

THE USE OF SMART CONTRACTS IN THE CRYPTOCURRENCY MARKET (AND BEYOND)

Pietro Andrea Podda – Pavel Macura – Harold Neal

Abstract

The current paper studies the use of the so-called Smart Contracts, potentially usable in several markets and particularly in that of Cryptocurrency. This latter market is characterised by impersonal transactions which often operate out of the control of any relevant authority. This creates security challenges for the transactions. Smart Contracts have been devised in order to guarantee the safe enforcement of an agreed transaction, even when there is not an agency (third party) in charge of monitoring the effective and correct implementation of a binding agreement. The system of Smart Contracts works using computer programs which operate automatically without any possibility of cancelling or withdrawing from the contract. The system is thought to guarantee certainty and curb transaction costs, which would otherwise become a hurdle on the party and encourage moral hazard as well as adverse selection. Indeed, the system of Smart Contracts is not immune from risks. Besides the risk embedded with potential hacking and violating individual accounts, there are also other potential issues related to the legal connotation of contracts. An automatic enforcement may prevent the effectiveness of legal actions aimed at claiming vices of the very contract and therefore put the rights of the parties in jeopardy.

Key words: Smart Contracts, Cryptocurrency, Security, Risk, Transaction Costs

JEL Code: K12, O3

Introduction

This paper contains a discussion of the growing use of Smart Contracts, as well as an analysis of some controversial aspects of their use, related to basic legal principles on the validity/not validity of Contracts. Smart Contracts are “self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code,, (Frankenfield, 2021, para. 4)

This topic appears of major importance because of the growing use of Smart Contracts in the contemporary, global, and often impersonal economy. Smart Contracts are normally associated with Cryptocurrency in the sense that Smart Contracts—besides representing agreements—are also electronic platforms that guarantee the performance of obligations. This particular association is grounded because Smart Contracts really perform the function described in the previous sentence. The current literature has paid a certain level of attention to Smart Contracts (see, for example, De Ridder et.al., 2017); nevertheless the legal aspects of these type of contracts have so far received only scant attention (but see Barbry, 2017; Governatori et.al., 2018). The literature tends to highlight the advantages of Smart Contracts in terms of their capacity to curb Transaction Costs, rather than discussing the disadvantages that automatically enforceable contracts may generate for persons invoking contractual vices. The legal problems with Smart Contracts have recently been studied, following different perspectives, by for example Smith and Bechtold (2019) and Wilkens and Falck (2019). Ferreira (2021) has recently provided a review of the literature on the topic. All these authors have highlighted the limitations and shortcomings typical of the online resolution of disputes and have also expounded the attempt to regulate Smart Contracts.

The use of Smart Contracts is not frictionless as their automatic enforceability leaves room for concern regarding the possibility that the underlying agreement may be contaminated by legal vices (i.e. duress, mistake). This would hardly be curable because the agreement is enforced automatically. In case any party of a standard (meaning not automatically enforceable via electronic protocols) contract contends that the underlying agreement is not valid, then this particular party may block performance and activate a judicial process. This option is not easily feasible when the enforcement of a specific transaction is guaranteed by a Smart Contract as the main characteristic of Smart Contracts is their automatic enforcement and, eventually, the anonymity of the parties.

The automatic enforcement of Smart Contracts has advantages and disadvantages. On the one side, this particular solution guarantees enforceability of transactions between parties often unaware of one another's identity and location. This appears, at least at first sight, to be of major importance in a global economy characterized by impersonal transactions whose enforcement may be opportunistically blocked. As highlighted by North (1990; 2005) and Williamson (1985; 1986) and many other scholars associated with the New Institutional Economics, an economic

environment based on impersonal transactions leaves the door open for multiple instances of opportunistic behaviour (i.e. fraud, avoiding respecting obligations). In these cases, the safety of the agreement is not reinforced by kinship and long-term ties between parties who feel that opportunistic behaviours are morally ungrounded and economically inconvenient (due to potential reputational damage). Hence, parties may behave opportunistically feeling that fraud, arbitrary litigation and similar mechanisms used to avoid respecting contracts are feasible and convenient. Indeed, opportunism may entail moral hazards and adverse selection (North, 1990), jeopardizing the efficient continuation of economic interactive processes. Enforcing contracts through courts is expensive, especially for small economic agents, and eventually ineffective, especially when the parties are located in different countries and the system of mutual recognition of judicial pronouncements is questionable. Therefore, a mechanism of automatic enforcement of contracts may represent a form of guarantee—an institutionally-based way to prevent opportunism, curb transaction costs and guarantee the achievement on an agreed-upon transaction. This perspective highlights how Smart Contracts can be advantageous.

On the other side, the very automatic enforcement of transactions may itself represent a source of concern. Parties of contracts may be misled in various ways, being prone to legal mistakes even when accepting a standard contract. Moreover, their judicial capacity at the moment of accepting any specific transaction could be questionable as they may, for example, be mentally disturbed on a permanent or temporary basis. In these types of cases, the other party is likely not to have awareness of the vices surrounding the apparently valid acceptance of a transaction from the other side. These risks represent a challenge for the safety of transactions based on Smart Contracts.

We recognise here that there has been some advancement in the regulation of Smart Contracts. The most recent Digital Dispute Resolution Rules, entered into force in the UK in 2021, represent a step forward. Nonetheless, these rules require the abandonment of anonymity, the preliminary acceptance by the party, and cannot be imposed on subjects out of the UK's jurisdiction. The problem, then, persists because the very conduct of the party not conditioning the contract to the respect of these rules may itself be vitiated by some sort of incapacity or by mistake. Hence, the validity of our arguments, which will be better expounded later, resist the very recent intervention of a legislator. In addition, the abandonment of anonymity and the

possibility to condition the enforcement of the Smart Contract to a dispute profoundly alters the initial, intrinsic connotation of Smart Contracts.

Our paper will investigate and discuss the problems outlined in this introductory first section. The next section will offer an overview of Smart Contracts and their use in the contemporary economy whereas the third section will focus on an analysis of the legal conundrums embedded in the use of Smart Contracts. Conclusion and references will follow.

1 The Emergence of Smart Contracts

Through Smart Contracts, transactions become enforceable without the presence of third parties (i.e. Clearing Houses or any equivalent organisation) acting as intermediators or guarantors. This independence for the very enforceability of the transaction is considered a major advantage by the supporters of the system. The enforcement of transactions becomes speedy, simple and effective, and the costs of enforcing contracts (in terms of money as well as time) are eliminated. This represents a major advantage in an economy where actors act through speculative transactions and where long term investments request certainty of contract enforcement. Niko Szabo is considered as the pioneer of this specific type of contract. The pioneering work of Szabo aimed to exploit electronic protocols in order to promote and facilitate electronic commerce. Currently, Smart Contracts are shaped as computer programs more than as Contracts per se and are embedded in BlockChains or Ledgers. Digital security is (or, better said, should be) guaranteed by Byzantine fault tolerant algorithms, programming is Turing-complete.

Smart Contracts are used in various types of transactions. Probably, the general public tends to associate them with the trade of Cryptocurrency, especially with Bitcoins. Indeed, the use of Smart Contracts is also widespread in the market of other Cryptocurrencies, like for example Ether. Moreover, Smart Contracts have been used for purposes different from the financial trade of Cryptocurrencies. Cryptocurrency-based Vouchers guaranteed by BlockChains have been used to provide support to Syrian refugees, are used to provide access to financial resources to persons living in areas not served by banks (or unable to pay the fees banks charge for their service), and can be used in the real estate market. Moreover, the technology underpinning Smart Contracts has a potential use in an activity like political elections as it is supposed to prevent fraud and abuse. The underlying mechanism is similar to the one at the base of Cryptocurrency use: a general ledger for votes and expression of political preferences.

Moreover, this type of ledger can also be used to render the whole healthcare sector more efficient.

The growing use of Smart Contracts and of the technology underpinning them (as said before, the terms “Smart Contract” takes a broader meaning going further than the scope of an agreement among willing parties) clearly creates a major need to ensure the safety of the whole system. Hackers and bugs represent a constraint and a threat for actors engaged in electronic transactions, especially when these particular transactions are irreversible and neither mediated nor controlled by any third party. This risk represents a major challenge for the use of Smart Contracts, and an attack to the safety of the whole system has happened in 2016 when the platform DAO was violated, draining 50 million dollars.

Academic research on Smart Contracts has been growing in recent years. As mentioned in the introduction, De Ridder et.al. (2017) have highlighted the fact that Smart Contracts are regulated by the Uniform Electronic Transaction Act and do not request specific regulating legislation (the next section will expand on this point). Mik (2017) has highlighted various technical and also legal limitations related to Smart Contracts, touching in part on the very core of our paper. Pop et al. (2018) discuss the applicability of Smart Contracts and Blockchain technology. Governatori et al. (2018) are studying specific technical-engineering aspects of Smart Contracts and their impact on the declarative language of Smart Contract architecture. Current research is interested in analysing the technological innovation of Smart Contracts, highlighting the advantages it has as for the simplification of transactions and at least the partial elimination of transaction costs. The legal controversies embedded with the use of Smart Contracts are not really at the core of the attention of scholars. Eventually, as said, De Ridder et al. (2017) have devoted some attention to the legal controversial aspects embedded with the use of Smart Contracts, suggesting that these aspects are currently under the scope of the Electronic Transaction Act. However, this piece of legislation regulates the validity of electronic signatures, establishes the principle of the general validity of electronic transactions, and provides directions regarding the solution of technical errors in the transmission and storage of electronic data. Other recent contributions, more focused on the legal dimension, have already been mentioned. However, they do not really focus particular problem of this present paper, namely the fact that an automatic enforcement of Smart Contracts may de facto deprive

parties affected by contractual vices of the possibility to invoke any legal redress. This issue will be discussed in the next section.

2 Validity of Transactions: How to Rectify a Vitiating Transaction?

Smart Contracts, in their narrow meaning, are intended as agreements between willing parties, as traditional contracts are. Nonetheless, the process of coming to an agreement may be marred by several factors which impact on the validity of the underlying contract. Consequently, contracts may be declared null or may be annulled by convened upon judicial authorities.

The first important limitation embedded in the use of Smart Contracts is, as touched upon above, the possibility of theft of identity, with hackers pretending being another person and using his/her money/assets. This problem is part of the wider challenge with safety of electronic transactions and is not really within the scope of our present section which is more focused on legal aspects. The evolution of computer science, more than legal standards, may provide a solution and limit the risks of appropriation of identity and on-line frauds. Here below, we will discuss two factors which undermine the validity of traditional contracts and the difficulties in invoking these specific factors to block the enforcement of Smart Contracts or reverse the transaction. These specific factors are lack of legal capacity (including declarations of insanity) and mistake.

A basic requirement of validity of contracts is the legal capacity of the persons acting. This is a point which can hardly be accounted for in transactions based on Smart Contracts. A person's legal capacity exists when the person has reached a minimal age (usually 18 years in Europe) and has not been incapacitated as a result of a mental disturbance or criminal conviction. These are factors which can eventually be controlled electronically. Eventually an agent acting through a Smart Contract may be asked to provide a certified digital certificate proving his/her own legal capacity. Age and deprivation of capacity are reported in appropriate documents which can eventually be provided to the counter party. There is a general risk of faking the documents; however this risk also exists when parties are transacting using traditional mechanisms.

Nevertheless, the vice of lack of capacity cannot be completely cured through the use of digital certificates. A person can act in a moment of mental disturbance independently of a previous legal declaration of incapacity. The validity of contracts is questionable when one of the party is not able to determine his/her own behaviour freely. Factors like intoxication from alcohol of

drugs, temporary insanity may definitely alter cognition mechanisms and influence the behaviour of persons. Current legal standards are that contracts are not valid *in toto*, or in part, when one of the party is acting without full control of his/her own decisional process, and this particular constraint is recognized or recognizable by the other party. The aggrieved party or its guardians may block the enforcement of the contract, pending a judicial decision or apply for a reversibility of the transaction.

From the picture provided in the previous sections, it appears that the automatic enforcement of Smart Contracts, the absence of any mediating third party, the anonymity of the parties involved seriously limits, or eliminates, the possibility of invoking temporary and undeclared incapacity. Contracts are self-executing and not reversible. Moreover, the lack of direct interaction between parties and the absence of any mediator renders the lack of capacity not recognizable by the other party. One may say that reversing a transaction marred by unrecognizable lack of capacity would be unfair towards the counterparty.

A second factor marring the validity of contracts is the so-called mistake. A mistake in contracts is the misunderstanding of essential terms and conditions of the very contract. This is possible even when parties are transacting through Smart Contracts. The general conditions governing the whole exchange (i.e. of Cryptocurrency) may be formulated unclearly or not be understandable to the average educated and reasonable person, let alone persons falling out of the standard. Hence, a person may enter into an exchange without having full cognizance of the act performed. Also in this case, and for the same reasons highlighted above when discussing the problem with capacity, the self-executing nature of Smart Contracts and their irreversible connotation clearly create a serious limit to any possibility of invoking mistake to prevent the enforcement of the agreements.

There would be other factors undermining the validity of contracts (i.e. duress), however the logic of the problem with legal validity as outlined above would not change substantially. The point is that Smart Contracts' self-executing and irreversible nature does not allow any aggrieved party to invoke standard vices which affect the validity of traditional contracts. In other words, the very presupposition of the existence of "wilful parties" is not verifiable and its absence not curable. At this stage, one may legitimately question the very contractual connotation of this type of transactions. The next step could be questioning the very legitimacy

of this type of operations. The issue appears even more serious because Smart Contracts have gained in popularity exactly because of their self-executing and irreversible nature. Eventually, an attempt to render their enforcement subject to judicial review (as done by the UK legislator), would deprive Smart Contracts of a meaningful part of their nature. Amending their functionality in order to take account of the necessity of curing legal vices would dramatically change the fundamental characteristics of these instruments and probably lead to a decline in their popularity. Finding a compromise appears difficult, because sacrificing the self-executing and irreversible nature of Smart Contracts would profoundly alter their essence and transform them into another instrument. On the other side, economic transactions entail legal consequences, and the lack of effective protection of parties whose decisional process has been affected by vices renders the organization of the whole system legally challengeable.

Conclusion

This paper has studied Smart Contracts and has discussed the legal implications of their automatic enforcement and of the non-reversibility of the transactions. The paper concludes by remarking how the lack of effective protection of parties whose agreement to the transaction may be contaminated by vices creates legal questions regarding the whole system of Smart Contracts. On the other side, Smart Contracts would lose their connotation if their functioning mechanism were fundamentally altered.

The contemporary evolution of Business and Finance creates challenges that require a careful re-thinking of traditional mechanisms, including mechanisms of safety. Anonymous and self-enforcing transactions have also disadvantages and finding a compromise can result being extremely tricky. Legislative interventions are surely necessary but the risk is to fundamentally alter the nature of some innovative forms of economic and financial transactions. Inventions contribute to the progress of Humanity and can prepare the soil for useful achievements. On the other side, inventions can also represent a break-up with the previously existing formal institutional set of rules and the solution may take time to come.

References

- Barbry, É. (2017). Smart contracts... Aspects juridiques !. *Annales des Mines - Réalités industrielles*, 2017, 77-80. <https://doi.org/10.3917/rindu1.173.0077>
- De Ridder, C.A., Tunstall, M.K., Prescott, N. (2017, June 1). Recognition of Smart Contracts. Pillsbury Law. <https://www.pillsburylaw.com/en/news-and-insights/recognition-of-smart-contracts.html>.
- Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, 45(2), 102081. <https://doi.org/10.1016/j.telpol.2020.102081>
- Frankenfield, J. (2021, May 26). Smart Contracts: What You Need to Know. Investopedia. <https://www.investopedia.com/terms/s/smart-contracts.asp>.
- Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, 26(4), 377–409. <https://doi.org/10.1007/s10506-018-9223-3>
- Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, 9(2), 269–300. <https://doi.org/10.1080/17579961.2017.1378468>
- North, D.C. (1990) *Institutions, Institutional Change and Economic Development*, Cambridge University Press, Cambridge.
- North, D.C. (2005) *Understanding the process of Economic Change*, Joel Mokyr Editor, Princeton.
- Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., & Bertoncini, M. (2018). Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids. *Sensors*, 18(2), 162. <https://doi.org/10.3390/s18010162>
- Quora. (2017, November 17). What Is Blockchain Used For Besides Bitcoin? Forbes. <https://www.forbes.com/sites/quora/2017/11/17/what-is-blockchain-used-for-besides-bitcoin/?sh=2fc3538446ee>.
- Smith, B. A., & Bechtold, T. L. (2019). When Smart Contracts Break: Developments in Blockchain, Smart Contracts, and Online Dispute Resolution. *The Computer & Internet Lawyer*, 36(11), 14–15.
- Schneider, L., Evans, J. B., & Kim, A. (2018). Why Blockchain Smart Contracts Matter. *International Financial Law Review*.

Wilkens R., Falk R. (2019) Aktuelle und geplante Anwendungsfelder. In: Smart Contracts. essentials. Springer Gabler, Wiesbaden. https://doi.org/10.1007/978-3-658-27963-9_4

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

Williamson, O.E. (1986) Economic Organization. Firms, Markets and Control, Wheatsheaf Books, Brighton.

Contact

Pietro Andrea Podda

Anglo American University

Letenská 5, 118 00, Prague 1

pietro.podda@aauni.edu

Pavel Macura

Anglo American University

Letenská 5, 118 00, Prague 1

pavel.macura@aauni.edu

Harold Neal

University of New York in Prague

Londýnská 41, 120 00 Praha

hneal@unyp.cz