relational contracts—works as *the* enforcement device in an SC.

| **Type of economic relationships** | **Enforcer** |
|---|---|
| Single firm (as result of M&A) | Internal authority |
| Traditional contract | A third trusted party (e.g. a court) |
| Relational contract | The socio-economic "network" |
| Smart contract | The blockchain network |

Table 1. Enforcing economic transactions

Because BC protocol seems to eliminate the need for and the costs of external enforcement, SCs are sold as able to solve the problem of opportunism which characterizes traditional contracts (cf. Wright and De Filippi 2015; Catalini and Gans 2018; Davidson et al. 2016, 2018) and naïve conceptualisations of SCs imagine a future in which economic transactions occur without any external legal enforcement or intermediary whatsoever.[2] However, the claim that SCs allow transactions to be conducted more efficiently than traditional contracts underestimates a central problem and exercise of transaction cost economics: the need for an efficient adaptive mechanism.[3] To quote Williamson (1973:318, italics added), "[I]nasmuch as a full set of contingent claim markets is infeasible (by reason of bounded rationality), *adaptive*, sequential decision-making procedures need be devised". Williamson (1979:241, italics added) later elaborated, "Intertemporal efficiency . . . requires that *adaptations* to changing market circumstances be made".[4] Transaction cost economics is focussed on ex-post inefficiencies (e.g. Williamson 2002), especially the ones stemming from the poor or bad adaptation in the contractual

[2] The range of possibilities derived from the basic idea of SCs has sparked significant discussion about how SCs could be used, as Swanson's (2014) broad list of actual and potential SCs shows. Nevertheless, the power of SCs is limited to transactions that can be controlled by a BC. For instance, an SC can neither force the service supplier to perform nor enforce the physical delivery of a purchased good to a consumer.

[3] Williamson (2010:9, italics added) stresses that transaction cost economics "has been an *exercise* in *adaptive*, intertemporal economic organization from the outset (Williamson 1971, 1975, 1985, 1991)."

[4] A similar claim regards efficient breach theory. Because a contract that seemed sweet when agreed upon may sour in the interval prior to its performance, a breach of contractual promises may be excusable (Shavell 2009; Bigoni et al. 2014).

execution.[5] An efficient contractual arrangement has to minimise the need for costly external enforcement as well as ensure adaptation to mutable and unpredictable *ex post* occurrences.

In this paper, the adaptation criterion does not concern the option for parties to postpone decisions on the progress of their contractual relationship in order to gain from information obtained subsequently, namely the case of a "self-adaptation". This option is theoretically and technologically possible both in the case of SCs and traditional contracts. For SCs, although they afford no room for second thoughts because all parties' responsibilities and obligations are coded *ex ante* (and executed with certainty *ex post*), the parties potentially may have incorporated a comprehensive contractual clause *ex ante* to halt that programme's execution. Similarly, in a traditional contract, parties who cannot construct bespoke contracts may prefer to avoid litigation and resolve contract disputes informally only *ex post*, for example, when contingencies occur. Instead, I consider a different criterion for comparing costs of transaction in a traditional contract with the same transaction in an SC: the *ex post* "external" adaptation of the agreement. With external adaptation I refer to the *ex post* intervention of a third party (typically a judge) for adapting, to some extent, the contractual relationship to new unexpected contingencies. Unlike traditional contracts, SCs are constructed to avoid such an external adaptation. Hence, although SCs reduce uncertainty in economic relationships, they also preclude any *ex post* efficiency-enhancing adaptation of contractual terms by an external third party. As I explain in this paper, the trade-off between *ex ante* precision, on the one hand, and external adaptation, on the other, can determine transaction costs *stricto sensu*.

A second central characteristic of BC platforms is that they are built on consensus mechanisms—the so-called "proof of work" is currently the most popular mechanism. Validated transactions have to have received the consent of the network. According to proof of work, the validation of a BC rests on a vote *with* central processing unit (CPU) power, which poses the risk that a user or a coalition of users with sufficient CPU power might distort the development of BCs and SCs.[6] Such a risk has become increasingly threatening as BC networks shift from the community at large to fewer and fewer hands that currently dominate several popular BCs. By using consensus mechanisms, BCs and SCs thus entail the risk that their development caters to the preferences of the majority and potentially against the interests of minorities. From the perspective of transaction cost politics (Olson 1982; North 1990; Dixit 1996; cf. also Vatiero 2018), consensus mechanisms could determine rules for SCs that are aligned with the majority's preferences but are nevertheless inefficient, unreliable and unpredictable. That dynamic would increase transaction costs *lato sensu*.

Hence, my paper deals with two central aspects of BC technology that are related to the (in)flexibility feature of SCs: the self-execution and the consensus mechanism (see Table 2). For their self-execution features, compared to traditional contracts, SCs pose a first disadvantage related to the inflexibility to *ex post* external adaptation. What is defined *ex ante* by parties (specifically parties' conducts, responsibilities and obligations, but also contractual clause to halt or not the execution) in an SC will be self-executed *ex post*, without any external intervention. Although there are relevant benefits from such an inflexible setting (especially, there is no risk of an *ex post* opportunistic renegotiation), there are costs due to a lack of external adaptation to new unexpected contingencies. Second, the consensus mechanism allows a degree of flexibility of the BC that could produce benefits, e.g. to update the BC to new needs of the network. However, the

[5] This is a central theme also for theory of the firm (e.g. Simon 1951; cf. Gibbons 2005) as well as for recent contributions of the property-rights theory *à la* Grossman-Hart-Moore—Moore (2016:12) has argued that "Hold-up is important, but looking around the world, it seems that ex-post inefficiencies are even more important" (see also Nicita and Vatiero 2014).

[6] In a similar vein, in July 2014, the European Banking Authority (2015:5) published a report highlighting those same concerns with virtual currencies (VCs): "The risks include the fact that a VC scheme can be created, and then its function subsequently changed, by anyone, and in the case of decentralised schemes, such as Bitcoin's, by anyone with a sufficient share of computational power".

*logic* of (majoritarian) groups may create a mal-adaptation of the BC. In particular, the consensus mechanism might create or increase the uncertainty of the institutional setting, disincentivise investments in contractual relationships and, therefore, raise transaction costs.

The tasks attempted in this essay are essentially twofold. First, for their self-executing features, I describe the costs due to a lack of external adaptation of SCs. Second, I deal with costs of mal-adaptation which comes from consensus mechanisms. From the perspective of transaction cost economics, I ultimately contend that though SCs reduce several transaction costs related to opportunistic renegotiations *à la* Williamson, they can also create or increase other costs related to poor or mal-adaptation of SCs.

| | | Transaction costs | |
|---|---|---|---|
| | Flexibility | Decrease | Increase |
| Self-executing features | NO, the BC prevents any deviation from what contracting parties have agreed upon *ex ante* | BC avoids any opportunistic renegotiation | BC prevents also efficiency-enhancing adaptations<br>**Costs due to a lack of external adaptation** |
| Consensus mechanism | YES, it provides the BC with a (limited) degree of flexibility | Users can adapt the BC and SCs to needs of the network | Olsonian groups' logic<br>**Costs for mal-adaptation** |

Table 2. (In-)Flexibility and adaptation of SCs

In what follows, I first review literature on SCs and BC technology that takes the perspective of transaction cost economics, generally defined, in the next Section. In Section 3, I describe the major characteristics of BC technology and SCs.[7] In Section 4, I illustrate the transaction costs of the inflexibility of SCs. After dealing with the transaction costs of consensus mechanisms in Section 5, I offer some concluding remarks in Section 6.

## 2. The state of art

This essay complements several recent papers. In one, Catalini and Gans (2018) have discussed the virtues of BC, including the reduction of information and networking costs. Although I acknowledge that, with BC, those costs can approach zero for many types of transactions, this essay focusses on other types of costs related to adaptation that BC technology and SCs can increase beyond those posed by traditional contracts. This essay additionally relates to the work of Holden and Malani (2018), who have argued that SCs can overcome some hurdles to credible commitments posed by traditional contracts. Their argument rests on several assumptions, however. One is that contracting parties have enough information to write an appropriate

[7] Because BC technology and SCs are exceedingly complex—there are different BCs, different SCs and different ways in which an SC relates to its underlying BC—I seek to present only their major characteristics and structures without digressing into technological minutiae. For an excellent introduction to those themes from an institutionalist perspective, see Werbach and Cornell (2017), Yermack (2017), De Filippi and Wright (2018) and Werbach (2018).

mechanism to allow an efficient self-adaptation of the SC. Another is that BCs are supposed to be objective, neutral devices. In this essay, I question both of those assumptions. First, considering bounded rationality as standard transaction cost economics does, the amount of information accessible to and exploitable by individuals is not adequate to devise an appropriate mechanism for adapting the design of an SC *ex ante*. Or, if available, then such a mechanism would be too costly and complex to be devised. Second, as I explain in this essay, the consensus mechanism could prompt the creation and persistence of interest groups that are liable to endanger the neutrality of the BC.

In another paper, Arruñada (2018) has described numerous difficulties of BC technology and SCs in providing a secure, effective alternative system for property rights. This essay, however, remains distinct from Arruñada's (2018) in both its subject matter and approach. Whereas Arruñada (2018) examined the problems of a BC-based system concerning the transfer of property rights, I examine costs related to the adaptation of SCs. Moreover, whereas I apply an incomplete contract approach to investigate SCs, Arruñada (2018) conducted an economic analysis of property rights.

This essay also relates to Arruñada and Garicano's (2018) work, which examines, among other things, a particular procedure based on a consensus mechanism that splits a BC into two BCs—the so-called "hard fork". Because a hard fork produces two BCs, each with a different set of rules, Arruñada and Garicano (2018) have advanced the hypothesis that the market will determine the best BC. For that reason, a hard fork can afford a means for the efficient adaptation of BCs and SCs.[8] In another work, Biais et al. (2018) have discussed consensus mechanisms in terms of how the decentralisation exposes BCs to coordination failures and externalities. My analysis differs from Arruñada and Garicano's (2018), as well as from Biais et al.'s (2018), insofar as I take the perspective of political transaction costs. From that perspective, in a world with incomplete contracts, agents can affect rules via consensus or political mechanisms.[9] Accordingly, each democratic process is liable to favour some or all components of the dominant coalition but disregard the interests of minorities. In that respect, the hard fork, which is a democratic mechanism within BC technology, can serve the interests of groups with the power to devise new rules (e.g. the majority of CPU power), even ones against minorities. As a result, the forking process can produce uncertainty about rules for contracting parties and increase the transaction costs of SCs *lato sensu* that neither Arruñada and Garicano (2018) nor Biais et al. (2018) have discussed.

Concerning the governance of BCs, my paper complements the work of Yermack (2017), who has discussed the potential implications of BC technology for corporate governance. He identifies benefits, especially greater transparency, which can have a positive impact on shareholders, investors, managers and other corporate actors, and several costs, especially ones related to the internal governance of BCs themselves. This paper differs from Yermack's (2017) by focussing on SCs and adopting the perspective of transaction cost politics to investigate problems related to the internal governance of BCs.

I do not, however, discuss a few other important aspects of SCs and transaction costs. First, I do not examine other types of transaction costs that might stem from SCs. One such cost is the cost of energy. In fact, as of January 2018, the electricity consumed for Bitcoin's BC roughly equalled the electricity consumption of more than 3,400,000 U.S. households (Biais et al. 2018). However, as Catalini and Gans (2018) have pointed out, such a massive energy requirement is small if compared to the costs of labour and capital involved in securing transactions in traditional ways. Second, I do not discuss hacking incidents or their potential to reduce the reliability of contractual

[8] A similar claim appears in Arruñada (2018:74–75).

[9] In other words, "if rents are not perfectly allocated ex ante by contracts and rules, there is ample space for economic actors to exert pressure on the regulatory, judiciary, and political system to grab a larger share of these rents" (Zingales 2017:119).

enforcement embedded in SCs. BC technology is not entirely infallible, as several such incidents (e.g. at The DAO and Mt. Gox) have shown (cf. Arruñada 2018; Werbach 2018),[10] and its shortcomings have required resorting to traditional legal enforcement tools. For instance, in response to crippling theft at Mt. Gox, the exchange suspended trading, closed its service, filed for bankruptcy protection from creditors in Japan and the United States and began traditional liquidation proceedings. SCs can likely benefit more from interacting with the law than by attempting to replicate a parallel system of their own (cf. Evans 2014; Werbach and Cornell 2017; Arruñada 2018; Werbach 2018). That issue, however, should be the topic of a separate paper.[11] Last, I do not focus on *smart property*, defined as "property whose ownership is controlled via smart contracts" (Swanson 2014:11),[12] a topic on which Arruñada (2018) has focussed in considerable depth. In work related to that topic, Werbach and Cornell (2017) have sought to clarify whether SCs are truly contracts in the legal sense.

## 3. In the blockchain protocol we trust

For markets to thrive, participants need to be able to verify and audit the attributes of transactions, including the characteristics of the goods exchanged. The traditional paradigm relies on ledgers often held by trusted intermediaries in order to create a reliable environment. Familiar traditional ledgers are used for double-entry bookkeeping, in real estate markets (e.g. land title registries) and to track the registration and assignment of rights in the domain of copyright, among other purposes. However, those traditional ledgers pose several costs. First, for their services, intermediaries might charge fees. Second, as Casalini and Gans (2018) have observed, those intermediaries might attain substantial market power that could determine consequences such as higher fees, switching costs and reduced innovation. Last, the system of the traditional ledger could expose users to the malfeasance of the intermediaries, as countless examples of corrupt behaviour attributed to banks and regulators show.[13]

On the contrary, a BC is a ledger distributed among users of a network around the world. For instance, Bitcoin's BC is currently stored on more than 6,000 computers in 89 jurisdictions (De Filippi and Wright 2018:213, fn. 8). Every participant of a BC has access to the entire database, as well as to its complete history, and keeps a replica of the digital ledger. Participants' computers periodically synchronise to ensure that all of them share the same database. Because no central clearinghouse exists, BC technology is supposed to reduce or nullify the role of intermediaries and, moreover, their potential abuses. Indeed, no single party controls a BC, and every party can verify the records of transaction partners. Accordingly, whereas the traditional view has held that a third party is necessary to enforce contracts, BC technology works as an enforcement device for SCs and allows P2P-based transactions to occur safely.

[10] On 17 June 2016, roughly $50 million was diverted from The DAO's BC-based venture capital fund during a hacking breach. A similar incident occurred at Mt. Gox, a bitcoin exchange based in Japan that handled more than 70% of all bitcoin transactions worldwide until 2014, when someone stole a sum of bitcoin valued at $450 million.

[11] Because SCs are necessarily conducted in the shadow of the law, including but not limited to contract law (cf. Werbach and Cornell 2017), they are not self-driving cars. Casey and Niblett (2016) have demonstrated, however, that predictive capabilities created by big data and artificial intelligence in the future could allow parties to draft contracts that fill their gaps and interpret their unique standards without adjudication.

[12] In the framework of smart property, *property* refers to exclusive knowledge or possession of a private password (i.e. a digital key) able to link a new block to preceding ones in the BC (cf. Swanson 2014). For example, a bitcoin is not a physical or even digital object but the ability, by virtue of possessing the digital key of a given schema, to cause a change in the BC by, for instance, transferring cryptocurrencies from one digital wallet to another (Swanson 2014).

[13] A list of recent scandals is in Yermack (2017:8, fn. 2).

Although debate about the definition of SCs persists (cf. Werbach and Cornell 2017), an SC is arguably "an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger" (Brown 2015). In a similar vein, the inventor of SCs, Nick Szabo, has described them as follows:

> The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as *to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher*. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble *vending machine*. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a beginner's level problem in design with finite automata, dispense change and product fairly. (Szabo 1997, italics added)

In short, a BC can be programmed likewise a vending machine; if someone inserts a coin, then he or she automatically receives a can of soda.[14] Each SC contains a set of rules that triggers automatic, predefined responses corresponding to particular contingencies in computational if–then logic.

In addition, BC protocol is built upon consensus. Each variation of the BC requires the consensus of the users, not of an external third party as with a classical ledger. Although several consensus mechanisms are used in BC-based platforms, the one deployed most often is the proof-of-work system. In proof of work, all of the computers in the network tasked with validating transactions and maintaining the security of the BC (the so-called miners) work to solve a mathematical puzzle. That puzzle is straightforward for a computer but extremely repetitive and therefore computationally expensive. Computers compete to find the solution to the puzzle, and the computer that finds the answer first—that is, proof that they have done the necessary work—is allowed to add a new block of transactions to the BC. That computer is also rewarded, typically with cryptocurrency. According to Bitcoin's pseudonymous creator, Satoshi Nakamoto, with proof of work people "*vote with their CPU power*, expressing their acceptance of the valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them" (Nakamoto 2008:8, italics added). Thus, the valid BC is the result of the miners' vote with their CPU power.[15]

The consensus mechanism does not involve only the validation process—users of BC vote for adding new digital blocks—but also the hard fork process—users of BC vote for changing (the chain of) past digital blocks. The hard fork is a particular but not uncommon procedure based on a consensus mechanism that splits a BC into two BCs.[16] In a hard fork, the original BC continues to operate under its original set of rules, whereas the new BC, stemming from the block at which the hard fork was implemented, operates under a different set of rules. Consider the Ethereum hard fork experienced in the summer of 2016. Following the hack of The DAO, members of the Ethereum community suggested rolling back the BC in order to cancel the transactions that

[14] However, the idea of a SC as a vending machine may hardly identify the core feature of SCs: their use of BC technology. As Savelyev (2017) has noted, there are well-known contractual constructs implementing automated performance; for instance, foreign exchange markets trades are frequently executed by a computer system. In addition, there are old examples of vending machines: The earliest known reference to a vending machine is in the work of Hero of Alexandria, a first-century AD Greek engineer and mathematician (Savelyev 2017). The difference of SCs from previous examples is that SCs rely on BC technology.

[15] Proof of stake is a different way to validate transactions. Unlike with proof of work, in which users pay in the form of CPU power, in proof of stake the validator of a new block depends on the wealth of his or her digital wallet, or what is called a *stake*. As a result, the valid BC in the proof-of-stake system is the outcome of the vote with the stake—namely, the ownership of cryptocurrency. Although other consensus mechanisms exist, including proof of value (see Davidson et al. 2017) and proof of authority (see https://poa.network), their use remains very limited.

[16] Hard forks are not uncommon. Bitcoin underwent two hard forks in the summer and fall of 2017, respectively. The first stemmed from the size of blocks that could be mined on the BC and involved the split of the original Bitcoin BC into two branches, with two different cryptocurrencies: Bitcoin and Bitcoin Cash. The second fork, Bitcoin Gold, has relied on a different proof-of-work algorithm than Bitcoin does.

diverted the fund's money. Ethereum split into two incompatible "worlds": one in which The DAO, along with all of the consequences of the hack, still exists (i.e. Ethereum Classic) and another in which The DAO never happened and in which blocks of The DAO hacking incident were removed (i.e. Ethereum). Both worlds continue to survive. The hard fork process, according to Arruñada and Garicano (2018), is a means of users to meet and adapt the BC to new their needs.

In sum, because BC technology prevents renegotiations *à la* Williamson due to its self-executing feature, as well as prohibits the malfeasance of third parties and external intermediaries due to its decentralised and disintermediated nature, SCs use the BC as a "trust machine" (*The Economist* 2015; Werbach 2018) that creates a reliable environment among people who have no particular confidence in each other. With an SC, trust in external enforcement that characterizes a traditional contract is therefore replaced with trust in the BC protocol.

## 4. Transaction costs due to a lack of external adaptation

The inflexible nature of a BC poses particular implications for contractual agreements. After all, for investment in a contractual relationship to thrive, clauses agreed upon should be stable and resistant to renegotiations *à la* Williamson. The common colloquialism "set in stone" can be used to explain that prominent requisite for good contracts and, more generally, for rules in a community.[17] In that analogy, the BC represents the stone for SCs.

For they react only according to predefined code, SC are inflexible. However, for their inflexibility, SCs prevent also *ex post* external adaptation and, therefore, transaction costs may emerge or increase. The following (incomplete) list presents several advantages of an external adaptation which are, nevertheless, precluded in an SC.

- When a traditional contract is breached, an external enforcer might issue one or more of multiple remedies, including rescission, specific performance and, more commonly, damages. Legal remedies represent a means of allowing an external party's *ex post* intervention to adapt, to some extent, a contract. Because SCs, by contrast, are supposed to be conclusive, they cannot allow such an *ex post* legal intervention.[18]
- A further way for adapting the agreement is via the judge's interpretation. That interpretation is not a mere academic exercise but a means to establish the exact scope of the parties' obligations and the outcome to be achieved under the contract. By interpretation, the external enforcer has a degree of flexibility for adapting *ex post* the contractual clauses. However, the interpretation of traditional contracts is performed by judges *after* that a dispute has arisen and not *before* the transaction in order to be included in an SC.
- In addition, it is not possible to translate into computer code and therefore include in an SC several important legal concepts that lack of a binary nature, such as force majeure, material breach and good faith, but that give traditional contracts adaptability that parties tend to desire when so many contingencies cannot be defined *ex ante* (cf. Sklaroff 2017).

[17] Unsurprisingly, in the Judeo–Christian tradition, the Ten Commandments were written on stone tablets by God and handed down to Moses on Mount Sinai. Similarly unsurprising is that the Babylonian Code of Hammurabi, dated roughly 1772 BC and consisting of 282 laws, including the famous "eye for an eye" (*lex talionis*), was etched in stone.

[18] As Werbach and Cornell (2017:376) have noted, legal intervention in SCs will concern only the claim of restitution: "Rather than complaining parties seeking fulfillment of alleged promissory obligations, complaining parties will seek to undo or reverse completed transactions. Litigation will persist, but it will shift from claims of breach, to claims of restitution".

Moreover, traditional contracts enable parties to use generally-defined contractual terms (e.g., trade standard or reasonable care) without requiring complete knowledge of what might happen in the future or costly bargaining among parties for that definition. However, these generally-defined contractual terms can not be translated in the binary computer code of SCs (see also De Filippi and Wright 2018) and, therefore, SCs might bring about high transaction costs.

- Finally, there are cases in which the intervention of an external party is the only way to achieve efficiency. For instance, in the cases of mistakes mutual to all parties, fraud and unconscionable terms, a court may order a modification of a traditional contract even over the objections of all parties. Even if these cases are of particular interest to SCs—the risks of error, fraud or unconscionability are high in SCs if computer code is a quite unknown language to people, SCs by construction do not allow such an *ex post* adaptive intervention of a third party.

In these cases, the BC-based enforcement of SC impedes the external adaptation of the agreement. In SCs, therefore, gains in *ex ante* precision impedes gains in *ex post* external adaptation, especially in long-term contractual relations in which the potential for a change in circumstances is particularly high. As a result, even if it reduces uncertainty in economic relationships, the self-executing feature of SCs also precludes *ex post* efficiency-enhancing adaptation of contractual terms by an external third party and therefore produces transaction costs *stricto sensu*.

## 5. Transaction costs for mal-adaptation

For its decentralized nature, at the heart of a BC there is the consensus mechanism. The most-used consensus mechanism is proof of work, which is based on the democratic principle that the majority rules. To validate transactions, a miner has to dedicate CPU power to verify transactions and rapidly search through potential solutions to solve the mathematical puzzle associated with each block in order to obtain the reward. In doing so, miners *vote with their CPU power*, to use the terminology of Nakamoto (2008). Such a system supposes that miners have an incentive to act purely out of self-interest and, in the process, fulfil a socially beneficial role.

However, an increasing concern with BC networks using proof-of-work systems is the risk of centralisation.[19] Amid the growing popularity of BCs, the difficulty of the validation process has spiked and thus decreased the probability that an individual using an everyday computer will mine a block. Due to that dynamic, miners seeking to validate transactions have organised themselves into so-called "mining pools" in which they combine their computational resources and deploy specialised hardware to mine new blocks and share rewards. In other words, because rewards are distributed at infrequent, random intervals, miners, which can be conceived as risk-adverse agents, behave strategically and form mining pools in order to decrease the variance of their income rate (cf. Eyal and Sirer 2014). Empirical evidence shows that such a centralisation of BCs does occur (cf. also Yermack 2017). As of August 2018, four mining pools controlled 55% of Bitcoin's network (BTC.com: 17%, SlushPool: 15%, AntPool: 13%, BTC.TOP: 11%; cf. https://www.blockchain.com/it/pool), and five mining pools controlled more than roughly 80% of the Ethereum BC (Ethermine: 28%, SparkPool: 17%, F2Pool: 14%, Nanopool: 11%, MiningPoolHub_1: 9%; cf. https://etherscan.io/stat/miner?range=7&blocktype=blocks). The chief

[19] Using a game theory model, Dimitri (2017) has argued that there is a risk of centralisation but not monopolisation. The incentive structure prevents the emergence of a monopoly in the mining activity, for it always remains profitable for the miner with the second-lowest operating costs to mine.

threat is that a group with sufficient CPU power may prohibit certain transactions (see also De Filippi and Wright 2018). In addition, BCs often rely heavily on the existence of a leader—for instance, their founders, as is the case with Ethereum and its founder Vitalik Buterin—and such a potentially biased environment could discourage parties' incentive to invest in an SC.

The risk, investigated at length in the context of economic institutions relates to Mancur Olson's (1965) hypothesis that subgroups (e.g. mining pools) may exploit larger groups (e.g. BC networks). At stake in that dynamic is the loss of social welfare (Olson 1965, 1982). To my knowledge, all such pools have been benign and followed the BC protocol. Nevertheless, several theoretical circumstances are possible in which those benign strategies would not be Nash equilibria for mining pools (cf. Eyal and Sirer 2014; Bonneau et al. 2015; and Biais et al. 2018). The risk, even if only potential, that mining pools may behave opportunistically can distort the choices of parties to SCs and therefore create transaction costs *lato sensu*.

The hard fork process is another source of transaction costs. In the abovementioned hard fork of Ethereum for the hack of The DAO, a majority of members of the Ethereum community voted for cancelling the transactions that diverted the fund's money, while roughly 15% of the network's members refused to alter the BC and rejected the hard fork. Therefore, Ethereum split into two BC, Ethereum and Ethereum Classic which still work today. As Yermack (2017: 28, italics added) has lucidly commented, that fork

> accomplished two things that were supposed to be impossible on a public blockchain: *rewriting the history of transactions,* and *introducing human intervention to negate the unanticipated consequences of a self-executing smart contract*. Implicitly, the event raised the possibility of future interventions into Bitcoin and other blockchains, even open ones, if a majority of the constituents wished to nullify a set of adverse economic outcomes after the fact. A minority of 15% of the Ethereum miners saw this precedent as dangerous and opposed the hard fork, creating a schism in Ethereum when they continued to mine and process transactions on the legacy blockchain.

Hence, because they can change rules of a BC and, in turn, the institutional setting of SCs, hard forks create uncertainty for parties to SCs—for instance, because each hard fork alters the value of the cryptocurrency upon which the SC is established (cf. Thompson 2017). More generally, when mining pools dominate a BC, again following Olson's (1965) *Logic of Collective Action*, a hard fork can define rules that favour the majority, that are subject to change along with the majority and that are thus inefficient, unreliable and unpredictable. Due to uncertainty and distorted incentives for group logic, hard forks thus are able to produce transaction costs that are absent with traditional contracts.

## 6. Concluding remarks

According to a naïve view, given their decentralized and disintermediated nature, SCs are supposed to work better in terms of transaction costs than traditional contracts. Because SCs equate enforcement with the execution of the agreement, SCs reduce several transaction costs related to *ex post* contractual opportunism. Unlike traditional contracts, in which the parties can decide whether to fulfil their obligations or not, the latter at the risk of being held liable by an external enforcer, SCs cannot be breached. Because an SC codifies parties' responsibilities and obligations *ex ante* and executes them with certainty *ex post*, SCs afford no room for second thoughts. However, this is not always a desirable result. Indeed, my counterargument takes into account a central theme of transaction cost economics: the need for an efficiency-enhancing adaptive mechanism. The lack of external adaptive mechanisms represents the chief drawback of SCs. In addition, for consensus mechanism used in a BC, which allows a degree of flexibility of

smart contracting, SCs have further costs due to a opportunistic, uncertain, majority-driven adaptation.

As a result, despite several clear benefits of SCs, when adaptation matters, they incur more transaction costs than traditional contracts.

**References**


Arruñada B. (2018), "Blockchain's struggle to deliver impersonal change," *Minnesota Journal of Law, Science & Technology*, 19:55-105.

Arruñada B. and L. Garicano (2018), "Blockchain: The birth of decentralized governance," *Economic working paper series*, n. 1608, Universitat Pompeu Fabra.

Biais B., C. Bisière, M. Bouvard, and C. Casamatta (2018), "The blockchain folk theorem," Tolouse School of Economics working paper, n. 17-817.

Bigoni M., S. Bortolotti, F. Parisi, and A. Porat (2014), "Unbundling efficient breach," *Coase-Sandor Institute for Law & Economics Working Paper*, No. 695.

Bonneau J., A. Miller, J. Clark, A. Narayanan, J.A. Kroll, E.W. Felten (2015), "SoK: Research perspectives and challenges for bitcoin and cryptocurrencies," *2015 IEEE Symposium on Security and Privacy*.

Brown R.G. (2015), "A simple model for smart contracts," available at https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/ (last access: August 06, 2018).

Casey A.J. and A. Niblett (2016), "Self-Driving Contracts," *University of Toronto Law Journal*, 66: 429-442.

Catalini C. and J.S. Gans (2018), "Some simple economics of the blockchain," *NBER working paper*, No 22952.

Coase R.H. (1937), "The nature of the firm, *Economica*, 4(16):386-405.

Davidson S., P. De Filippi, and J. Potts (2016), "Disrupting governance: The new institutional economics of distributed ledger technology," mimeo.

Davidson S., P. De Filippi, and J. Potts (2018), "Blockchains and the economic institutions of capitalism," *Journal of Institutional Economics*, 14(4):639-658.

De Filippi P. and A. Wright (2018), *Blockchain and the law: The rule of code*, Cambridge: Harvard University Press.

Dimitri N. (2017), "Bitcoin mining as a contest," *Ledger*, 2:31-37.

Dixit A. (1996), *The making of economic policy: A transaction-cost politics perspective*, Cambridge: MIT Press.

European Banking Authority (2014), "EBA opinion on 'virtual currencies'," 4 July 2014, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (last access: August 06, 2018).

Evans D. (2014), "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms." *Coase-Sandor Institute for Law and Economics Working Paper*, n. 685.

Eyal I. and E.G. Sirer (2014), "Majority is not enough: Bitcoin mining is vulnerable," in Böhme R., M. Brenner, T. Moore, and M. Smith (eds.), *International conference on financial cryptography and data security*, Berlin: Springer, pp. 436-454.

Gibbons R. (2005), "Four formal(izable) theories of the firm?" *Journal of Economic Behavior & Organization* 58:200-245.

Hart O. (2017), "Incomplete contracts and control," *American Economic Review*, 107(7):1731-1752.

Holden R. and A. Malani (2018), "Can blockchain solve the holdup problem in contracts?", University of Chicago Coase-Sandor Institute for Law & Economics research paper No. 846.

Moore J. (2016), "Introductory remarks on Grossman and Hart (1986)," in Aghion P. et al. (eds.), *The impact of incomplete contracts on economics*, Oxford: Oxford University Press.

Nakamoto S. (2008), "Bitcoin: A Peer-to-peer Electronic Cash System" available at https://bitcoin.org/bitcoin.pdf (last access: August 06, 2018).

Nicita A. and M. Vatiero (2014), "Dixit versus Williamson: the 'Fundamental Transformation' reconsidered," *European Journal of Law and Economics*, 37(3): 439-453.

North D. (1990), "A transaction cost theory of politics," *Journal of theoretical performance*, New York: Cambridge University

Olson M. (1965), *The logic of collective action*, Harvard University Press.

Olson M. (1982), *The rise and decline of nations: Economic growth, stagflation, and social rigidities*, New Haven: Yale University Press.

Savelyev A. (2017), "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law," *Information & Communications Technology Law*, 26:2:116-134.

Shavell S. (2009), "Why Breach of Contract May Not Be Immoral Given the Incompleteness of Contracts," *Michigan Law Review*, 107:1569-1581.

Simon H. (1951), "A formal theory of the employment relationship," *Econometrica*, 19:293-305.

Sklaroff J. (2017), "Smart contracts and the cost of inflexibility," *University of Pennsylvania Law Review*, 166:263-303.

Swan M. (2015), *Blockchain. Blueprint for a new economy*, Cambridge: O'Reilly.

Swanson T. (2014), *Great chain of numbers: A guide to smart contracts, smart property and trustless asset management*, Amazon digital service.

Szabo N. (1997), "The idea of smart contracts," available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (last access: August 06, 2018).

The Economist, "The Trust Machine. The promise of the blockchain," October 31, 2015.

Thompson P. (2017), "How Bitcoin Forks Influence Bitcoin Price Rise and Fall," *Cointelegraph*, Oct 28, available at https://cointelegraph.com/news/how-bitcoin-forks-influence-bitcoin-price-rise-and-fall (last access: August 06, 2018).

Tirole J. (1999), "Incomplete contracts: Where do we stand?", *Econometrica*, 67(4):741-781.

Vatiero M. (2018), "Transaction and transactors' choices: What we have learned and what we need to explore," in Ménard C. and M.M. Shirley (eds.), *A research agenda for New Institutional Economics*, Edward Elgar Publishers, pp. 97-108.

Werbach K. (2018), "Trust, but verify: Why the blockchain needs the law," *Berkeley Technology Law Journal*, forthcoming.

Werbach K. and N. Cornell (2017), "Contracts *ex machina*," *Duke Law Journal*, 67:313-382.

Williamson O.E. (1971), "The vertical integration of production: Market failure considerations," *American Economic Review*, 61:112-123.

Williamson O.E. (1973), "Markets and hierarchies: Some elementary considerations," *American Economic Review*, 63(2):316-325.

Williamson O.E. (1975), *Markets and hierarchies: Analysis and antitrust implications*. New York: Free Press.

Williamson O.E. (1979), "Transaction-cost economics: The governance of contractual relations," *Journal of Law and Economics*, 22(2):233-261.

Williamson O.E. (1985), *The economic institutions of capitalism*, New York: Free Press.

Williamson O.E. (1991), "Comparative economic organization: The analysis of discrete structural alternatives," *Administrative Science Quarterly*, 36:269-296.

Williamson O.E. (2002), "The theory of the firm as governance structure: From choice to contract," *Journal of Economic Perspectives*, 16:171-195.

Williamson O.E. (2010), "Transaction cost economics: An overview." In Klein P.G. and M.E. Sykuta (eds.), *The Elgar companion to transaction cost economics*, Aldershott: Edward Elgar, pp. 8-26.

Wright A. and De Filippi P. (2015), "Decentralized blockchain technology and the rise of lex cryptographia," available at http://ssrn.com/abstract=2580664 (last access: August 06, 2018).

Yermack D. (2017), "Corporate governance and blockchains," *Review of Finance*, 21(1):7-31.

Zingales L. (2017), "Towards a political theory of the firm," *Journal of Economic Perspectives*, 31(3):113-130.

*Discussion Papers*
Collana del Dipartimento di Economia e Management, Università di Pisa



*Email della redazione:* lfanti@ec.unipi.it