Transaction Costs of Blockchain Smart Contracts

Jakub J. Szczerbowski

SWPS University of Social Sciences and Humanities

Law and Forensic Science, Volume 16 (2018/2).

Submitted: July 11, 2018

Abstract: Smart contracts are computer programs executed on virtual machines, which are used to regulate relationships between the subjects of law. They allow parties to foresee, with a high degree of certainty, how will the contractual relationship develop and by the use of blockchain technology they provide a high degree of certainty. It has been conjured that smart contracts will offer significantly lower transaction costs in relation to traditional contracts. The paper analyzes this proposition and finds that not only are the gains doubtful, but also that in some cases transaction costs may be significantly higher.

Keywords: smart contract, transaction costs, blockchain

Introduction

Smart contracts are computer programs executed on virtual machines, which use blockchain as its memory and are used to regulate relationships between the subjects of law. This simplistic definition implies, that what we already are used to in the realm of cryptocurrencies – namely transparency, immutability and irreversibility – gets transposed to the realm of relationships more complex than mere transfers of money-like units. Smart contracts are subject to limitations inherent to any computer program. They are deterministic and it is very hard to code general clauses like "reasonable care" into them (Sklaroff, 2017, p. 279). Smart contracts are also limited by the nature of blockchain based virtual machines used to run it, meaning they are not optimized for speed but for security (Dannen, 2017, p. 15). Because of these limitations smart contracts usually regulate simpler relationships than traditional contracts. In spite of those limitations smart contracts have potential to become useful devices able to supplant traditional contracts in some applications. It is also reasonable to assume that with rapid development in the field of all blockchain related technologies the above limitation will become less and less relevant. Smart contracts are traditionally related to the ideology of crypto-anarchism (see May, 1992) but their gradual acceptance by state actors makes this connection weaker. Still, it is one of the main arguments of smart contracts that the parties may enforce performance outside of the state-based justice system.

Smart contracts allow parties to foresee, with a high degree of certainty, how will the contractual relationship develop. This is made possible by the deterministic nature of software (Christidis & Devetsikiotis, 2016, p. 2297). Parties can audit the contract code and test how will it react to various circumstances (Peters & Panayi, 2016) as the code does only what it says – there are no implied terms.

Because smart contracts are "executed on blockchain" they are immutable (unless the code allows changes explicitly– this however is not the preferred way of doing business as the parties usually decide to use smart contracts to avoid changes). This feature of smart contracts ensures parties or third parties cannot tamper with the code and creates a sort of machine-based "trust" (Künnapas, 2016, p. 126).

Smart contracts are also irreversible meaning once they are deployed they will do exactly what they are programmed to do (Luu, Chu, Olickel, Saxena, & Hobor, 2016). This implies parties need to include the possibility of withdrawal in the contract code or they will be helpless in case of change of mind (Szczerbowski, 2018, p. 117). This feature of smart contracts is clearly problematic in scope of civil law rules on error as the voidability of smart contracts does not influence its performance. Also, this may lead to overenforcement by means of code in cases where parties would recognize the need to cancel the contract for efficiency reasons (Szczerbowski, 2018, p. 164).

Smart contracts may be used for various contractual relationships where the performances are possible to describe in a formal (quantitative) language (lack of open-textured terms; no expressions such as "will take all necessary steps to ensure *x*" or "will build according to the best practices" would be viable to cheaply translate into contract code.). The possible contracts include lotteries, options, crowdfunding, contracts related to digital assets, insurance and so on.

Because of their "speed" (they are "slow" compared to other software but still much "faster" than the traditional contracts) smart contracts give promise of reducing transaction costs (Levy, 2017, p. 393). This promise may, however, never be fulfilled (see Sklaroff, 2017). The goal of this paper is to discuss the possibilities of transaction costs reduction compared to traditional contracts. For the needs of this paper transaction costs are divided into (1) search and information cost, (2) bargaining and decision costs, (3) policing and enforcement costs (see Dahlman, 1979, p. 148).

Search and information costs

The cost of search and information includes cost of querying the market for potentially interesting deals (Vatiero, 2013, p. 46) and after finding such a deal to assess the risk connected with a particular contractor (Dyer & Chu, 2003, p. 2). Looking for a particular deal in traditional setting seems to be as costly as within the smart contracts framework. Means of querying the market are approximately the same in both cases (use of http protocol over the Internet).

On the other hand, getting to know one's perspective business partner incurs certain cost in traditional setting. Smart contract setting does not offer any advantage when it comes to acquiring knowledge about the other party but due to its particular characteristics (transparency, immutability and irreversibility) one may rest assured, that the contract will be performed as promised no matter the reputation and faith of the other party (see Cunningham, 2016, p. 236). This leads to a weak conclusion, that smart contracts offer reduction of transaction cost in this particular aspect.

Bargaining and decision costs

Bargaining costs are cost incurred by communication of preferences between the parties and by analyzing whether the proposal of one party fits the preferences of another party (commonly known as negotiations). One of the factors leading to increase of transaction cost in this aspect is the asymmetry of information. Information is asymmetrical if it cannot be verified at the same cost by both parties (Schwartz & Scott, 2003). The phenomenon of asymmetry of information may lead to parties suspecting the other party is withholding information, to take excessive precaution leading to inefficiencies. Because of similar mechanism working in both traditional and smart contracts it may be presumed, that the costs of bargaining are at a similar level.

Decision cost are the costs of determining whether the contract terms are mutually agreeable. There are various mechanisms of lowering the decision costs, one particularly significant are adhesion contracts, where the terms

of contract are defined by one party and the other may only decide take the offer or leave. This phenomenon usually implies inequality of bargaining power.

Posner proposed to describe transaction cost in contract by

$$C = x + p(x)[y + z + e(x, y, z)]$$

where *C* is the total amount of transaction costs, *x* are costs of negotiations and decision incurred by the parties, *y* are the costs of litigation, *z* are the costs incurred by the state, *p* is the probability of a lawsuit and *e* is the cost of error (Posner, 2004). It is significant, that error cost depends on the costs incurred by all the interest subjects. It is a well a known fact that "small" mistakes in contract code may lead to huge economic losses for the parties; a fact most proven by the famous The DAO hack (DuPont, 2017; Mehar et al., 2017; Wojdyło, 2016).

As smart contracts strive to provide enforcement outside the judiciary one might be tempted to omit the second term of the right side of the equation leaving $C = x$. This conclusion is clearly absurd as it would mean that complete lack of attention to the contract code (zero-cost) could lead to efficient results. A correct solution, allowing the assumption of state-less enforcement, considers the relationship between decision cost and the probability of errors:

$$C_s = x_s + p(x_s)e_s(x_s)$$

(subscript *s* for costs relating to smart contracts). If we however, do not assume smart contracts exist outside of the legal system the transaction costs would have to include both costs of $x_s + p(x_s)e_s(x_s)$ and the cost of judicial enforcement:

$$C_s = x_s + p(x_s)e_s(x_s) + q\big(p(x_s)e_s(x_s)\big)[y + z + e(x_s, y, z)]$$

This conclusion allows to further deduce that the decision cost for smart contracts are higher than the same in relation to traditional contracts.

Policing and enforcement costs

Policing costs are the resources used to check if performance was done in accordance with the agreement. Transparency and determinism of smart contract may lure us to conclude the contract costs would be significantly lower. Some authors opine smart contracts have much lower policing costs than traditional contracts (Sklaroff, 2017, p. 275). I do not share this opinion. It is necessary to compare apples with apples, i.e. the contracts of same content concluded both as smart contracts and as traditional contracts. For example, and exchange of one cryptocurrency for another may be accomplished in both ways. This example clearly shows the policing cost would be roughly equal.

Enforcement cost are the resources used to remove the discrepancy between what was promised and what was performed. This cost has to be analyzed in two variants (1) assuming state-less enforcement, (2) allowing for court dispute of the result of code execution. In first variant, the cost of enforcement is equal to the cost of mistakes in code; i.e. a perfect code would allow for practically costless enforcement. In the second variant, I dare say a more probable one, the cost of enforcement seems lower than in traditional contracts. This is caused by the transparency and immutability of records related to particular smart contracts. In traditional contractual setting events are subject to proof (witness testimony, counterfeit documents). Blockchain allows to ensure perfect records so the case would be "law-bases" not "fact-based", and factfinding is the most resource hungry part of civil procedure.

Conclusion

The analysis lead to two areas where transaction costs are lower in smart contracts than in traditional contracts. First are the costs of information about the other party – which are substituted by the costs of auditing the code. Second are the costs of enforcement which are lowered because of the near perfect information about the "history" behind contract performances.

Decision costs (cost of drafting the contact) seems to be significantly higher for smart contracts. This observation is further confirmed by the efforts to make smart contracts drafting easier (see Clack, Bakshi, & Braine, 2016). It is also proposed, that the switch from imperative programming languages to declarative programming languages may make smart contracts less prone to errors (Governatori et al., 2018, Chapter 4).

The difficulty of drafting smart contracts is directly related to risk created by any code mistakes. Outside of blockchain software is being constantly patched and updated – this shows that even for experienced professional it is normal to make code errors. As the contract code is immutable the cost of auditing and testing the code is significantly higher, it may even exclude the feasibility of complex smart contracts (due to exponential probability of error in relation to the size of the code).

References

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303.

Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart Contract Templates: Foundations, Design Landscape and Research Directions. *ArXiv:1608.00771 [Cs]*. Retrieved from http://arxiv.org/abs/1608.00771

Cunningham, A. (2016). Decentralisation, Distrust & Fear of the Body – The Worrying Rise of Crypto-Law. *SCRIPTed*, *13*(3), 235–257. https://doi.org/10.2966/scrip.130316.235

Dahlman, C. J. (1979). The Problem of Externality. *The Journal of Law and Economics*, *22*(1), 141–162. https://doi.org/10.1086/466936

Dannen, C. (2017). *Introducing Ethereum and Solidity*. Retrieved from http://link.springer.com/content/pdf/10.1007/978-1-4842-2535-6.pdf

DuPont, Q. (2017). Experiments in Algorithmic Governance: A History and Ethnography of "The DAO," a Failed Decentralized Autonomous Organization. In *Bitcoin and Beyond: Cryptocurrencies, Blockchains and Global Governance*. New York.

Dyer, J. H., & Chu, W. (2003). The Role of Trustworthiness in Reducing Transaction Costs and Improving Performance: Empirical Evidence from the United States, Japan, and Korea. *Organization Science*, *14*(1), 57–68. https://doi.org/10.1287/orsc.14.1.57.12806

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*. https://doi.org/10.1007/s10506-018-9223-3

Künnapas, K. (2016). From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda? In *The Future of Law and eTechnologies* (pp. 111–131). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-26896-5_6

Levy, K. E. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Engaging Science, Technology, and Society*, *3*, 1–15.

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart Contracts Smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 254–269). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2978309

May, T. C. (1992). The Crypto Anarchist Manifesto. Retrieved October 25, 2017, from https://www.activism.net/cypherpunk/crypto-anarchy.html

Mehar, M., Shier, C., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., … Laskowski, M. (2017). *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack* (SSRN Scholarly Paper No. ID 3014782). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=3014782

Peters, G. W., & Panayi, E. (2016). Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In *Banking Beyond Banks and Money* (pp. 239–278). Cham: Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-42448-4_13

Posner, R. A. (2004). The Law and Economics of Contract Interpretation. *U Chicago Law & Economics, Olin Working Paper*, (229). Retrieved from http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=610983

Schwartz, A., & Scott, R. E. (2003). Contract Theory and the Limits of Contract Law. *The Yale Law Journal*, *113*(3), 541–619. https://doi.org/10.2307/3657531

Sklaroff, J. M. (2017). Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, *166*, 263.

Szczerbowski, J. J. (2018). *Lex cryptographia. Znaczenie prawne umów i jednostek rozliczeniowych opartych na technologii blockchain*. Warszawa: PWN.

Vatiero, M. (2013). Law, Transaction Costs and Coase's Institutions. A Reappraisal. *Economia e Politica Industriale*. https://doi.org/10.3280/POLI2013-004006

Wojdyło, K. (2016). DAO a prawo karne. In J. Zandberg-Malec (Ed.), *Nowy raport: Blockchain, inteligentne kontrakty i DAO | Co do zasady*. Warszawa: Wardyński i Wspólnicy. Retrieved from http://www.codozasady.pl/nowy-raport-blockchain-inteligentne-kontrakty-i-dao/