Smart contracts vs incomplete contracts: A transaction cost economics viewpoint

Massimiliano Vatiero

Università di Trento (Italy) and Università della Svizzera italiana (Switzerland)
vatierom@usi.ch

Abstract. For the deterministic nature of the blockchain, smart contracts (agreements enforced by a blockchain) are supposed to work at lower transaction costs than traditional, *incomplete* contracts (which instead exploit a costly legal enforcement). This paper challenges that claim. I argue that because of the need for *adaptation* to mutable and unpredictable occurrences (a chief challenge of transaction cost economics), smart contracts may incur higher transaction costs than traditional contracts. This paper focuses on two problems related to adaptation: first, smart contracts are constructed to limit and potentially avoid any ex-post legal intervention, including efficiency-enhancing adaptation by courts—this may increase transaction costs in smart contracts. Second, the consensus mechanism on which every smart contract depends may lead to additional transaction costs due to an uncertain, majority-driven change of the blockchain that follows Mancur Olson's *Logic* of groups. The paper further proposes several institutional expedients that may reduce these transaction costs of smart contracts.

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

Acknowledgements. I received exceptionally helpful comments from Michal Gal, Inge Graef, Nadia von Jacobi, Bertin Martens, Giorgio Monti and participants at the 2021 TILEC workshop titled *Regulating digital markets: Enforcement and remedies* (Tilburg University). This paper benefitted from the generous financial support of the Brenno Galli Foundation. The usual disclaimers apply.

1. Introduction

As a traditional contract, a smart contract constitutes an exchange of promises between parties. Unlike a traditional contract, a smart contract exploits a blockchain as the enforcing medium for agreements between parties,[1] apparently without need of a legal enforcement (e.g., a court). The key feature of smart contracts is neither their digital nature nor the automatic mechanism, both of which characterize also computer-mediated transactions in many sectors,[2] but the fact that they use the blockchain protocol as enforcement. In that sense, smart contracts realize the 'code is law' paradigm,[3] according to which *code itself provides enforcement*. Furthermore, as the code-is-law paradigm *supposes*, blockchain constitutes the cheapest substitute for costly legal enforcement.[4] Indeed, the code obeys a 'if-this-then-that' logic: *if* the '*this*' is met, *then* the '*that*' automatically follows. Because of this deterministic nature of blockchain enforcement, parties cannot deviate from what is agreed ex-ante and validated by a blockchain. Apparently, there are relevant benefits of the irrevocable settings of smart contracts. For this reason, smart contracts are (promoted as) able to solve the risk

[1] A first question should be whether smart contracts are legally valid. Answering that question is beyond the scope of this paper. For this reason, instead of referring to 'contracts' I refer to 'agreements' between parties. For discussions on the legal enforcement of smart contracts in this journal, see: M Giancaspro, "Is 'smart contract' really a smart idea? Insights from a legal perspective" (2017) 33 *Computer Law and Security Review* 825; TJ de Graaf, "From old to new: From internet to smart contracts and from people to smart contracts" (2019) 35 *Computer Law and Security Review* 1; H Eenmaa-Dimitrieva H and MJ Schmidt-Kessen, "Creating markets in no-trust environments: The law and economics of smart contracts" (2019) 35 *Computer Law & Security Review* 69.

[2] For this type of transaction see: H Varian, 'Computer-mediated transactions' (2010) 110:2 *American Economic Review* 1. For a more detailed technical explanation of smart contracts, see T Swanson, *Great chain of numbers: A guide to smart contracts, smart property and trustless asset management* (Amazon digital service 2014); J Sklaroff, "Smart contracts and the cost of inflexibility" (2017) 166 *University of Pennsylvania Law Review* 263; K Werbach, "Trust, but verify: Why the blockchain needs the law" (2018) 33 *Berkeley Technology Law Journal* 439; JS Gans, "The fine print in smart contracts" (2019) *NBER working paper* No. 25443; M Maggiolino and L Zoboli, "Blockchain governance: The missing piece in the competition puzzle," (2021) 43 *Computer Law and Security Review* 1.

[3] Smart contracts lead to a shift of confidence, from trust in courts and the legal system to trust in code. Cf. L Lessig, *Code, and other laws of cyberspace* (Basic Books 1999); P De Filippi and A Wright, *Blockchain and the law: The rule of code* (Harvard University Press 2018). *The Economist* provides an easily introduction of blockchain as a trust machine: *The Economist*, "The trust machine. The promise of the blockchain," October 31, 2015. Concerning the trust in smart contracts, see also in this journal: RH Weber, "Rose is a rose is a rose is a rose—what about code and law?" (2018) 34 *Computer Law & Security Review* 701; de Graaf supra note 1; Eenmaa-Dimitrieva and Schmidt-Kessen supra note 1.

[4] D Tapscott and A Tapscott, *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world* (Penguin 2016); De Filippi and Wright supra note 3; A Wright and P De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia" (2015) <http://ssrn.com/abstract=2580664> accessed August 16, 2021; S Davidson, P De Filippi and J Potts, "Blockchains and the economic institutions of capitalism" (2018) 14:4 *Journal of Institutional Economics* 639. That blockchain technology represents a great revolution for our society is also witnessed by the fact that this technology may cover many fields, including the area of medicine. See C Thomson and R Beale, "Is blockchain ready for orthopedic? A systematic review" (2021) 23 *Journal of Clinical Orthopedics and Trauma* 1.

of opportunistic deviations (or hold-ups) and reduce consequent transaction costs that characterize traditional, "incomplete" contracts à la Oliver Williamson.[5]

In this article, I show that the claim that smart contracts allow transactions to be conducted more efficiently than traditional (incomplete) contracts underestimates a central problem of transaction cost economics: the need for an efficiency-enhancing adaptive mechanism.[6] Namely, an efficient institutional arrangement needs to be adaptive to mutable and unpredictable occurrences. In this paper I illustrate two main sources for smart contracts of transaction costs related to the problem of adaptation. First, for the deterministic nature of blockchain enforcement, smart contracts are constructed to limit and potentially avoid any legal intervention, even if an ex-post legal adaptation—in particular, a court's gap-filling intervention and interpretation—may reduce transaction costs of agreements between parties. The problem is that blockchain enforcement may prevent efficiency-enhancing adaptation by courts. A second disadvantage derives from the consensus mechanism. Although that mechanism affords the blockchain a degree of adaptation that can generate benefits, the actual governance of main blockchains is such that smart contracts have additional transaction costs due to a majority-driven adaptation that follows Mancur Olson's *Logic* of groups:[7] a group of blockchain's participants may change a blockchain to favor their own particular interests instead of the interests of all participants of a blockchain. The risk is that the consensus mechanism might increase (and not reduce) the uncertainty of the institutional setting and, therefore, distort choices of parties in a smart contract. We refer to such risk in terms of transaction costs for *mal*-adaptation. Table 1 summarizes my two main theses.

[5] The concepts of transaction costs, opportunism and incomplete contracts are here used in accordance with the meanings of the transaction costs economics à la Williamson. See, among others, OE Williamson, *The economic institutions of capitalism* (Free Press 1985). See also U Pagano and M Vatiero, "Costly institutions as substitutes: Novelty and limits of the Coasian approach" (2015) 11:2 *Journal of Institutional Economics* 265.

[6] Oliver Williamson highlights that "TCE [transaction cost economics] has been an *exercise* in *adaptive*, intertemporal economic organization from the outset" OE Williamson, "Transaction cost economics: An overview" in PG Klein and ME Sykuta (eds.), *The Elgar companion to transaction cost economics* (Edward Elgar 2010) pp. 8–26 at 9, italics added. In other words, "inasmuch as a full set of contingent claim markets is infeasible (by reason of bounded rationality), *adaptive*, sequential decision-making procedures need be devised," OE Williamson, "Markets and hierarchies: Some elementary considerations' (1973) 63:2 *American Economic Review* 316 at 318, italics added; and again, "[i]ntertemporal efficiency […] requires that *adaptations* to changing market circumstances be made" OE Williamson, "Transaction-cost economics: The governance of contractual relations" (1979) 22:2 *Journal of Law and Economics* 233 at 241, italics added. The adaptation is not only a central theme for transaction cost economics but also for the efficient breach theory: 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. See for instance, S Shavell, "Why breach of contract may not be immoral given the incompleteness of contracts" (2009) 107 *Michigan Law Review*, 1569.

[7] M Olson, *The logic of collective action* (Harvard University Press 1965); see also M Olson, *The rise and decline of nations: Economic growth, stagflation, and social rigidities* (Yale University Press 1982).

	Transaction costs	
	Decreasing	Increasing
1. Because the blockchain prevents any deviation from what contracting parties have agreed upon ex-ante	Blockchain avoids *opportunistic* renegotiations of smart contracts	Blockchain also prevents efficiency-enhancing adaptation • Transaction costs due to a lack of *legal adaptation*.
2. Because the consensus mechanism provides the blockchain with a degree of flexibility	Users can adapt the blockchain and smart contracts to new needs	Consensus mechanism may lead to an uncertain, majority-driven adaptation • Transaction costs for *mal-adaptation*.

Table 1. Transaction costs and adaptation in smart contracts.

To date, a comprehensive analysis of smart contracts from the perspective of transaction cost economics is severely lacking in the literature.[8] My contribution is twofold. First, this paper investigates and makes explicit transaction costs related to a lack of legal adaptation of agreement when they are enforced by a blockchain as in the case of smart contracts. Second, adopting the *Logic* of Mancur Olson, I show that the consensus mechanism may lead to a maladaptation and consequent high transaction costs for smart contracts. I ultimately argue that, from the perspective of transaction cost economics, though smart contracts reduce transaction costs related to contracting parties' deviations, they can also create or increase other costs related to adaptation.[9]

The remaining part of the paper unfolds as follows. In the next section, I offer a description of smart contracts by proposing a categorization in four types of enforcement. In Section 3, I illustrate the transaction costs in a smart contract due to a lack of legal adaptation. Transaction costs coming from a maladaptation (which depends on the consensus mechanisms and forking processes) are explained in Section 4. Section 5 is dedicated to an initial discussion on institutional expedients that may reduce transaction costs in smart contracts. I offer some concluding remarks in Section 6.

[8] Relevant exceptions are: D Yermack, "Corporate governance and blockchains" (2017) 21:1 *Review of Finance* 7; B Arruñada and L Garicano, "Blockchain: The birth of decentralized governance" (2018) Economic working paper series, n. 1608, Universitat Pompeu Fabra; R Holden and A Malani, "Can blockchain solve the holdup problem in contracts?" (2018) *University of Chicago Coase-Sandor Institute for Law & Economics research paper*, n. 846; C Catalini and JS Gans, "Some simple economics of the blockchain," (2020) 63:7 *Communications of the ACM* 80.

[9] I do not discuss a few other types of transaction costs that might stem from smart contracts. One such cost is the cost of energy. Cf.: B Biais, C Bisière, M Bouvard and C Casamatta, "The blockchain folk theorem" (2019) 32:5 *Review of Financial Studies* 1662. On the other hand, there are many other real benefits of smart contracting besides replacing a costly legal enforcement that are covered at length by other commentators such as Tapscott and Tapscott supra note 4.

2. Enforcing transactions: A taxonomy

In presenting different types of enforcement, let me follow the elegant reasoning of Ronald Coase's *The nature of the firm*:[10] because there are costs of functioning of market transactions (or transaction costs), an alternative institutional arrangement, that is, the firm, emerges. In a similar manner, because relevant costs arise from the legal enforcement of traditional contracts, as the literature on incomplete contracts has shown,[11] alternative institutional arrangements may emerge as cheaper alternatives. Blockchain enforcement is thus presented here as an alternative to a costly legal enforcement apparatus needed in a standard setting for traditional contracts.

Let us consider a familiar setting in the transaction cost economics literature: a supplier of a widget who can invest in asset-specificity and a client (e.g., a car manufacturer) who buys this widget.[12] For instance, this investment can represent a specific piece of equipment, bought by a supplier and needed for joint production with the car manufacturer. Alternatively, it can represent a relocation of a supplier's factory closer to the car manufacturer (e.g., the classic case of Fisher Body and General Motors). Because a specific investment is—by definition of specificity—not re-employable without sacrificing its productive value, the investor is locked into the specific relationship. The parties could write a contract and rely on a legal enforcement, a judicial system whose power comes from the political monopoly of power, to settle their conflicts ex-post. To ensure the contracted outcome, the legal enforcement will observe contracting parties' conduct and eventually impose penalties or other requirements if contracted obligations are not met. In this context, for the threat of a legal intervention, contracting parties should abide by their traditional contract (see Table 2).

Transactions by/within	**Enforcer/enforcement**
Traditional contract	A legal enforcer, such as a court
Firm	Internal hierarchical structure (à la Coase)
Relational contract	The socioeconomic network
Smart contract	The blockchain network

Table 2. Enforcing economic transactions.

[10] RH Coase, "The nature of the firm" (1937) 4:16 *Economica* 386.

[11] Cf. among others, O Hart and J Moore, "Foundations of incomplete contracts" (1999) 66 *Review of Economic Studies* 115; O Hart, "Incomplete contracts and control" (2017) 107:7 *American Economic Review* 1731.

[12] For instance, J Moore, "Introductory remarks on Grossman and Hart (1986)" in P Aghion, M Dewatripont, P Legros and L Zingales (eds.), *The impact of incomplete contracts on economics* (Oxford University Press 2016), pp. 3–16; M Vatiero, *The theory of transaction in Institutional Economics* (Routledge 2021).

However, according to incomplete contract theory, this legal enforcement is costly. In the parlance of incomplete contract theory, the exact nature of the widget, though it is potentially observable by parties, is not verifiable by the legal enforcer. The main consequence is that the client can threaten to deviate from what is agreed ex-ante and the investor (in our case, the supplier) will not recoup the full value of his or her investment in asset specificity (*hold-up*). Because of hold-up risk, the general result is that the investor will choose a lower level of investments in asset-specificity.

With asset-specificity and incomplete contracts, the two parties may, and do, have an interest in merging into a sole firm, which is organized through an internal hierarchical structure, in order to deal with transaction costs related to the risk of hold-up.[13] A transaction in a firm can be performed at lower transaction costs than the same transaction via a traditional contract. Orders by a boss rather than verification by a legal third party will *enforce* transactions within the firm. In other terms, when the legal enforcement is costly, then it is substituted by an internal hierarchy—a firm's "hierarchy is its *own court of ultimate appeal*"[14] (see Table 2).

Nonetheless, transactions enforced by a hierarchy, as in firms, as well as transactions via a legal intervention, as in traditional contracts, are not without costs. Another alternative is represented by so-called "relational contracts," the enforcement of which is based on the fact that parties care about their reputation for the sake of their future transactions.[15] That is, the threat of a stigma in a socioeconomic network—for instance, in a given community—encourages parties to abide by agreements, even without any explicit legal intervention (see Table 2).

Smart contracts secure transactions without any external legal intervention as well. Indeed, both relational contracts and smart contracts are self-enforcing in the sense that they rely on a peer-to-peer governance: the enforcement is performed by the community network in the case of relational contracts, while through a digital network in the case of smart contracts (see Table 2). However, there is an important difference between the enforcement in a relational contract and the one as conceived in a smart contract. In the case of relational contracts, there is an ex-post punishment, namely, deviating behaviors are possible but they are disciplined ex-post throughout a reputation mechanism. In contrast, for the determinist nature of the blockchain, smart

[13] See Williamson supra note 5. Cf. also Coase supra note 10.

[14] OE Williamson, "Comparative economic organization: The analysis of discrete structural alternatives" (1991) 36 *Administrative Science Quarterly* 269 at 274. Similarly, Margaret Blair and Lynn Stout: a firm's hierarchy serves to "resolve disputes between parties for whom resolution through explicit contracting is too costly ... [or] settle an internal dispute over transfer prices between two units or subsidiaries of the same corporation, or between two individuals in a firm over work assignments, promotions, or division of a bonus pool" MM Blair and LA Stout, 'A team production theory of corporate law' (1999) 85:2 *Virginia Law Review* 247 at 284–285.

[15] See, among others: B Klein, "Why hold-ups occur: The self-enforcing range of contractual relationships" (1996) 34 *Economic Inquiry* 444.

contracts cannot be breached. Each smart contract contains a set of rules that triggers predefined responses corresponding to particular contingencies in computational *if-this-then-that* logic.[16] However, as I show in the next section, even if smart contracts can and do avoid any ex-post deviation from an ex-ante contractual agreement (and, therefore, protect from any risk of hold-up), they can and do also avoid any efficiency-enhancing legal adaptation.

Hence, blockchain technology provides theory and economic systems with a fourth type of enforcement (see Table 2).[17] A blockchain represents an enormous ledger that, like traditional ledgers,[18] records information on transactions. Its chief novelty in relation to other ledgers is that a blockchain has no central repository. By way of the consensus mechanism, blockchain's participants validate and store information as well as enforce transactions. The most widely used consensus mechanism in a blockchain is called proof-of-work: the majority of computational power in a blockchain does indeed rule. In a proof-of-work system, participants (called miners) of a blockchain, using words of the inventor of the blockchain technology, "*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."[19] An alternative mechanism to validate transactions is based on proof-of-stake, in which 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 blockchain in the proof-of-stake system is the outcome of the *vote* of blockchain's participants *with their wallet*.

However, what is called a "hard fork" in the blockchain community can deny the determinism of smart contracts. A hard fork is any change in the rules of a blockchain that involves forward incompatibilities with the previous rules, such that a transaction accepted in the new blockchain could be invalid in the old one. When a part of a blockchain's participants vote for that change and a part against, then a blockchain splits into two blockchains: the original continues to operate under its original set of rules, whereas the new one, stemming from the block at which the hard fork was implemented, operates under different rules. In 2016, for instance, the Ethereum community split after the DAO hacking incident. The DAO was an online crowdfunding system built entirely on smart contracts and that stole $50–60 million from backers. Members of the Ethereum suggested rolling back the blockchain in order to cancel the transactions that diverted the blockchain's money. Ethereum forked and split into two incompatible "worlds": one world in which the DAO, along with all of the consequences of the hack, still exists (Ethereum Classic) and another in which the DAO never happened, and

[16] Cf. Holden and Malani supra note 8.

[17] Eenmaa-Dimitrieva and Schmidt-Kessen supra note 1 propose a similar scheme but their categorization includes only three enforcement mechanisms: contract (law), community enforcement and enforcement through technology such as smart contracts.

[18] 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.

[19] S Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" (2008) available at <https://bitcoin.org/bitcoin.pdf> accessed August 16, 2021 at 8, italics added.

in which blocks of the DAO hacking incident were removed (Ethereum). Both blockchains continue to survive. What is more relevant here is that the forking process is a means for recouping thefts and frauds as the DAO hacking incident shows, and, more generally, this process can afford a means for changes/adaptation of the blockchain. According to Arruñada and Garicano,[20] the hard-forking process may represent a means of blockchain's users to meet their new needs and adapt the blockchain. However, Section 4 shows that there are transaction costs related to a blockchain's internal governance: although, through a forking process, participants may "adapt" the blockchain, the *logic* of groups may create a bad adaptation of the blockchain. This problem of governance within the blockchain may determine costs for transactions performed in a smart contract.

3. Transaction costs for the lack of an external legal adaptation

With a legal adaptation, I refer to an ex-post legal intervention to adapt the contractual relationship to some extent. A major claim of the economic analysis of law and theory of contracts is that courts intervene in order to complete or close an incomplete contract.[21] In particular, the intervention of a legal enforcer could enable an avenue for contracting parties even in circumstances of hold-up conduct: "Courts can obtain substantial information after the realization of events, so they may do tolerably well in controlling holdup."[22]

Let me consider and revisit an example that Szabo provided when he introduced the concept of smart contracts: in a car rental smart contract (Szabos' example is on a car purchase[23]), because of a car immobilizer installed by the lessor, the car cannot be driven if the lessee has not fulfilled their payment obligations within the agreed timeframe. Once this agreement is validated in the blockchain, because of its deterministic nature, the execution of the agreement (the performance as well as the corresponding transfer of value, i.e., payment) occurs with certainty. Namely, there is no way to deviate from what the parties agreed to ex-ante: The code executes itself and cannot be stopped as is described by the 'code is law' paradigm. Now, suppose that, after the smart contract is validated, the lessor has an immediate need to go with the car to a hospital, for example

[20] Arruñada and Garicano supra note 8.

[21] See: I Ayres and R Gertner, "Fillip gaps in incomplete contracts: An economic theory of default rules" (1989) 99 *Yale Law Journal* 87; A Schwartz and RE Scott, "Contract theory and the limits of contract law" 2003 113:3 *Yale Law Journal*, 541; R Posner, "The law and economics of contract interpretation" (2004) 83 *Texas Law Review* 1581; S Shavell, "On the writing and the interpretation of contracts" (2006) 22:2 *Journal of Law, Economics & Organization* 289; S Shavell, "Contract holdup and legal intervention" (2007) 36:2 *Journal of Legal Studies* 325; A Schwartz and RE Scott, "Contract interpretation redux" (2010) 119:5 *Yale Law Journal* 926.

[22] Shavell 2007 supra note 21 at 348.

[23] N Szabo, "The idea of smart contracts" (1997) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html> accessed August 16, 2021.

because of an accident at work. Let me further assume that the lessee wants to help the lessor and get the latter to the hospital immediately, but the lessee's digital wallet is unable to fulfill the payments agreed upon in the smart contract. What follows is that even if both parties agree to *deviate* from the smart contract (namely, to get the lessor to the hospital even if lessee's digital wallet is insufficient), this will not be possible unless the parties waste additional time and resources renegotiating the previous smart contract and/or writing a new smart contract in this emergency scenario. What would happen with a traditional contract? The lessee would immediately accompany the lessor to the hospital with the car, even in the absence of financial coverage. Only after that would a court judge parties' conduct and define compensations. Likely, the court would not punish the lessee who has not fulfilled the agreement, justifying that conduct on the basis of *force majeure* (a concept, among others, untranslatable in computer code of a smart contract). In this sense, the court *completes* the *incomplete contracts* after unforeseeable events have occurred. The court has an informational advantage over the private parties—because the court's intervention is ex-post when (ex-ante unpredictable) circumstances occur—that the same private parties, in traditional contracts but not in smart contracts, can take advantage of.

In more detail, let me develop the example of the transaction of a widget in Section 2. After a smart contract is coded, validated, and stored in a blockchain, there is an exponential, unexpected rise in the production costs of the widget (e.g., for the lockdown order to curb the spread of COVID-19). The rise in costs implies that the agreed-upon price no longer covers the costs of making the widget. In that scenario, a smart contract with a price defined before the unexpected contingency may be inefficient. The contractual agreement should adapt to new contingencies with a different price, if available, or should be breached. Neither of those cases is (supposed to be) possible for the deterministic construction of smart contracts. In a traditional contract, in contrast, legal intervention can adapt the contractual agreement in different, sometimes complementary, ways: "The courts fill gaps in contracts, resolve conflicts and ambiguities of language, and sometimes replace the parties' express terms with the courts' terms."[24]

It is worth distinguishing several types of external intervention available to the legal enforcer. The first type derives from the adjudicative gap-filling doctrine: a court fills any gap in the contract *when and if* the gap emerges and prompts a dispute. Adjudicative gap-filling is efficient for parties when the costs of carefully drafting the contract to deal with contingencies (i.e., writing costs), especially ones highly unlikely to materialize, exceed the benefits that are discounted by the extremely low probability that they will ever be realized. In a smart contract, parties could have exceedingly high costs to write all contingencies, including highly unlikely ones—for example, the coronavirus pandemic in our example. That condition means that the parties either face high transaction costs in including highly unlikely contingencies or do not specify those contingencies in order to save writing costs. However, if those unlikely contingencies materialize as in our example, the smart contract can determine inefficient outcomes. Instead, in a semantic contract, the parties

[24] Shavell 2006 supra note 21 at 290.

could contract in (quasi-)ignorance, leave gaps in exceedingly unlikely contingencies, and trust in the efficiency and good sense of a legal enforcer.

The second type of judicial intervention, which needs to be distinguished from adjudicative gap-filling, is contract interpretation, in which courts determine the meaning of express terms. In interpretation, the external enforcer has a degree of flexibility in efficiently adapting contractual clauses ex-post, at least in merchant-to-merchant traditional contracts.[25] For instance, the court could interpret the pricing of parties to reflect unexpected costs as well. This recalls the case of *Aluminum Co. v. Essex Group, Inc.*, in which the parties, Alcoa and Essex, included in a traditional contract a price escalation clause centered on the wholesale price index for industrial commodities.[26] As a result of the steep increase in the price of oil and therefore in the cost of electricity in 1973–1974, Alcoa's cost of contractual performance rose far faster than the wholesale price index, thereby precipitating its suit for reformation. Ruling in Alcoa's favor, the court held that the parties had intended the price escalation clause to reflect the increase in Alcoa's cost over the life of the contract. Thus, the court efficiently completed the traditional contract by adapting the contractual agreement to unexpected costs and contingencies. In a smart contract, the supplier—in the case above, Alcoa—would have instead received an ex-ante defined price, even if that price were no longer able to cover the widget's production costs. Because smart contracts are constructed to avoid the need for a legal intervention, they also preclude the benefits arising from judicial interpretation.

The general message is that adjudicative gap-filling and interpretation may close otherwise incomplete traditional contracts. Furthermore, the prospect of adjudicative gap-filling and/or interpretation spares the parties from contracting efforts, especially the transaction costs of writing a clause for each scenario in a contract. For those reasons, whereas traditional contracts trust in and (benefit from) a court's gap-filling intervention and interpretation, smart contracts have to either deal with exceptionally high writing costs, especially for drafting, unlikely contingencies and performance that are realized in the long run, [27] or deal with inefficient outcomes if parties leave gaps in several aspects of the smart contract.

Let me also underline that the fact that most traditional contracts never reach the courts does not diminish the role of legal enforcement. The mere possibility of judicial intervention prevents breach and litigations. That is, the judicial system enacts enforcement over traditional contracts, not only explicitly, by implementing its decisions, but also implicitly, by encouraging private adaptation: considering a potential legal intervention in

[25] Cf. Schwartz and Scott 2003 and 2010 supra note 21.

[26] Cf. Posner supra note 21.

[27] Note that the longer the performance of a contract, the more difficult it is for parties to foresee and include the various contingencies that may affect performance; hence the more favorably the balance between smart contracts and traditional contracts inclines toward the latter.

the case of conflicts, parties may agree to voluntarily adapt ex-post their traditional contract to unexpected contingencies.[28]

Legal intervention also poses (transaction) costs, however. First, because every external legal intervention originates in a legal dispute, there are necessarily costs of litigation.[29] Second, courts may make mistakes[30] and hold-up conduct is often particularly subtle: The court has to understand if a deviation represents opportunistic behavior (i.e., hold-up conduct) or if it is justified on legal reasons. Third, judicial intervention is slow, and slower courts reduce incentives for economic transactions.[31] These costs can be high and, in several contexts, prohibitively so. In a comparison between traditional and smart contracts, in contexts (e.g., countries) in which legal enforcement has a low quality, the smart contract, even when high writing costs are taken into account, could represent a cheaper alternative to traditional contracts. In other contexts where the quality of the judicial system is high, by contrast, the benefits of a legal intervention of a traditional contract could overpass the costs of writing smart contracts.

4. Transaction costs for maladaptation

The consensus mechanism serves to upgrade the blockchain. However, a mounting concern with consensus mechanisms is the risk of concentration, both in the case that blockchains use proof-of-work and when they use proof-of-stake. In the case of proof-of-work, the difficulty of the validation process has spiked and thus decreased the probability that an individual using an everyday computer will mine a block, and therefore miners (seeking to validate transactions) have incentives to merge and create so-called 'mining pools' in which they combine their computational resources and deploy specialized hardware to mine new blocks. An example of evidence of such a concentration of computational power is provided by the fact that in 2016 the four biggest mining pools had more than 53% of the computational power in the Bitcoin blockchain and the three biggest mining pools had 61% of the computational power in the Ethereum blockchain.[32] There was a similar

[28] This is the idea of *private ordering* à la Williamson, e.g., Williamson 1979 supra note 6.

[29] For a comparative analysis of costs of litigation see: C Hodges, S Vogenauer, and M Tulibacka (eds.), *The costs and funding of civil litigation: A comparative perspective* (Hart Publishing 2010).

[30] Cf. G Tullock, "Court errors" (1994) 1 *European Journal of Law and Economics* 9; S Shavell, "The appeals process as a means of error correction" (1995) 24 *Journal of Legal Studies* 379. In addition to courts' errors, there are "legal bubbles" when courts ex-post attempt to readapt their decisions that previously ignored implications of innovative activities. See M Giraudo, "On legal bubbles: some thoughts on legal shockwaves at the core of the digital economy" 2021 *Journal of Institutional Economics* 1.

[31] Cf. M Chemin, "Does court speed shape economic activity? Evidence from a court reform in India" (2012) 28:3 *Journal of Law, Economics, & Organization* 460; J Ponticelli and LS Alencar, "Court enforcement, bank loans and firm investment: Evidence from a bankruptcy reform in Brazil" (2016) 131 *Quarterly Journal of Economics* 1365.

[32] AE Gencer, S Basu, I Eyal, RT Van Renesse and E Gün Sirer, "Decentralization in bitcoin and ethereum networks" (2018) arXiv preprint arXiv:1801.03998.

concentration also in the period between December 2020 and January 2021.[33] This (tendency for) concentration is destructive for a system that wants/wanted to be diffused. Big mining pools or cartels of mining pools can put malicious strategies into action: they can selectively reject competing miners' transactions, raise fees, and engage in selfish mining and transaction differentiation.[34] In particular, Eyal and Gün Sirer show how a pool of miners can increase their relative income by using a malicious strategy, referred to as *Selfish Mining*.[35] Gal and Szabo add a further deviant strategy to collect rewards, which they called the "piggyback" strategy, and they show that this strategy permits controlling the blockchain with less than half the computing power.[36]

Similar problems emerge in blockchains that use the proof-of-stake mechanism. This mechanism is a reformulation of the general system of voting in assemblies used by public companies—that is, voting proportionate with ownership stakes (i.e., shares). As such, the mechanism faces problems familiar in corporate law, including the presence of a majority stakeholder or groups of dominating stakeholders. Those with a majority of stakes (i.e., voting rights) may make decisions about blockchains, as may occur in public companies, in order to benefit themselves at the expense of others—they are called private benefits of the control in the lexicon of corporate governance literature.

Adopting the perspective of *The Logic of Collective Action* of Mancur Olson (i.e., one subgroup of a group may exploit the group), the consensus mechanisms in general and hard fork in particular can serve the interests of groups with the power to make changes in the blockchain (e.g., the majority of computational power). In concrete, the risk of centralization may lead a subgroup of a blockchain's participants to exploit the entire blockchain. That risk is more evident if one looks at hard forking. After all, a "[h]ard fork may pursue different objectives, from eliminating security hazards in the code to implementing new functions or *even reversing transactions.*"[37] Reversing the transaction was indeed experienced in Ethereum's hard fork, following the hacking of the DAO, when members of the Ethereum community suggested rolling back the blockchain in order to cancel transactions that had diverted the fund's money. A majority of members of the Ethereum

[33] AR Sai, J Buckley, B Fitzgerald and A Le Gear, "Taxonomy of centralization in public blockchain systems: A systematic literature review" (2021) 58:4 *Information Processing & Management* 1.

[34] I Eyal and E Gün Sirer, "Majority is not enough: Bitcoin mining is vulnerable" in R Böhme, M Brenner, T Moore and M Smith (eds.), *International conference on financial cryptography and data security* (Springer 2014), pp. 436–454; K Dowd and M Hutchinson, "Bitcoin will bite the dust" (2015) 35:2 *Cato Journal*, 357 at 372–374; J Gal and MB Szabo, "Majority is not needed: A counterstrategy to selfish mining" (2021), file with the author.

[35] Eyal and Gün Sirer supra note 34.

[36] Gal and Szabo supra note 34.

[37] Arruñada and Garicano supra note 8 at 8, italics added. As Arruñada and Garicano describe in their article, not all blockchains' participants benefit equally from a hard-forking process. A forking process can and very often does create winners and losers. Authors note also that blockchains often rely heavily on the existence of a leader, as is the case with Ethereum and its founder, Vitalik Buterin, who could bias the blockchain environment.

community voted to revoke those transactions, which was achievable by upgrading the blockchain without the allegedly fraudulent transactions, whereas a minority refused to alter the blockchain, as they believed that it should continue to be immutable. As David Yermack 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.[38]

For those reasons, majority-driven changes in blockchains can reverse transactions and therefore might make uncertain the institutional setting of smart contracts.[39]

Let me develop the example of the transaction between the supplier of the widget and the client (as introduced in Section 2). Assume a blockchain in which a large majority of transactions between a supplier and the client work along with a smart contract in order to ensure investments in asset-specificity. In this smart contract, parties have defined a clause with a set of fines for every deviation of clients. Now, suppose that one coalition of clients proposes to alter the blockchain in a way that reverses this clause on fines. If such a coalition of clients has enough computational power or stake to change the blockchain, then fines will be cancelled or renegotiated. It implies that all clients who behave opportunistically are no longer fined. It implies also that all clients who behaved opportunistically in past transactions may recoup their fines or part of these (as participants recouped their funds after the DAO fraud). Anticipating this opportunity, all clients could have incentives to behave opportunistically. Eventually, a coalition of suppliers could react to the turn of events, voting against the proposal to reverse or renegotiate fines. This blockchain may split into two: a blockchain in which the clause with fines continues to exist and one in which it ceases to exist. In such cases, one consequence is that each supplier incurs potential losses because he or she did not attain the revenue of his or

[38] Yermack supra note 8 at 28, italics added.

[39] Of course, one could object that such group logic affects only public or permissionless blockchains (in which any participant can vote for the validation of blocks), which is the most common type of blockchain, but does not affect private or permissioned ones. It is possible that the restricted number of users who "govern," so to speak, the private blockchain can limit the formation of big mining pools or majoritarian stakeholders, prevent the blockchain from becoming biased, and prompt a hard fork only if it benefits the entire blockchain. Nevertheless, private blockchains face a basic contradiction: the fewer the potential validators, the easier it may be to manipulate the blockchain via consensus mechanism by validators. In similar terms, Maggiolino and Zoboli supra note 2 at 9, italics added: "*within a permissioned blockchain*, it is also possible that a very strong coordination mechanism within a group of users would enable them to control the blockchain. In such a case, permissioned blockchains might resemble industry consortia or joint ventures, potentially raising antitrust concerns."

her investment *with certainty*. That is, a potential renegotiation via forking—reversing or redefining fines stored in the blockchain—can distort the supplier's choices about investing in asset-specificity and generate a suboptimal outcome.

Consensus mechanisms can determine rules for smart contracts that are aligned only with a subgroup of a blockchain's participants.[40] Then, smart contracts may incur high transaction costs due to the risk that the blockchain is driven by one or more coalitions of users with sufficient computational power or stakes that change rules to favor their own, particular interests at the expense of others.

5. Reducing transaction costs of smart contracts

Blockchain technology is not a free lunch, that is, it does not create an environment without transaction costs. When compared, as I have argued, smart contracts may incur higher transaction costs than traditional contracts if there are high benefits from legal adaptation costs and high costs from maladaptation deriving from concentrated computational power in a blockchain. However, even if I have presented four ways of enforcing transactions (Section 2), hybrid scenarios may and do emerge in which a transaction is arranged along with different but complementary types of enforcement. Namely, smart contracts may be complementary to, not only substitutes for, traditional contracts. In particular, smart contracts can likely benefit more from interacting with other (traditional) institutional arrangements than from attempting to set a parallel system of their own.[41] That issue is a problem for future studies. However, here, I can advocate the plan of important rule-makers in "making law more code-like,"[42] namely in improving the institutional setting to facilitate smart contracts. For instance, the European Commission announced that it wants to create the right enabling environment for blockchain technology and smart contracts.[43] Similarly, in the UK, the government is considering "reviewing the current legal and regulatory framework for ensuring that it facilitates the use of smart contracts."[44]

---

[40] In a similar vein, in July 2014, the European Banking Authority 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." European Banking Authority (2014), "EBA opinion on 'virtual currencies,'" July 4, 2014, <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed January 6, 2021 at 5.

[41] See Werbach supra note 2.

[42] Werbach supra note 2 at 541ff.

[43] See de Graaf supra note 1.

[44] Law Commission—Reforming the law, 'Thirteenth programme of Law Reform' (2017) at section 2.39 <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2017/12/13th-Programme-of-Law-Reform.pdf> accessed January 6, 2022.

However,"[j]ust as regulators and lawyers can adapt to the blockchain environment, distributed ledger systems can become more hospitable to legal enforcement."[45] As de Graaf underlines in this journal, programmers of smart contracts may collaborate with lawyers in order to develop better smart contracts.[46] It could imply that, given potential benefits of an ex-post intervention by a court, in particular when there are unpredictable scenarios, throughout suitable technicalities, parties involved in smart contracts may prefer leaving room for a legal adaptation.

Regarding the group's Logic in blockchain, it is worth considering that even traditional contracts may face the same problem. After all, in a parliamentary democracy, a group of citizens could vote for political parties to revise contract law according to their own, particular preferences, and at the expense of the minoritarian groups. However, that circumstance is more costly than in the case of smart contracts, because a reform of contract law as well as each legal reform is intermediated by a costly and long legislative process that involves political parties and several socioeconomic stakeholders, and is characterized by a parliamentary debate. In addition, there are constitutional norms in democratic countries that set limits and rigid procedures to change the rules in order to safeguard minoritarian parties. These limits and rigidities may reduce the flexibility of a legal ordering but create "legal certainty" for private parties, including minoritarian groups. Moreover, these constitutional norms that provide limits and rigidities can be changed only with specific and qualified procedures—for instance, with qualified majorities.[47] In a blockchain, instead, every rule can be changed with a simple majority (of computational power or of stakes) and this can and does create uncertainty and transaction costs. One way to mitigate this problem, which recalls legal requirements to change constitutional norms, is to increase the threshold to make a fork (for instance, 66% or 75% of the computational power or of stakes), at least if the fork determines several types of consequences (e.g., economic consequences). This could increase confidence of participants in the rules of a blockchain and encourage agreements via smart contracts. An alternative institutional expedient could be to define a pecuniary compensation for participants of a blockchain who refuse a hard fork. Indeed, for protecting minoritarian groups it could be *fair* to transfer a part of advantages deriving from a fork (if a fork occurs, it means that advantages should overpass disadvantages,

[45] Werbach supra note 2 at 545. See also possible regulatory responses by Eenmaa-Dimitrieva and Scmidt-Kessen supra note 1.

[46] De Graaf supra note 1.

[47] In Switzerland, each amendment of the Swiss Federal Constitution requires the double majority: the majority of people and the majority of Cantons. In Italy, each amendment of the Italian Constitution must be approved by an absolute majority of the members of each House in two successive debates at intervals of not less than three months. Said amendment is submitted to a popular referendum when, within three months of their publication, such a request is made by one fifth of the members of a House or five hundred thousand voters or five Regional Councils. The law submitted to popular referendum shall not be promulgated if not approved by a majority of valid votes. A popular referendum shall not be held if the amendment has been approved in the second voting by each of the Houses by a majority of two thirds of the members.

otherwise no one would vote for a fork) from the group that wants to change the rules of the blockchain to group(s) that may suffer such a change.

6. Concluding remarks

While the economic transactions can be enforced by a legal party as in traditional contracts, by a 'hierarch' as in transactions within the firm, and by reputation as in relational contracts, smart contracts represent another category, one based on blockchain enforcement. This paper has attempted to respond to a growing chorus of scholars who assert that smart contracts, given their disintermediated, deterministic and (apparently) decentralized nature, work more efficiently than semantic contracts.

Herein, I have focused on one source of transaction costs in smart contracts: the adaptation of institutional arrangements. I have argued that smart contracts preclude any ex-post efficiency-enhancing adaptation of contractual terms by a legal intervention, while an external legal enforcement "closes" or completes a traditional contract, as theories mentioned here have shown. Thus, compared to a traditional contract, a smart contract poses an initial disadvantage related to the lack of an ex-post legal adaptation. A second disadvantage derives from the consensus mechanism. The consensus mechanism and in particular forking pose the risk that a group of a blockchain's users with sufficient computational power or stakes, whether in permissionless or permissioned blockchains, change the rules to favor itself and thereby create an inefficient, unreliable, and uncertain institutional setting for smart contracts. This implies that, even though that mechanism affords the blockchain a degree of adaptation that can generate benefits—for example, the ability to be updated to meet new needs or recoup investors in the case of fraud, as in the DAO's incident—smart contracts have additional costs due to an uncertain, majority-driven adaptation that follows Mancur Olson's *Logic* of groups.

Once potential transaction costs in smart contracts have been identified, this paper proposes an initial list of institutional expedients that could reduce them. Further effort and future research in this direction are necessary, however.

Address:

Massimiliano Vatiero
Via Inama, n. 5
Department of Economics and Management
38122—Trento
Italy

Biosketch:

Massimiliano Vatiero is an associate professor in Political Economy at the University of Trento (Italy) and research fellow in Law and Economics at the Università della Svizzera italiana (Switzerland). His research interests cover Institutional Economics, Law and Economics, and Corporate Governance. He has published articles on *History of Political Economy*, *Journal of Economic Surveys*, *Journal of Institutional Economics*, *Journal of Economics Issues* and *Kyklos*, and chapters in edited books such as the *Oxford Handbook of Corporate Law and Governance*, JN Gordon and R Wolf-George, eds., (Oxford University Press, 2018).