THE LEGAL FRAMEWORK AND CHALLENGES OF
SMART CONTRACT APPLICATIONS

Dr. Maciej Hulicki
Faculty of Law and Administration
Cardinal Wyszyński University in Warsaw
m.hulicki@uksw.edu.pl

Abstract
The subject matter of this paper concerns the emerging solutions based on blockchain type
distributed ledgers. This topic is analysed from the legal perspective, and its goal is to
indicate potential challenges that such technology may generate for the legal system. In
particular this study is focused on smart contracts that are based on such solutions. A
distinctive feature of smart contracts is their capability of self-execution. The current legal
framework does not regulate specifically such contracts. Together with the practical
evolution of this concept regulatory intervention is very likely. It is however possible that
smart contracts will eventually be self-regulated. Extreme utility of such solutions
challenges the hitherto understanding of contractual obligations. Moreover, the interplay of
computer algorithms and terms of the contract should be further surveyed, as the latter can
be significantly influenced by the programing code.

1. Introduction – blockchain and
smart contracts
This paper contains an analysis of the
subject matter of blockchain technology and
its implications for the legal domain. In
particular it considers development of the
smart contracts idea. Hence, it is first
necessary to introduce and shortly describe
most important notions, which are used in
the paper.

The concept of blockchain was introduced
in 2008 by Satoshi Nakamoto, who is the
creator of the fist digital currency (bitcoin)¹.
Although bitcoin is a currency, its
architecture provides a global system of
electronic commerce transactions, which
safeguarded by decentralized cryptographic
mechanisms, as opposed to trust to central
institutions, as in regular transactions², ³.
Yet, this architecture is overarching matters
such as digital currencies or e-commerce.
Decentralized structure democratized the
transaction process in a sense that each user
has insight into entire history of transactions,
but simultaneously the anonymity is not
compromised, since the users are visible
through the public key⁴. However, most of
all the democratization manifests itself
through exchange of actors. Namely, it
provides a system without a central

¹ S. NAKAMOTO, Bitcoin: A Peer-to-Peer
Electronic Cash System.
² Z. ZHENG, S. XIE, H.N. DAI, H. WANG,
Blockchain Challenges and Opportunities: A
Survey, International Journal of Electric and
Hybrid Vehicles, 01/2017.
³ Hence blockchain may be regarded as the
central trust machine. See: J. BERKLEY, The
promise of the blockchain The trust
⁴ M.HULICKI, PLUSTOFIN, Wykorzystanie
koncepcji blockchain w realizacji
zobowiązań umownych, Człowiek w
cyberprzestrzeni, forthcoming.
institution responsible for authentication of a conducted transaction, as its verification is done through a consensus, meaning that more than half of the system users (nodes) must confirm it\(^5\).

Blockchain is therefore a dispersed database stored in the chain of blocks. A single entity does not control such ledger, but instead all users of this decentralized system fulfil that role \(^6\). Furthermore, blockchain type solutions are characterized by irreversibly of the transactions done through it\(^7\)\(^8\).

Technology based on blockchain can have numerous applications. In particular, solutions currently being developed involve such areas as banking, finance, health, network connectivity, public sector, security, and authentication systems.

Smart contracts are the next step in the development of blockchain technology. The above-described technology allows for automatic execution of the contract by a computer program when a consensus has been reached. This implies remote, complete, and swift performance of the contractual obligations. Hence, this technology enables programming of various transactions, implementing certain business logics\(^9\). In consequence, smart contracts exerting the blockchain technology can allow for a system of digital and open transactions between network users within a decentralized database\(^10\).

Some authors suggested even a new term: „lex cryptographia”, to denote an emerging branch of law comprising self-enforcing contracts and decentralized autonomous organizations \(^11\). They claim that the distributed ledgers can yield a new digital revolution connected with decentralization of the Internet. For the legal environment this would be a breakthrough that can be compared to the invention of the print\(^12\).

The process of automation of law seems to be inevitable. Its implementation through utilization of blockchain technology can dramatically change the legal practice, and even social relations. However, it needs to be stated upfront that these solutions are in a very early stage of development therefore a

\(^5\) Ibid.
\(^6\) Ibid.
\(^7\) S. NAKAMOTO, op. cit.
\(^8\) Currently three main solutions based on blockchain can be identified: public, corporate, and private. The key difference between them is the level of trust between the users of a certain system, from low in public to high in private systems. These differences are reflected in the structure of these solutions and authority to induct changes to the ledger. See: M.HULICKI, P.LUSTOFIN, op. cit.

\(^9\) Ibid.
\(^11\) Such organizations are in fact advanced programming codes having smart contract features, which can autonomously manage their assets, make decisions and interact with other entities. See: K. PIECH (ed.), Leksykon pojęć na temat technologii blockchain i kryptowalut, 08.11.2016.
precise assessment of their impact is untimely.

2. Regulatory framework and some legal issues arising with respect to the blockchain based smart contracts (from the perspective of the Polish legal system)\textsuperscript{13}

2.1 Introductory remarks

Blockchain has a substantial potential of application in the domain of executing contractual obligations and indeed numerous institutions conduct R&D projects in this regard\textsuperscript{14}. Employing blockchain architecture allows generation of smart contracts that enable full automation in determining and enforcing contractual provisions without interaction of the third party.

The concept of smart contract – as defined by its originator Nick Szabo – denotes computerized transaction protocol executing terms of the contract \textsuperscript{15}. An alternative definition encompasses a computer program capable of making decisions when certain preconditions are met\textsuperscript{16}.

Implementation of such smart contracts can be executed through a bitcoin-alike blockchain solution, yet their introduction is feasible also with the help of other forms of distributed ledgers \textsuperscript{17}. Since, blockchain is relatively a novel idea, and its utilization in the legal domain is still under development, its specific applications can differ significantly. Hence, this paper contains a syntactical analysis that could induce further discussions on this matter by signalizing some of the key issues that may arise due to its implementation.

2.2 Lack of Regulation

New technologies always pose a challenge for the rigid legal regulations. The law is often not adapted to the pace of socio-economical changes related with a new technology. At the same time, without hindsight it is burdensome to assess and predict the true impact of new solutions. Notwithstanding the positive side of introduction of a new technology, it usually entails some kind of hazards.

The matter of blockchain exploitation does not seem to be regulated and so far does not

\textsuperscript{13}Although this paper refers primarily to the Polish legal system, the normative situation should not differ significantly in other jurisdictions, since in the current stage of blockchain and smart contracts evolution most of deliberations are still very general. 
\textsuperscript{15}D. HE (et. al.), Virtual Currencies and Beyond: Initial Considerations, International Monetary Fund, 01/2016, SDN/16/03 citing N. Szabo, Smart Contracts, 1994.
\textsuperscript{17}The architecture of the bitcoin system could be applied to manage transfers of any kind of digital assets, and also other goods, which are connected to the network/system and utilize the blockchain technology. See: P. FRANCO, Understanding Bitcoin: Cryptography, engineering and economics, Chichester 2014, pp. 183-186.
require regulatory intervention. From the formal point of view, the application of blockchain solution is not directly regulated in Polish legal system. There are also no provisions that could lead to its special normative qualification. Thus, exploitation of this solution is perfectly licit, since the legislation does not differentiate the legal situation of this solution ("quod lege non prohibitum, licitum est")\(^\text{18}\).

Most of the studies are focused on the most prominent instance of the blockchain idea, i.e. bitcoin system. A comparative analysis shows that even in this area in most jurisdictions the crypto-currency remains unregulated. However, in minority of cases the regulations concerning utilization of crypto-currencies have a restrictive character\(^\text{19}\). The legal situation of bitcoin in the European Union is clearer after the judgment of Court of Justice, which has considered bitcoin as a mean of payment\(^\text{20}\). However, it must be noted that considerations regarding bitcoin concern the issue of crypto-currencies not the application of blockchain technology itself, on which these means are build. Therefore, in its current stage and in case of lack of specific legal regulations this technology should not be legally qualified differently from other IT tools\(^\text{21}\). Since in the free-market economies parties usually have contractual freedom, they could decide, to exploit the blockchain enabled automation of obligation enforcement. Naturally, the current legislative measures to safeguard the interest of consumers, data protection and other provisions relevant for e-commerce will have their respective application to blockchain based smart contracts\(^\text{22}\).

The current legal framework in Poland is sufficiently prepared to encompass blockchain solutions and at present no special needs for adjustment of legal regulations exist in this respect\(^\text{23, 24}\). However, presumably for the time being regulatory attention should be concentrated on ensuring a so-called regulatory sandbox, comprising legal regulations facilitating start-up R&D activity dedicated to blockchain technologies\(^\text{25}\).

Whereas it can be expected that many aspects of blockchain technology will become self-regulated likewise the

---

\(^{18}\)M.HULICKI, P.LUSTOFIN, op. cit.

\(^{19}\)G. SObIECKI, Regulowanie Bitcoina, Międzynarodowy Kongres Płatności Bezgotówkowych, 03/2015.

\(^{20}\)Judgement of the Court of 22.10.2015 in Skatteverket v David Hedqvist (C-264/14).

\(^{21}\)M.HULICKI, P.LUSTOFIN, op. cit.

\(^{22}\)Ibid.

\(^{23}\)K. ZACHARZEWSKII, K. PIECH (ed.), Przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych, Stanowisko Strumienia w sprawie kierunków ewentualnych prac legislacyjnych oraz działań regulacyjnych instytucji publicznych, 19.01.2017.

\(^{24}\)Some of the blockchain projects, which are currently being realized, include necessity of normative analysis and consideration of possible legislative amendments. See: M. GARSTKA, K. PIECH (ed.), op. cit.

\(^{25}\)Since these entities take a substantial risk to produce novel solutions they should be ensured a safe legal ecosystem. See: K. ZACHARZEWSKII, K. PIECH (ed.), op. cit.
Internet\textsuperscript{26}, one can suppose a regulatory interest parallel to the progress of smart contracts development. In the first place, elimination of a trusted intermediary from the transaction process will challenge rules regulating it\textsuperscript{27}.

2.3 Legal status of smart contracts

Another potential issue that rises in relation to the formal side of smart contracts is their legal status and their connection to the actual legal contract? Smart contracts do not need to be actual legal contracts that are concluded between the parties. They can coexist independently. For the smart contract to become a legal contract it is necessary to fulfil the legal requirements of a contract, in particular a mutual intent of the parties to be bound by such contract with all legal consequences \textsuperscript{28}. Specific qualification of smart contracts will depend on their practical implementation into a actual solution\textsuperscript{29}. Therefore, smart contracts may be merely used as a tool for contract enforcement beside the actual legal contract, or enable a mechanism that will transform the agreement from its smart version to a

27 The potential requirement of authentication by the trusted third party for transaction to take place can be eliminated through distributed ledgers and decentralization of the verification process.
28 M. KÖLVART [et al.], op. cit., p. 135.

physical document written in a natural language\textsuperscript{30}.

2.4 “Extreme” utility

One of the most inquiring aspects of smart contracts is their utmost utility. One can indicate this utility throughout the entire lifecycle of the contract, but the distinctive feature is their capability of self-enforcement. Namely, it facilitates parties to the contract in completing the transaction process in a very efficient way. Hence, utility of such solutions is often regarded as one of the main advantages that the smart contracts can entail\textsuperscript{31}. In fact, if the smart contract follows the premise of self-enforcement parties do not have the freedom to breach the conditions of the contract, as it is executed remotely and in real-time. Naturally, this feature could carry a significant relief for the judicatory and enforcement system\textsuperscript{32}.

31 According to the report of the International Monetary Fund the main advantages of the smart contracts are their speed, efficiency, and certainty of enforcement. See: D. HE (et. al.), op. cit., p. 23. Other benefits may include lower transaction costs, greater confidentiality and control of the transaction process.
32 It may be a risk that the smart contracts may entail, as freedom to breach contractual terms is a part of traditional contracts whose enforcement takes place \textit{ex post}, and breach of which is sanctioned, e.g. by damages. In this sense impossibility of contractual infringement may be seen as a limitation of parties’ freedom and autonomy. A. WRIGHT, P. DE FILIPPI, op. cit., pp. 26, 43.
2.5 Code is law

The “extreme” utility of smart contracts derives from the essence of such solutions, i.e. them being in fact nothing else than an algorithm. Such contracts are expressed in a specific programming language that constitutes the substance of the legal norms.

What follows from above is that smart contracts in order to fulfil their role must have precise algorithms underlying them. Otherwise these solutions would not entail expected benefits, as they will provide a room for potential abuses. Hence, the correctness of the code is essential for ensuring the legal certainty that the program will execute the intent of the parties accordingly to the terms of the contract. The transfer of programming code to the terms of the contract involves another problem, i.e. lack of common understanding of the programming languages. Hence, creating and understanding a smart contract may require comprehensive programming knowledge that for ordinary consumers could be unsuitable. Some authors argue that true implementation of smart contracts would require employment of artificial intelligence, but such statement in the light of current state of art seems disputable. Smart contracts to fulfil their basic functions do not need involvement of advanced semantics. The meaning of the contract in terms of specific actions that need to be taken by parties would be conducted by mere operational semantics. However, the advanced semantics - involving necessarily legal knowledge for interpretation of contractual terms - would be engaged only incidentally, e.g. in a case of legal dispute.

The code itself may also be defective. This would disable the execution of the contract or derail the mutual intent of the parties, and could also allow hackers to exploit it. Hence, self-enforcement of contracts without control and potential engagement of third party seem not readily available.

3. Conclusions

Blockchain technology can prove to be a game changer in the area of law due to implementation of smart contracts. Their distinctive feature, i.e. self-enforcement, provides enormous potential for exploitation in the economy. Even though, the current state of play concerning development of such solutions is still in its early phase, one can expect considerable impact of this technology on the legal area.

34 T. SIMONITE, Bitcoin's dark side could get darker, 13.08.2015, MIT Technology Review.
35 D. HE (et. al.), op. cit.
36 M. KÖLVART (et al.), op. cit., p. 135.
37 See also: L. LAUSLAHTI (et al.), op.cit., p.3.
38 C. CLACK (ET AL.), Smart contract templates: foundations, design landscape and research directions, p. 5.
39 Such situation took place with respect to the DAO institution. Defective code allowed a hacking attack in 2016 when $55 million were stolen.
40 M.HULICKI, P.LUSTOFIN, op. cit.


Within the legislative framework such technologies are not qualified distinctively from other IT solutions. In such early stage of development there are neither special regulations concerning it nor there is a need to introduce such. It is not yet know whether blockchain will follow the Internet-kind model of self-regulation or it will be soon an interest of regulators, e.g. in providing a supportive legislative ecosystem for R&D in this area.

The blockchain based smart contracts may be implemented in numerous ways, and so it is premature to prejudge their relation to actual legal contracts concluded by the parties. They may overlap, but they could also be independent from each other and in such sense smart contract would be simply IT tool used to assist in transactional process, contract management and enforcement. Nevertheless they entail an “extreme” utility, which can unburden parties and enforcement institutions, but which can limit the freedom of the parties.

Smart contracts produce a situation where programming code is becoming law. This transformation has significant meaning for the understanding of contractual obligations. Algorithms on which the smart contract is based need to be precise enough to avoid abuses and defections.