Routledge
Taylor & Francis Group

Information & Communications Technology Law

ISSN: 1360-0834 (Print) 1469-8404 (Online) Journal homepage: http://www.tandfonline.com/loi/cict20

Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law

Alexander Savelyev

To cite this article: Alexander Savelyev (2017) Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law, Information & Communications Technology Law, 26:2, 116-134, DOI: 10.1080/13600834.2017.1301036

To link to this article: https://doi.org/10.1080/13600834.2017.1301036

INFORMATION & COMMUNICATIONS TECHNOLOGY LAW, 2017
VOL. 26, NO. 2, 116–134
https://doi.org/10.1080/13600834.2017.1301036

Routledge
Taylor & Francis Group

Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law

Alexander Savelyev[a,b]

[a]Faculty of Law, National Research University Higher School of Economics, Moscow, Russian Federation; [b]IBM Russia/CIS, Moscow, Russian Federation

ABSTRACT

The paper analyzes legal issues associated with the application of existing contract law provisions to so-called Smart contracts, defined in the paper as 'agreements existing in the form of software code implemented on the Blockchain platform, which ensures the autonomy and self-executive nature of Smart contract terms based on a predetermined set of factors'. The paper consists of several sections. In the second section, the paper outlines the peculiarities of Blockchain technology, as currently implemented in Bitcoin cryptocurrency, which forms the core of Smart contracts. In the third section, the main characteristic features of Smart contracts are described. Finally, the paper outlines key tensions between classic contract law and Smart contracts. The concluding section sets the core question for analysis of the perspectives of implementation of this technology by governments: 'How to align the powers of the government with Blockchain if there is no central authority but only distributed technologies'. The author suggests two solutions, neither of which is optimal: (1) providing the state authorities with the status of a Superuser with extra powers; and (2) relying on traditional remedies and enforcement practices, by pursuing specific individuals – parties to a Smart contract – in offline mode.

KEYWORDS

Contract; obligation; Blockchain; Bitcoin; Smart contract

Day by day, however, the machines are gaining ground upon us;
day by day we are becoming more subservient to them;
more men are daily bound down as slaves to tend them,
more men are daily devoting the energies
of their whole lives to the development of mechanical life.
The upshot is simply a question of time,
but that the time will come when the machines
will hold the real supremacy over the world and its inhabitants
is what no person of a truly philosophic mind can for a moment question. (Samuel Butler, 1863)

The future is already here – it's just not very evenly distributed. (William Gibson, 1993)

CONTACT Alexander Savelyev alexandersavelyev83@gmail.com

1. Introduction

The beginning of the twenty-first century revealed multiple innovative technologies which have produced a substantial impact on the new data-driven economy. The most notable of these are: Cloud Computing, Big Data, the Internet of Things, Augmented Reality, and Blockchain. The latter technology, initially introduced as a technological backbone of cryptocurrency Bitcoin, has started to have a significance of its own. Governments and companies all over the world are puzzling over the possible implementation of Blockchain technologies in many areas of life, not associated with the use of cryptocurrency. One of most promising areas of implementation of Blockchain technology is its use for creating fully automated contracts – agreements which are performed without human involvement. Such agreements in the IT-environment are frequently referred to as 'Smart' contracts.

2. What is Blockchain?

This is perhaps the first question which a person faces when coming for the first time to address the issues relating to 'Smart' contracts. In order to answer it, one has to understand the origin of this technology which is inseparably linked with the Bitcoin cryptocurrency, and forms the core of its technological infrastructure.

Bitcoin was developed by an unidentified programmer, or group of programmers, under the name of Satoshi Nakamoto, who is indicated as an author of a White paper describing the basics of functioning of Bitcoin.[1] In the most general terms, Bitcoin can be described as a decentralized, open-source, software-based, peer-to-peer, electronic currency. The key features of Bitcoin can be summarized as follows:

(1) *Decentralized nature*. Bitcoin does not have a centralized emission center or any trusted central authority. Maintenance of the Bitcoin transactions is performed by a network of communicating nodes running special software. From a technical perspective, Bitcoin as a currency unit is nothing more than a computer file, created on the basis of a special algorithm processed on computing power belonging to the Bitcoin community members. Even the Bitcoin protocol developers do not have control over Bitcoin-related transactions. Since the relevant code is distributed on the terms of MIT open-source license, it is available for inspection by any interested person, and is subject to the possibility of modifications, which can become a standard only if accepted by the majority of the community.
(2) *Anonymous nature*. One can use Bitcoin without any special registration or identification procedure. It is sufficient to install a special wallet application to enable one to initiate transactions with Bitcoin. Each wallet consists of Bitcoin units, a public key and a private key. The private key is used for transfer of a Bitcoin unit by its owner to another user's wallet. Without knowledge of the private key, the transaction cannot be signed and the Bitcoin unit cannot be spent.[2] The public key is used by other persons to send Bitcoin units to the recipient user's wallet, and is used by the

[1]Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, p 3. < www.bitcoin.org>.
[2]From a technical perspective, it is possible to state that ownership of a Bitcoin unit amounts to knowledge of the private key.

Bitcoin network for verification of transactions. Thus Bitcoin is a pseudonymous currency, in the sense that funds are not tied to real-world entities but rather to specialized addresses. Their owners are not explicitly identified, but all transactions on the Blockchain are public.

(3) *Mathematic algorithm as a basis of Bitcoin value*. There is no specific intrinsic value in Bitcoin, similar to commodities with limited availability such as gold, nor is there governmental authority (as in fiat money) behind it. However, this does not mean that Bitcoin does not have anything backing up its value. It is backed by mathematics, cryptography, and computer code. Bitcoin units are created during a process known as 'mining'. Each person who has installed specialized software may 'mine' a Bitcoin unit as a reward for solving a complex mathematical problem, associated with verification of transactions performed with Bitcoins. The complexity of such problems is growing, together with the amount of transactions performed in the Bitcoin network. In other words, emission of new Bitcoin units is a result of performance of computing activities to the benefit of the whole Bitcoin community. The overall number of Bitcoins is defined by the protocol and amounts to 21 million units. Since computational power is a valuable and limited resource, having intrinsic costs (e.g. for hardware involved and electricity), and Bitcoin has limited availability, which is ensured by mathematic algorithms, it is possible to claim that Bitcoin has some value behind it.

(4) *Absence of single administrator of transactions*. It is a well-known fact that electronic money is subject to the risk of double-spending.[3] Unlike physical coins, electronic money (like any computer data) can be duplicated and thus be used more than once. Traditional electronic money systems prevent double-spending by having a centralized trusted administrator which follows established process for authorizing each transaction. The problem with this solution is that the fate of the entire money system depends on the company running the administrative function, with every transaction having to go through them, just like a bank. Bitcoin resolves the double-spending problem by using a peer-to-peer network, and this is where Blockchain technology plays the key role. All the transactions ever performed with all Bitcoin units are included in a publicly available database. Information about a new transaction with Bitcoin is distributed through the network, is verified by miners, and then is fixed with indication of the time it was made (the timestamp) and the unique number of the Bitcoin unit. Thus, it is possible to trace the entire history of transactions with each particular Bitcoin unit in the database of all the transactions with Bitcoin – the Blockchain.

(5) *Resilience to data manipulations from outside*. Cryptography used in the process of creating records on Bitcoin-related transactions in the Blockchain database prevents tampering with the content of such records and ensures their perpetual nature. Whenever two people exchange Bitcoin units, an encrypted record of the transaction is sent out to all other nodes in the Bitcoin network. The other nodes verify the transaction by performing complex cryptographic calculations on the data in the record ('mining'), and notify one another each time a new 'block' of transactions is confirmed as legitimate. When a majority of the nodes agree that a block passes review, they all add it to

[3]See, for example, G Schneider, *Electronic Commerce* (8th edn Cengage Learning, 2008) 522 ff.

the Blockchain database and use the updated version as a cryptographic basis for encrypting and verifying future transactions. Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known. Each block is also computationally impractical to modify once it has been in the chain for a while, because every block after it would also have to be regenerated. Thus, it is not possible to rewrite information about certain transaction once it is included in the Blockchain. Such information will be rejected by the network, unless the intruder possessed more than 50% of the overall computational power of the Bitcoin network.[4] As a result, all the members of the Bitcoin community have a single version of 'truth', which is irreversible. Each participant to a transaction has a copy of the Blockchain database, and this is synchronized with the others' copies by the use of a specialized algorithm. All this creates an unprecedented level of trust between the users of Bitcoin, the Blockchain being the core element facilitating such trust.

Most of the features of the Bitcoin cryptocurrency are facilitated by Blockchain technology. However, the potential of this technology goes far beyond facilitation of decentralized electronic payments. To name a few examples from other spheres, there are existing prototypes of solutions, built on Blockchain technology, facilitating electronic voting in the sphere of corporate governance. The Russian national payment depositary has created a distributed database of votes, protected by cryptographic measures. Copies of this database are stored by all the shareholders and, as developers claim, cannot be falsified. Regulators or auditors may receive all the necessary information for performance of supervisory functions simply by connecting to the database.[5]

There are potential applications for Blockchain technology within the real estate industry. Once information on the title to a piece of real estate is in the Blockchain, the owner can transfer the property without any further interaction with the registry. Moving forward, each new transfer of property would add to the chain of title on the Blockchain. A Blockchain-based land registration system (in conjunction with associated business process changes) has the potential to decrease insurance premiums.[6]

Finally, Blockchain may be used for creating a new contracting environment, where the contracts are performed, or even both concluded and performed, automatically, without human involvement, or at least with substantially minimized involvement.

Based on the above explanation, Blockchain can be defined a decentralized distributed database of all verified transactions that take place across a P2P-network system operating on cryptographic algorithms. Its value can be characterized by the following two core enablers: (1) it allows the transfer of a digital asset (or a virtual representation of a physical offline asset) in a way that (2) facilitates disintermediation of the economy by allowing the maintenance of truthful records about the asset owners without involvement of a trusted intermediary (registrar, financial institution, notary, etc.). Blockchain ensures equal access to transparent and trustworthy information. Not surprisingly, this potential is already

[4]T Swanson, *Great Chain of Numbers* (2014) 18 <https://goo.gl/IBDVE5>.
[5]CNews, *NSD Tested a Blockchain-Based E-Proxy Voting Prototype* (29 April 2016) <https://www.nsd.ru/en/press/pubs/index.php?id36=629089>.
[6]A Spielman, *Blockchain: Digitally Rebuilding the Real Estate Industry* (2016) <http://dci.mit.edu/assets/papers/spielman_thesis.pdf>.

recognized. According to a World Economic Forum report, by 2027 around 10% of the world's GDP will be concentrated in Blockchain-based technologies.[7]

Now it is time to proceed to analysis of 'Smart' contracts as one of the most promising implementations of Blockchain technology.

3. Definition of 'Smart' contract and its key features

Contract law is one of the most dynamically developed areas of law. It constantly evolves, responding to the appearance of new business models and technologies. Based on the analysis of the evolution of the methods of contracting and the shape of the freedom of contract principle, it is possible to argue that each type of society has its own predominant form of contracting.[8]

Agrarian economies were mostly dominated by individually agreed contracts where the parties to the contract negotiated 'at arms length' all its terms. Industrial society is dominated by more simplified form of contracting using standardized terms, which allow mass-market contracting with minimized human involvement in the negotiation process and lower transaction costs. The information society will tend to go further by minimizing human involvement not only in defining the contractual terms but also in their performance. Moreover, new types of agreement may be also concluded without direct human involvement, by electronic agents. 'Smart' contracts are a good example of the development of contracting procedure in this direction.

There is no universally agreed definition of 'Smart' contracts, what is not a surprise, both in view of the very novel nature of this phenomena, and of its complex technological basis. According to the simplest definition, a Smart contract is an agreement whose performance is automated. According to Nick Szabo, one of the pioneers in analysis of automated self-performed agreements, a Smart contract is a computerized transaction algorithm, which performs the terms of the contract.[9] However, this definition may hardly identify the difference of 'Smart' contracts from some already well-known contractual constructs implementing automated performance, such as vending machines.

Vending machines are defined as self-contained automatic machines that dispense goods or provide services when coins are inserted or payment in other forms (e-cash, credit card) is made. Vending machines are programmed with certain rules that could be defined in a contract, and perform such rules.

If there is no difference in principle between vending machines and Smart contracts, then we will have to admit that Smart contracts are almost as old as Roman law itself. The earliest known reference to a vending machine is in the work of Hero of Alexandria, a first-century AD Greek engineer and mathematician. Hero Ctesibius (sometimes referred to as Heron) of Alexandria documented the first vending machine in the published journal entitled *Pneumatika* in 62 AD. His machine accepted a coin and then dispensed holy water. When a-five-Drachma piece deposited in, it was exchanged for a small supply of holy

[7]'Deep Shift. Technology Tipping Points and Societal Impact', *World Economic Forum* (Survey Report 2015) 24.

[8]Using the level of development of contract law as a litmus paper for assessing the degree of maturity of the society has a long tradition, leading to the famous statement by Henry Maine, according to which civilization's progress can be generally determined as a movement from 'status to contract'. See, H Maine, *Ancient Law: Its Connection with the Early History of Society and its Relation to Modern Ideas* (London, 1920) 151.

[9]N Szabo, *Smart contracts* in *Essays on Smart Contracts, Commercial Controls and Security* (1994) <http://szabo.best.vwh.net/smart.contracts.html>.

water in Egyptian temples. The lever opened a valve which let some water flow out. The pan continued to tilt with the weight of the coin until it fell off, at which point a counterweight snapped the lever up and turned off the valve.[10] So, a contemporary vending machine is based on a piece of technology that is nearly 2000 years old.

Acknowledging the well-known statement that there is nothing new under the sun, it is still necessary to analyze whether or not there is something new in principle in Smart contracts as compared to automated vending machines. The degree of novelty of Smart contracts and the presence of certain special features in them becomes especially relevant if we turn to practices used in exchange markets, where so-called automated trading systems are widely used. For example, in foreign exchange markets trades are frequently executed not by the trader himself, but by a computer system based on a trading strategy implemented as a program run by the computer system. As of 2014, more than 75% of the stock shares traded on United States exchanges originate from automated trading system orders.[11] Thus automated contracts per se are not something new: they have been widely used in many spheres for a long period of time already. So what is so special with Smart contracts then?

For this it is useful to refer to another definition of Smart contracts provided by Gideon Greenspan: 'A smart contract is a piece of code which is stored on an Blockchain, triggered by Blockchain transactions, and which reads and writes data in that Blockchain's database'.[12] This definition is more concrete, as it places emphasis on the Blockchain technology as one of the core features of Smart contracts.

However, the question is: whether Blockchain has certain legal implications for the contracting process, which would make it significant for characterization of Smart contracts, or it is only a fashionable technology, of interest mostly to IT-specialists. In the present author's view, Blockchain can be regarded as a 'paradigm-shifter' in the sphere of contracting: *it allows automation of the process of contractual performance of both parties*. Old-school vending machines automate performance only of one party, requiring at least some personal involvement on the other side (e.g. coin insertion or application of a banking card). When both parties' performance can be fully automated, a new quality arises in the contract, even triggering a question whether there is still a contract in a legal sense and not some other kind of phenomenon. Another peculiarity of Blockchain-based contracts is that they allow not only automation of contractual performance, but also of the process of conclusion: the contract can be concluded by electronic agents, employed by the parties.

In some cases, a contracting party can be represented by a so-called Decentralized Autonomous Organization (DAO).[13] This concept has not yet received universally recognized definition. According to one position, DAO is nothing more than a set of long-lasting 'Smart' contracts, as opposed to a regular 'Smart contract' having specific purposes and coming to an end once they are achived. The organizational theorist Arthur Stinchcombe once wrote that contracts are merely organizations in miniature, and by extension

[10]K Segrave, *Vending Machines: An American Social History* (McFarland and Company, 1944) 3.
[11]D Levine, 'A Day in the Quiet Life of a NYSE Floor Trader' *Fortune* (29 May 2013) <http://fortune.com/2013/05/29/a-day-in-the-quiet-life-of-a-nyse-floor-trader/>.
[12]G Greenspan, 'Beware of the Impossible Smart Contract' *Blockchain News* (12 April 2016) <http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract>.
[13]A Hayes, 'Decentralized Autonomous Organizations: IoT Today' *Investopedia* (29 February 2016) <http://www.investopedia.com/articles/investing/022916/decentralized-autonomous-organizations-iot-today.asp>.

all organizations are just complexes of contracts. Firms are created using a series of contractual agreements, ranging from employment contracts and employee benefits, to deals with vendors and suppliers and obligations to customers, to building leases and sales and purchases of equipment. Traditionally, these contractual obligations are quite costly because they need to be enforced externally by society in the form of a trusted legal system and through legal enforcement. Courts, lawyers, judges, and investigators all form this system of contract enforcement. With a Blockchain-based 'Smart' contract, however, much of these costs are greatly reduced or eliminated. This promises to make Blockchain-based organizations more efficient, cost-effective, and competitive, compared to traditional firms in the marketplace.

All the above illustrates that 'Smart' contracts go far beyond the existing models of contracting process and represent a new paradigm of interaction in cyberspace. To illustrate this thesis it is necessary to provide some examples of potential application of 'Smart' contracts in real life.

'Smart' contracts allow the creation of pools of resources and their allocation according to agreed criteria, what can be especially relevant for crowdfunding activities or for insurance-type contracts. To give some examples, a Smart contract may track the amount of funds submitted to a crowdfunding project, and once it exceeds the necessary total, the amount will be transferred to the beneficiary. Otherwise, funds are returned back to the donors.

Another example: A group of farmers may agree to create a pool of resources as an insurance against drought, flood, or other natural disaster. Once such a disaster occurs, a machine verifies it according to the specified procedure (e.g. by checking the weather or news in predesignated sources) and allocates resources. Needless to say, that Smart contract provides a high degree of transparency and auditability, mitigating the risks associated with an intermediary's decision-making process and 'human factor', as well as with time delays. As an additional 'bonus', such payments occur seamlessly across borders.

But is it possible to claim that a Smart contract is still a contract in the sense attributed by contract law? It seems that this is one of the most controversial issues in relation to Smart contracts. Some scholars argue that Smart contracts are a form of self-help, because no recourse to a court is needed for the machine to execute the agreement.[14] Self-help can be understood as 'legally permissible conduct that individuals undertake absent the compulsion of law and without the assistance of a government official in efforts to prevent or remedy a civil wrong'.[15] Such an approach, while having some merits, appears to be too simplistic, depriving Smart contracts of deeper analysis within the framework of contract law and avoiding certain questions worthy of addressing.

According to Russian law, a contract is an agreement between two or more parties, which establishes, amends, or terminates civil legal relations between them (Article 420 of the Civil Code of the Russian Federation, hereinafter – 'CCRF'). This definition is quite similar to one commonly used in Europe ('A contract is an agreement which is intended

[14]M Raskin, *The Law of Smart Contracts* (2016) p 31 <http://ssrn.com/abstract=2842258>.
[15]IB Douglas et al, '*SPECIAL PROJECT: Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*' (1984) 37 Vand L Rev 845, 850. A similar understanding of self-help is shared in Russian law.

to give rise to a binding legal relationship or to have some other legal effect. It is a bilateral or multilateral act'[16]).

One of the theses of this paper is that a Smart contract can be regarded as a legally binding agreement. First of all, it is used to govern relations associated with the circulation of certain digital assets, and thus is intended to govern economic relations between the parties, a matter which falls within the realm of civil law. The transfer of a digital Blockchain-based asset from one person to another is a typical subject matter of a Smart contract and may qualify as a 'legal effect', being one of the constitutive elements of a contract.

Secondly, although the performance of a Smart contract is automated, such a contract still requires the presence of the will of its parties in order to become effective. Such will is manifested at the moment when an individual decides to enter into such an agreement on the terms specified in advance; or, in cases involving electronic agents, when an individual decides to use such an agent for conclusion of certain agreements and agrees to be bound by their actions. The person expresses his consent to the terms of the contract and mode of their performance at the moment of conclusion of the contract. Taking into account that such a person will not be able to influence the performance of the agreement, once it is entered to, there should be a certain trust in place, which gives rise to a kind of 'fiduciary' relation in Smart contracts. But in contrast to classic contracts, where trust is put in the personality of the other party to the contract, in Smart contracts such trust is put in the computer algorithm standing behind the agreement ('trustless trust').

It is also possible to find offer and acceptance in the process of Smart contract formation. If we take an example with a crowdfunding Smart contract, its terms are predefined by the beneficiary ('offer'), and a person willing to donate to the project by transferring a certain asset to the pool is making an acceptance of that offer by his behavior. Under existing contract law provisions, a contract is considered to be concluded in such a case (Article 438 (3) of the CCRF, II. – 4:204 DCFR). It may be qualified as a contract of adhesion (Article 428 of the CCRF), or (more broadly) a contract concluded on standard terms (Section II. – I:109 DCFR).

Whether or not there is an intent to create legal relations by the parties to a 'Smart' contract is a tricky question. It is possible to argue that by entering into a 'Smart' contract they have an intention to use an alternative regulatory system, not a classic contract law, and thus that there is no true intent to create legal relations. However, if the *result* is in fact the same in substance as in the case of an ordinary contract – the transfer of ownership over a particular asset – then it may be argued that the nature of the relations at its core are also the same. Moreover, 'Smart' contracts do not fall into a class of agreements where legal contracts are not normally made (such as social invitations, e.g. invitations to dinner, or family arrangements, e.g. a promise to wash the dishes).

Finally, the mere fact that the contract is concluded by electronic means does not mean that it is not a contract. The same is true for contracts that exist solely in cyberspace.

[16]sII. – 1:101(1) of the Draft of a Common Frame of Reference (DCFR). DCFR is an academic text, one of the functions of which is to sharpen awareness of the existence of a European private law and also (via the comparative notes that will appear in the full edition) to demonstrate the relatively small number of cases in which the different legal systems produce substantially different answers to common problems. The drafters of DCFR claim that 'it may furnish the notion of a European private law with a new foundation which increases mutual understanding and promotes collective deliberation on private law in Europe'. See, Study Group on a European Civil Code, *Draft Common Frame of Reference* (Outline edn Sellier, 2009) 7.

Next it is necessary to outline the features of Smart contracts, which could be used for finding their place in the framework of existing contractual concepts. Based on the current understanding of Smart contracts, it is possible to identify the following features: (1) solely electronic nature; (2) software implementation; (3) increased certainty; (4) conditional nature; (5) self-performance; (6) self-sufficiency.

Let's take a closer look at each of them.

(1) *Solely electronic nature*. Classic contracts may exist in various forms, e.g. in oral form or in writing. Of course, the development of e-commerce has substantially increased the quantity of agreements concluded in electronic form, the most obvious examples of which are various click-wrap agreements. However, even in case of e-commerce contracts, there may be still some classic paperwork required (such as invoices, receipts, or certificates of delivery), especially when the contract provides for the purchase of offline goods or services. Sometimes, those documents are the only evidence or manifestation of the electronic contract. In contrast, *Smart contracts can exist only in electronic form; it is not possible to use any other form of contract for them* (e.g. a written hardcopy). This characteristic arises partly from the specific subject matter of Smart contracts: they may relate to digital assets (such as cryptocurrency), or to digital manifestations of offline assets, title to which is registered in Blockchain. This distinguishes Smart contracts from most click-wrap agreements, which also exist in electronic form, but only impose some negative obligations on the user (e.g. not to perform certain activities while using the service, or not to object to certain activities performed by the service-provider).

Performance of the terms of a 'Smart' contract must also be linked to certain electronic events/data. Otherwise the 'Smart' contract will not be self-enforceable (see below). All these features require a solely electronic form as essential to the existence of a Smart contract.

Moreover, a 'Smart' contract by its nature requires the use of electronic digital signatures, based on encryption technology. Under Russian law such a signature, due to the presence of cryptography, qualifies as an 'advanced non-qualified signature', and their usage is generally governed by the agreement of the parties using them.[17]

(2) *Software-implemented*. Code is law, and in Smart contracts computer code also comprises contractual terms. Thus contractual terms are manifested in computer code, and this is compatible with the 'freedom of contract' principle. Therefore, it is possible to argue that each Smart contract by its legal nature is also a computer program within the meaning of intellectual property law.[18]

Thus, *a Smart contract has a dual nature in the law: it serves as a 'document' governing the contractual relations of the parties, and it is also object of IP rights*, representing the valuable object of intellectual activity. Therefore, programming certain Smart contracts based on

[17]Russian law also recognizes both a so-called 'advanced qualified signature', which is provided by the specialized center accredited by the government authority, and which attaches the highest legal force to a document signed therewith; and a 'simple electronic signature' which can be based on a wide range of technologies (sms-codes, passwords), and whose legal force is based on the prior agreement of the parties to use such type of signature in their relations. See, Federal'nyy zakon ot 06.04.2011 N 63-FZ 'Ob elektronnoy podpisi' [Federal Law of the Russian Federation No. 63-FZ 'On electronic signature' of 6 April 2011].

[18]The Russian definition of computer program is quite similar to the US definition. According to Article 1262 of the CCRF, a computer program is a set of statements and instructions, to be used by a computer in order to achieve a certain result. Under the US Copyright Act, a computer program is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result.

the requirements of the customer can be treated as a software development process, while distribution of subsequent rights to the 'Smart' contract should be performed within the framework of the relevant IP rights and licenses.

To give an example of how a 'Smart' contract may look like from a factual perspective, here is an extract from a text of the Smart contract based on the Ethereum platform attached.[19]

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

  /* Initializes contract with initial supply tokens to the creator of the contract */
  function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

  /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

(3) *Increased certainty*. Since a Smart contract has software code in its core, its terms are expressed in one of the available computer languages, which are rather formal languages in their substance, with strictly defined semantics and syntax.[20] A computer language does not allow discretion in its interpretation by the machine. Smart contract terms are interpreted by machine on the basis of Boolean logic,[21] in contrast to classic contracts, where interpretation of terms is performed by the human brain on the basis of subjective criteria and analogous ways of thinking. Thus the precision of programming languages is able to reduce possible problems associated with unpredictable interpretation of contractual terms by a party to the contract or an enforcement agency. Although ambiguity may exist in programming languages, these ambiguities are less than in the real world because there are simply fewer terms that a computer can recognize than those which a human being can recognize. As a result of the specific characteristics of a Smart contract (described above), existing rules on interpretation of contracts do not apply to Smart contracts. There is no place here for 'Interpretation according to the common intention of the parties even if it differs from the literal meaning of the words or in accordance with the meaning which a reasonable person would give to it'.[22] Smart contracts are meant to be stand-alone agreements – not subject to interpretation by outside entities or jurisdictions. The code itself is meant to be the ultimate arbiter of 'the deal' it represents.

[19]Etherium Blockchain App Platform, 'Create Your Own Cypto-currency with Ethereum' <https://www.ethereum.org/token>.

[20]For example, Solidity – the language based on JavaScript – was created as a language for Smart Contracts on the Ethereum platform.

[21]Boolean logic is a form of algebra in which all values are reduced to either TRUE or FALSE. Boolean logic is especially important for computer science because it fits nicely with the binary numbering system, in which each bit has a value of either 1 or 0.

[22]See, sll. – 8:101 DCFR; Article 431 of the CCRF.

However, a couple of important points need to be made. First of all, due to technical complexities of Smart contract architecture and the necessity to possess advanced programming skills to create such an agreement, in many cases Smart contracts will be created by specialized companies based on a request from the client. Due to a separation between the person programming the code and the person intending to use it in its commercial activities, there is a risk of misunderstanding between them with regard to the terms of the future agreement. Ultimately, differences may exist between implementation and intent, and this danger may be aggravated by the huge gap of abstraction between legal language and a programming language. However, it can be argued that such misinterpretations should be within the sphere of responsibility of the person making available the Smart contract, and resolved within the existing contractual framework with its counterparty. Such errors should not affect external parties, who subsequently accept the terms of the agreement and become a party to a Smart contract.

Secondly, since it is only the computer code which regulates the Smart contract, the latter becomes automatically subject to various flaws and bugs which may accompany any computer program. A recent hacking attack on one of the Ethereum's Smart contracts is an excellent example. In June 2016 attackers exploited a software vulnerability and drained millions of ether – with a theoretical value in the tens of millions of dollars. One wallet identified by community members as a recipient of the apparently stolen funds holds more than 3.5 million ether. At an exchange rate of about $14 a unit, that works out at $47 million.[23] In an open letter to the Ethereum community, the attacker claimed that he has not done anything illegal, he was only 'making use of this explicitly coded feature as per the smart contract terms'.[24] Leaving the matter of qualification of the attacker's actions aside, it is possible to state that Smart contracts are still subject to human's misjudgment, and although they are potentially immune to mistakes in legal terminology and drafting, they are still vulnerable to coding errors. This vulnerability probably needs to be addressed by the newly developed rules on interpretation of such contracts.

(4) *Conditional nature*. Earlier it was argued that a Smart contract is drafted in one of the computer languages. Conditional statements are foundational to computing: computer code is based on statements like 'if "x" then "y"'. Such an approach is in harmony with contractual terms and conditions. As Raskin correctly puts it, the enforcement of a contract is nothing more than the running of a circumstance through a conditional statement.[25] Under Russian law, such an agreement can be qualified either as a 'conditional transaction' (Article 157 of the CCRF) if all of the terms of the contract are conditioned on a certain event, or as a contract with conditional obligation (Article 327.1 of the CCRF), where a contract as such becomes effective at the moment of its conclusion, but execution of some of its terms is conditioned to certain events. Similar provisions are provided in Section III. – I:106 DCFR. In this regard Smart contracts fall within the existing taxonomy of contract law.

(5) *Self-enforceability*. Once a Smart contract is concluded, its further performance is no longer dependent on the will of its parties or a third party. It requires no additional approvals or actions on their part. A computer verifies all the conditions, transfers assets, and makes entries in the Blockchain database about such transfers. Thus a Smart contract is technically

[23]R Price, 'Digital Currency Ethereum is Cratering Because of a $50 Million Hack' *Business Insider* (17 June 2016) <goo.gl/SY90Ks>.
[24]Pastebin, 'An Open Letter' (June 18 2016) http://pastebin.com/CcGUBgDG>.
[25]M Raskin, *The Law of Smart Contracts* (2016) p 11 <http://ssrn.com/abstract=2842258>.

binding for all the parties to it, they are no longer dependent on any human intermediary, which would be subject to errors and subjective discretion. A subsequent change of circumstances, or the intent of the parties in regard to such a change, is irrelevant. There is no room for opportunistic behavior or 'efficient breach'.[26] This feature of Smart contracts create substantial tensions with classic contract law, as will be shown later.

(6) *Self-sufficiency* is closely related to the previous feature of Smart contracts – its self-enforcing nature. However, self-sufficiency has a different emphasis. A Smart contract does not need any legal institutions to exist: neither enforcement agencies, not the corpus of legal rules (default or mandatory rules to supplement the express terms), as are needed by classic contracts in case of their incompleteness. As Russian prime minister, Dmitry Medvedev, stated in his speech on the perspectives of development of law, 'Smart Contracts represent [a] new challenge to legal regulation. Systems creating such contracts live by their own rules, beyond the boundaries of law'.[27] Self-sufficiency is especially important in transborder transactions, since it avoids dependency on differences in languages, national laws, and their interpretation (including various types of geopolitical economic sanctions). The same rules are applicable all over the world.

Based on the above features, it is possible to define *a Smart contract as a piece of software code, implemented on a Blockchain platform, which ensures self-performance and the autonomous nature of its terms, triggered by conditions defined in advance and applied to Blockchain-titled assets*.

Thus not every contract embodied in a computer language can be regarded as a Smart contract, but only the one based on Blockchain technology, and having a self-enforcement nature. Situations where Blockchain technology is used for securing real-world transactions are also possible; for example, where it is used for monitoring performance of sales of offline goods based on radio frequency identification-technologies, or for securing payments for leased equipment by disabling the equipment in case of default. In such situations Blockchain technology has a complementary nature in regard to the overall transaction, and the transaction may be structured without use of a Blockchain, by using other conventional means. Thus, from the author's point of view, it would be more correct to treat such contracts as electronic contracts, but not as true 'Smart' contracts. Otherwise the concept of a Smart contract will be so blurred that it loses its useful meaning, and further discussion of the ways of its regulation will be obstructed by avoidable confusion.

Among the benefits of Smart contracts is their ability to decrease a number of transaction costs which accompany regular contracts, such as costs associated with ensuring contractual performance (e.g. litigation costs or costs associated with provision of collaterals). In addition, costs associated with the involvement of an intermediary in the process of performance of a contract (such as a bank or insurance organization) are also excluded in Smart contracts due to their disintermediating nature. However, it would not be correct to conclude that Smart contracts are cheaper than regular ones. Infrastructure necessary for implementation of Smart contracts and costs associated with the development ('drafting') of terms of Smart contracts are still rather high.

[26]According to Black's Law Dictionary, efficient breach theory is 'the view that a party should be allowed to breach a contract and pay damages, if doing so would be more economically efficient than performing under the contract'.

[27]Vystupleniye Dmitriya Medvedeva na plenarnom zasedanii [Speech of Dmitry Medvedev on Plenary Session], Saint-Petersburg International Legal Forum, 18 May 2016].

Some Smart contract platforms have already emerged and gained popularity and recognition. The most obvious example is Ethereum, which is a public Blockchain-based distributed computing platform, featuring smart contract functionality. It provides computing capacity (a decentralized virtual machine) that can execute peer-to-peer contracts using a cryptocurrency called 'ether'. In contrast to the Bitcoin ecosystem, which does not allow exchange of any other object than the Bitcoin unit, Ethereum allows to facilitate the exchange of virtually any class of assets which is capable of transfer in the Internet environment. Ethereum was initially proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer of Russian origin. This platform is viewed as the most prominent basis for further development of Smart contracts. Today Ethereum is the second-longest and fastest-growing public Blockchain (after Bitcoin). It even can be perceived as posing a threat to Uber-like business models.[28]

> Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center. Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.[29]

Thus there is no doubt that this platform will attract further investments and the quantity of Smart contracts developed on it will increase. Besides, other similar platforms will appear. All this will definitely provoke further attention to the legal nature of smart contracts and issues associated with the application of the classic contract law provisions to them.

4. Smart contracts in the context of the present contract law: issues and challenges

The concept of Smart contracts creates numerous concerns and challenges when one tries to apply classic concepts of contract law. Moreover, such challenges have a universal nature, going to the core of contract law provisions, which are more or less the same regardless of the jurisdiction. The main problem lies in the fact that Smart contracts are created and are developing in a technical universe 'parallel' to the legal realm, without a backward glance to any legal considerations, like the Internet in its early days. Thus the computer is indifferent to the fundamental legal principles, such as lawfulness, fairness, and protection of the weaker party. Instead the principles of certainty and effectiveness prevail. The fact that provisions of Smart contracts are enforced solely by technical code leads to the following issues.

(1) *Smart contract does not create obligations in the legal sense*. The notion of obligation, which originates from Roman law and is a key to the Continental contract law, is alien to Smart contracts. The Institutes of Justinian contain a famous definition of an obligation ('obligatio' in Latin): 'it is a bond created by law in accordance with the laws of our community. This bond we can be compelled to sever by the performance of some act,

[28] Uber removes the traditional middleman – in the case of taxis, the taxi dispatcher – from the buyer/seller equation, allowing each driver to be his own boss and work independently of a central company, replacing it with a new type of middleman – the computer application.

[29] D Tapscott, A Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (Kindle edn Penguin Publishing Group, 2016) 18.

generally the transfer of some thing'.[30] An obligation corresponds to a right, but the term 'right' denotes only one side of the relationship which is embraced by the Roman law term, 'obligatio'. To every right there must be a correlative duty: if A has a right that B shall give him an asset, B must be under a duty to give A the asset. The term 'obligation' denotes, therefore, sometimes the right, sometimes the duty, but more properly it denotes the whole relationship.[31]

These ideas have survived the centuries and are reflected in modern contract law. In accordance with Russian law,

> by virtue of an obligation one person (the debtor) has the duty to take for the benefit of another person (the creditor) a defined action, such as: to transfer property, to do work, to pay money, etc., or refrain from a defined action, and the creditor has the right to demand from the debtor the performance of his obligation. (Article 307 of the CCRF)

One of the key elements of obligation is (1) its orientation in the future and (2) a 'will' component. Since an obligation is a legal bond between two persons, such a bond exists to the extent that certain action or inaction has to be performed in the future,[32] and the debtor has a certain discretion to perform or not to perform it. If nothing depends on the will of the debtor then he is under no obligation to the creditor, since there can be no liability for breach of such an 'obligation', it is discharged on an automatic basis.

In order to illustrate this thesis, it is possible to highlight the difference between Smart contracts and contracts with vending machines. In the latter case, although performance is automated, the seller (owner of the vending machine) has a discretion regarding the performance of the contract. He may interfere in the process of functioning of such machine (e.g. by shutting it down) and thus change the outcome of the deal. In the case of a Smart contract, it is not possible for a party to it to change the outcome by shutting down its computer – all the transactions continue to exist and to be processed in cyberspace.

The absence of obligations (understood in the classic legal sense) in Smart contracts leads to the conclusion that all of the legal regime associated with the notion of 'obligations' is inapplicable. This applies to rules relating to the mode of performance (place and time of performance, performance by third party, etc.), and the consequences of non-performance. This accords with nature of Smart contracts: once all the provisions are enforced by technical code, there is no need for provisions having the purpose of regulating human interactions.

Does all of the above mean that the Smart contract is not a contract because it does not contain any obligations? Such a conclusion is still too simplistic for a number of reasons. First of all, the parties still express their will when entering into a contract, and they are bound by the result of their action. Secondly, contract law acknowledges certain types of agreements, which are performed instantaneously at the moment of conclusion ('executed' contracts in Anglo-American law). Probably, it would be more correct to state that the main consequence of the conclusion of a Smart contract is not an appearance of 'obligations', but the resulting self-limitation of certain rights by technical means.

[30]"Obligatio est iuris vinculum, quo necessitate adstringimur alicuius solvendae rei secundum nostrae civitatis iura". Inst. iii, 13, pr.
[31]B Nicholas, *An Introduction to Roman Law* (Oxford, 1962) 158.
[32]It is possible to state that essence of a notion of 'obligation' in Continental contract law performs similar functions to the notion of an 'executory' contract in Anglo-American law.

Smart contract does not give rise to legal bond between the parties. Even if there is some kind of 'bond', which all the parties to it share, it relates to technical bond of a party with Blockchain platform of Smart contract and such a bond is much more solid than a legal one.

(2) *A Smart contract cannot be breached by a party to it*. This follows from its self-enforceability feature and is a logical consequence of its 'code is law' nature. A party to a Smart contract cannot breach the contract if circumstances have changed and a more profitable alternative to its performance has appeared. It is the Roman law principle, 'pacta sunt servanda' (Latin for 'agreements must be kept)' in its absolute form. As a result, all established remedies for breach of contract, e.g. damages, penalties, or liquidated damages, and specific performance, are not relevant for Smart contracts, unless they are explicitly included in its code. There is also no need for specific legal devices designed to secure an obligation (collaterals). In other words, all remedies and guarantees, which the creditor has in the analogue world, do not have any role to play in the digital realm of Smart contracts. There is no need to seek enforcement of a Smart contract by addressing the claims to a third party – the judiciary or some other enforcement agency. This is one of the main 'selling points' of this contractual form. However, as was mentioned before, this feature is to some extent 'compensated' by the potential vulnerabilities of the code of a Smart contract, opening it to exploitation, either by a party to the contract or by a third party.

One disclaimer should be made here, though. It is possible to imagine a contract according to which the performance is structured in a way that may still require party's involvement in the process of its completion. For example, where the relevant amount of cryptocurrency is not blocked/deposited on a special account until the specified event occurs, but only details of the account are provided, and once the event occurs, there is a payment order directed to that account, but it may then contain no assets. Thus the contract may be formally breached. Or, for another situation, we may suppose that the counter-performance requires transfer of an electronic asset of certain kind (e.g. passcode to a certain database), but such asset is not valid (e.g. the password does not actually work). Again, in such case the question of non-performance of the contract can be raised. However, although such agreements may be automated by using some kind of computer code, they are not Smart contracts. As was stated earlier, not every contract performed in a computer language can be regarded as a Smart contract, but only a contract based on Blockchain technology and having electronic assets as its subject matter, so as to ensure its self-enforcement nature. The above examples relate to contracts which are not self-enforceable and still depend on a degree of discretion of a party to the contract. In such circumstances, it will be not possible to ensure the trustworthiness of information in the Blockchain, since it may change in a given moment of time. Thus, it is more correct to treat contracts indicated in the above examples as ordinary electronic contracts.

Another interesting question relates to situations where the 'obligations' of the parties to a Smart contract may not be performed due to technical malfunction. For example, when a hacker attack results in shutting down the infrastructure in which the Smart contract operates. In such situations execution of the computer code with the 'if' and 'then' may not occur due to the technical issues, thus jeopardizing the expectations of the parties. A natural question follows: whether the 'obligations' of the parties expressed on computer code continue to exist regardless of the malfunction, with the result that

such parties will have to perform them in some other way and face liability for non-performance, or whether the malfunction of the code of the Smart contract results in the death of the Smart contract? In the author's opinion, the answer on this question depends on how we understand what Smart contract is. If one adheres to a broad understanding of a Smart contract as any agreement containing automated performance of some of its obligations, then technical failures may not lead to termination of such an agreement to the extent that the automated action in question can be performed using other means (e.g. the asset may be delivered in offline mode). However, as was stated before, this is not the understanding of a Smart contract which the author of this paper advocates. The concept of a Smart contract will be innovative enough only if it allows complete self-enforcement and increased trust in it, ensured by Blockchain technology. In that case, a technical malfunction preventing the computer code of Smart contract from executing will mean the impossibility of its performance for each party. It will be impossible to execute it on other platforms, since the database of electronic assets subject to transfer under Smart contracts (e.g. a specific type of cryptocurrency with its particular value) may exist only within the ecosystem of a particular Smart contract platform, and it is not generally possible to replicate it in another one, only to reconstruct from scratch. Thus, all the parties to a Smart contract take and share the same risk that such contract may not be performed, but in contrast to a classic contract, such non-performance may be attributed not to actions or inactions of a certain party to it, but only to technical malfunctions. Perhaps in some cases, there may be a valid claim against the owner of such a platform for its malfunction, but it seems that some kind of preventive measures (e.g. backup) and insurance may provide a better solution in this case.

(3) *Vitiated consent or intent do not have any impact on Smart contract's validity*. Whether a Smart contract was concluded under a mistake, as a result of fraudulent misrepresentation, coercion, or threats, or by way of unfair exploitation of relationship of trust, is completely irrelevant for its performance. This contrasts with classic contracts, where such circumstances serve as a basis for court interference in all the legal systems. Moreover, consideration of such vitiating factors is in contradiction with the main feature of Blockchain-based databases of transactions: their 'single version of truth' for everyone. If such factors may serve as a basis for changing the content of such database post factum, it will undermine the trust in Blockchain and depreciate its value. Therefore, in Smart contracts there cannot be a collision between intent and its expression; what really matters is only an expression of intent represented in computer code. Such an approach can be viewed as a triumph for protection of certainty and market expectations.

Of course, there is some residual possibility of applying relevant provisions on the invalidity of a contract and its consequences (damages claims, obligations to return everything received under the agreement, etc.). But this will be possible only if the party to the Smart contract is identified and within the jurisdictional reach of the enforcement authority. Anyway, such enforcement actions will not have impact on the content of Blockchain database, unless it is created on different principles than the currently known Blockchain in Bitcoin.

(4) *Smart contracts are egalitarian by its nature*. Thus, Smart contract architecture does not allow protection of weaker parties, such as consumers, to be ensured. The whole layer of legal provisions relating to consumer law and unfair contract terms is inapplicable to Smart contracts. At the same time, Smart contracts may provide some extra leverage for consumers to protect their interests. Currently consumers do not have any realistic

choice as to conclude or not to conclude a contract: they do not have time to read the terms and conditions, and even if they do, they do not understand the terms. Even if an individual understands them, he does not have bargaining power to change them; and if he decides to go to another seller, the outcome will be the same. Smart contracts allow using electronic agents for conclusion of the agreement, and potentially they may be programmed in a way allowing them to search favorable terms and even negotiate them within the established boundaries. For example, so-called 'snipers' in eBay online auctions allow the user to select offers based on certain criteria, as well as to place offers on behalf of the user within certain parameters.[33] It is argued that in the very near future Smart contracts will allow consumers to conclude contracts based on terms pre-established by them, e.g. on certain pricing terms, warranties, absence of monitoring individual's behavior online, etc.[34] Time will tell whether this will be the case. However, it is quite possible to expect that at some point Smart contracts will become routine technology, like the Internet itself in the 1990s. Usually certain technology becomes routine when the technological elite becomes bored with it, and after that it becomes mass market. In any case, it is likely that in the initial stages Smart contracts will mostly exist in the B2B and C2C sectors, but not in the B2C segment of e-commerce.

(5) *Possibility of illegal smart contracts*. Smart contracts treat legal and illegal subject matter in the same way; what matters is only the possibility to implement such subject matter in a code. There are numerous debates relating to the potential illegal uses of the Bitcoin cryptocurrency, which cast a shadow on Blockchain technologies as well. In Russia use of Bitcoin is not in itself illegal, but there are warning statements from the Central Bank of Russia, and the Committee of Financial Monitoring, according to which Bitcoin may be used for money laundering schemes and the financing of terrorism.[35]

Smart contracts can also be used for illegal purposes; for example, for procuring hacker services by means of a contract offering a cryptocurrency reward for hacking a particular website. Ethereum's programming language makes it possible to control the promised funds. It will release them only to someone who provides proof of having carried out the job, in the form of a cryptographically verifiable string added to the defaced site.[36] Taking into account that Smart contracts may be programmed for verification of certain facts based on information available on certain websites, it may verify the fact of completion of certain illegal acts (terrorist acts, assassination, theft, etc.) and release established remuneration for that act. Although such a contract will be invalid as infringing fundamental principles of legal order (Article 169 of the CCRF, II. – 7:301 DCFR), it will still be executed by program code. The only response by the law is to try to deanonymize and to pursue the individuals involved in the transaction in real life.

(6) *Autonomous nature of Smart contracts*. Strictly speaking, Smart contracts do not need a legal system for their existence: they may operate without any overarching legal framework. De facto, they represent a technological alternative to the whole legal system. Apart from conclusions already mentioned above, it means that there is no

[33]eBay Inc, *eBay Automated Bidding System* (30 December 2013) <http://goo.gl/NPgryF>.
[34]J Fairfield, 'Smart Contracts, Bitcoin Bots, and Consumer Protection' (2014) 71 *Wash Lee L Rev Online* <http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3>.
[35]Statement of the Central Bank of Russia, 'On the Usage of Cryptocurrencies, Including Bitcoin, for Performance of Transactions' of 27 January 2014; Statement of the Committee of Financial Monitoring of the Russian Federation 'On the Usage of Cryptocurrencies' of 6 February 2014.
[36]P Duggal, *Blockchain Contracts & Cyberlaw* (Amazon E-Book, 2015).

need for conflict of laws provisions, since there are no collisions of various legal systems. Mathematics is a universal human language. Thus, Smart contracts are truly transnational and executed uniformly regardless of the differences in national laws. It is a perfect example of new type of regulator governing relations in cyberspace – Reidelberg's lex informatica[37] or Lessig's 'code is law'[38].

5. Conclusion: the ultimate question of Blockchain and Smart contracts

In *The Hitchhiker's Guide to the Galaxy* by Douglas Adams, there was an 'Ultimate Question of Life, the Universe, and Everything', the answer to which was being calculated by the supercomputer 'Deep Thought' over a period of 7.5 million years. The resulting answer, however, was rather disappointing to most people.

The above analysis has shown that a similar question may be posed in respect of Smart contracts using Blockchain technology by reference to the relation of their core features with established approaches to legal regulation. The question, which is a global one, may be regarded as the 'ultimate question of life and universe', at least for the destiny of particular technology. Let us call it the ultimate question of 'Blockchain and Smart contracts'. This question is: 'How to align the powers of the government with Blockchain if there is no central authority but only distributed technologies'?

It is possible to illustrate the essence of the question in the following example. Suppose that a certain asset is transferred by its owner A to the new owner B, and the fact of such transfer is reflected in Blockchain. However, later the owner A claims that B threatened A, and thus that the transaction is invalid. The claim succeeds in court and there is a judgment according to which the transaction is considered invalid and the asset belongs to the initial owner A. Thus, there are two realities: the first one is depicted in Blockchain and in accordance to it, the owner is B, since it is impossible to introduce changes in the content of Blockchain and reverse its data. The second reality is a legal one, sanctioned by the authority of the legal system: according to the official judgment the owner is A. How to align these realities in a way that would be acceptable for all the stakeholders and will not diminish the advantages of new technologies? This is the ultimate question.

Currently, it is possible to suggest two solutions, neither of which seems to be optimal enough.

(1) To introduce the concept of a 'Superuser' for government authorities, which will have a right to modify the content of Blockchain databases in accordance with a specified procedure in order to reflect the decisions of state authority.
(2) To enforce decisions of state authorities in 'offline' mode by pursuing the specific users and forcing them to include changes in Blockchain themselves as well as by using traditional tort claims, unjust enrichment claims, and specific performance claims.

The problem with the first solution is that it leads to substantial mutation of Blockchain technology and strips it of the main advantage: resilience to data manipulations from

[37] J Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 *Tex Law Rev* 55.
[38] L Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).

outside and a facilitated unique level of trust. If some kind of user of Blockchain technology will have extra powers, including the power to influence the data in it, the resulting solution based on such a Blockchain will be hardly more attractive than traditional databases and registers maintained by the state authorities. All the most attractive and innovative features of Blockchain will be diminished.

The problem with the second solution is that it is associated with instruments from the old era, which are time-consuming and inefficient in transborder cases, and which do not keep pace with new technologies. De-anonymization and jurisdictional problems will substantially weaken the effectiveness of such an approach and lead to diminishing the sovereign power of the national authorities in the cyberspace area.

It is quite likely that users of Smart contracts will sooner or later create their own system of dispute resolution. The recent example of the hack attack on Ethereum DAO in June 2016 shows that some mechanism of reaching a consensus between the parties to Smart contracts on certain unexpected (non-programmed) events is necessary. But this will not solve that Ultimate question of Blockchain and Smart contracts. Rather it will give rise to further problems, since the legitimacy of such mechanisms and their recognition by the state authority will become at issue.

So it is necessary to state that the Ultimate question of Blockchain and Smart contracts is still waiting for its answer, since the current ones are hardly satisfactory for all the stakeholders and for development of these technologies. One thing is evident, however. Those jurisdictions which will have the most Blockchain-friendly regulations will have a competitive advantage in attracting new innovative business models and companies willing to exploit them in a legal way.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This paper was prepared within the framework of the Basic Research Program at the National Research University Higher School of Economics (HSE) and supported within the framework of a subsidy by the Russian Academic Excellence Project '5–100'.