Citizens’ digital infrastructure as a new element of modern society critical infrastructure

Leonid A. Reingold[1], Elena A. Reingold[2], Alexander V. Soloviev[3], Oleg S. Grin[4]
leonidrein@gmail.com | l_r@mail.ru | soloviev@isa.ru | osgrin@msal.ru
[1]LLC DIAVER, Moscow, Russia;
[2]LLC MCD PARTNERS, Saint Petersburg, Russia;
[3]Institute for Systems Analysis Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia;
[4]Kutafin Moscow State Law University, Moscow, Russia

Widespread digitalization of the modern society - the emergence of digital devices, the introduction of Internet of Things, the development of Big Data processing and other technologies result in new challenges. Not only industrial and corporate automation that has already been considerably covered by the legislation initiatives but also the digitalization of everyday life has started to constitute a critical infrastructure in the modern society. This largely happens because digital devices substituting traditional technologies owned by citizens are incorporated into corporate, financial and state business processes. For instance, citizens’ devices are becoming the source of primary data for energy and utility companies. More opportunities for the direct interaction of automation solutions between themselves resulting in a controversial synergy effect have been emerging recently. The article addresses specifics of citizens’ digital infrastructure in the light of critical infrastructure, in particular the necessity and special aspects of legal and regulatory framework and possible development trends of this functionality.

Keywords: *Internet of Things, Big Data, smart contract, digitalization, critical infrastructure.*

1. Introduction

Digital infrastructure of modern society becomes critical for its functioning, which is reflected in the legislation [1]. Critical businesses are not limited to finance, corporate and state regulation spheres. Digital infrastructure formed and used by the citizens also becomes critical nowadays. Equipment owned by individuals becomes an element of global infrastructure affecting the functioning of large systems.

Very often personal automation solutions are necessary extensions of corporate systems. For instance, the shutdown of financial, communication or other subsystems servicing citizens’ mobile devices can cause a collapse in the modern society. Traditional, non-digital technological solutions may either not function or solve only a limited number of tasks. However, a massive failure of citizens’ peripheral devices also may cause critical implications. For example, a modern finance system largely operates in digital environment. Transactions, operations, analytical functions are performed in an automated environment. In case of unexpected failure of automated solutions, including citizens' devices, the shift to previous “paper” information processing technologies may not be possible and result in overall collapse of the financial system. In the article, we will address the issues of incorporation of citizens and their devices into the critical infrastructure of the modern society.

2. The challenges of citizens’ modern infrastructure

Citizens’ devices interact directly with each other on the basis of certain contracts. These contracts are made automatically and require special legal and regulatory infrastructure. Smart contracts are a good example of this.

Every person owns several “smart” devices that can be:

- programmed;
- used simultaneously in concerted manner;
- updated or reconfigured (e.g. by the update of embedded software);
- replaced by a new device due to the low cost caused by massive replication.

3. Possible solutions

When building society's digital infrastructure it is important to take into account changes happening at the personal level. Risks should be detected and prevented – unauthorized access to IoT objects, phishing of personal data, location tracking etc. In order to do so it is necessary to have solutions enabling to prevent unauthorized use of IoT infrastructure, and solutions allowing establishing mutual trust between them and other personal digital devices.

Solutions for the diagnostic of unnatural or unexpected behavior of IoT objects and prevention of these states either by the user himself or automatically are highly sought-after. These solutions should be implemented technically and must be automatically supported by legislative norms and regulations.

It is crucial to reasonably define areas of responsibility for incorrect or fraudulent functioning of personal devices. For instance, it should be clearly defined in the legal framework who is responsible for the incident – the user of the device, the owner of the device or infrastructure interacting with the device, the manufacturer of the device or software installed on the device or external intruder.

In should be clear to everybody which actions must be performed by conscientious users of an IoT device or a system consisting of these devices to provide a sufficient response in order to avoid liability for the damages caused by these devices.

Providing a widespread incorporation of digital devices, including for instance IoT devices, there is a need for the new methods to support social and economic structure of the modern society.

Every person in modern circumstances has to be technologically-savvy, demonstrate a new level of situational awareness and understand the behavioral culture of digital society. This should be ensured by new norms and regulations in the sphere of digital technology.

Devices in the public digital infrastructure are explicitly or implicitly registered; objects are being interconnected and co-used. This connectivity and its usage is often performed automatically. The examples of connectivity between objects are – establishing ownership of an IoT object by a particular person, content and usage rules set by that person, object's location registration and tracking of its movements etc. Automated systems can provide information about the objects connected with or interesting to a certain person, about his movements or his usage patterns for IoT objects. A new level of information awareness has led to the emergence of new social and economic challenges.

In is not uncommon in digital infrastructure when a person cannot detect risks arising out of the incorporation of IoT devices, new means of communication and processing of information, or assess implications of the use of the new technologies. Besides, possible risks in digital infrastructure tend to increase due to the development of device technical characteristics and introduction of new data processing tools.

Many challenges arise out of the development of the emergent properties in digital systems. These challenges are associated, for example, with the integration of data about the digital devices usage by a certain person and accumulation of data history. For instance, it is possible to collect data and use it implicitly with the Big Data technologies. These methods allow to detect new links between objects, e.g. to personify previously anonymous information. The application of these methods may result in the situation when data harmless for a user today may jeopardize him in future if these data is somehow specified or new data aggregation and processing technologies are applied in unexpected ways.

Thus, there is a need for scientific researches, development and implementation of tools guaranteeing a certain level of situational awareness for persons who are not familiar with the specifics of surrounding digital infrastructure, allowing to be efficient in a rapidly changing digital infrastructure environment.

Tools enabling situational awareness should be implemented predictively, i.e. their emergence should precede the development and implementation of new communication features, IoT devices and systems based on them. The new device development process should be comprehensive, addressing not only technical and technological aspects but also considering psychological, social, economic and legislative factors.

4. Legal environment around digitalization

Preventive development of regulatory framework for the application of digital infrastructure is crucial in modern world.

To implement legal restraints corresponding to the requirements of the new digital infrastructure it is necessary to use technologies adapted for the application in digital environment, e.g. technologies that can operate automatically. The use of smart contracts is the example of the application of such technology. With the use of smart contracts, it is possible to implement automated means of communication, for example, for settlements between elements of the IoT infrastructure.

Smart contracts is a new, evolving technology that requires conceptual research, technological improvement of available solutions, and the development and adoption of new norms and regulations. Let us discuss some conceptual issues related to the use of smart contracts in digital environment.

The term smart contract is not standard. It does not fully reflect the essence of the technology behind it. It actually means not a smart contract but a form of formal contract representation with the use of digital infrastructure that is enough for preparation and execution of a contract in digital environment. In [2] it is suggested to use the terms smart contract and automated (self-executing) contract as synonyms. Besides, the term self-executing in authors' opinion more accurately reflects the essence of this technology. The term digital contract may be suggested – it reflects the fact that operations with contracts using this technology are incorporated into digital infrastructure one way or another. Smart contract may not be executed as a traditional document but still somehow enables the execution of necessary arrangements in a particular situation. However, as the term smart contract is the most commonly used in literature, we will use it here.

Technological implementation of smart contracts can be different. The same requirement, for instance to have a formalized form and automated execution of some contracts can have different technological implementation and apply different social and economic technologies. Under the social and economic technologies, we mean the combination requirement – technology that is used to fulfill the requirement [3]. The same requirement can be met by different technologies; the same technology can be used to meet different requirements.

When talking about smart contract implementation it is often meant the use of Blockchain technology. Many authors consider Blockchain as a part of the technology implementing smart contracts. However, others point out that smart contract should be technologically- neutral [4]. Now smart contracts often use Blockchain technology and thus they are often considered as complementary technologies [5]; in future the use of smart contracts may require the application of advanced technologies guaranteeing data immutability at the execution of smart contract. Differences and interaction specifics between smart contract using Blockchain and a traditional contract should be taken into account. There is an opinion that smart contract fits into the existing system of legal documents and becomes a one more semantic layer of a traditional contract [6].

The example of implicit smart contract implementation when traditional documents are not produced at all is automated taxy ordering system. One of the most well-known services of that kind is Uber [7]. A person orders a taxi for the price calculated by the system for a particular itinerary. The price is calculated with consideration to demand and traffic situation. Prepayment or funds reservation is not needed. The driver that accepted the price set for the trip provides the service, receives payment in cash or by any type of cashless payments. After the trip the driver and the user assess each other. Obviously, negative assessments can be caused by unsatisfactory service.

In this example, smart contract is implemented without traditional documents. Correctness of communication between parties is guaranteed by the automated system – if one of the parties does not fulfill its obligations, it is fined and the further use of service can be blocked. Technology supporting data immutability with the use of distributed ledgers is not needed in this case – the contract is short term, mutual assessment and sanctions are done immediately. Automated system enabling the service operation arbitrates the parties.

The issue whether a traditional contract should be supplemented by a smart contract is being brought up in literature [8]. In our opinion, the example described above demonstrates that at the current level of technological development this is possible only in cases when contract negotiations can be formalized. This allows to clearly specify parties' rights and obligations, register in detail the state of a contract execution and undoubtedly interpret all possible ways of its violation. It may be expected that further technological development will broaden the scope of situations where it is reasonable to use smart contracts.

Technologies similar to the described taxi ordering service are becoming more and more popular and are used for the provision of services with the help of digital devices - smartphones and computers. These technologies considerably change social and economic landscape of the modern society. Thus, for example, they have fundamentally transformed the taxi market – prices decreased due to free competition, traditional taxi ordering method with the use of a telephone in many cases became an add-on to the described automated system. However, operating principles require the development of legislative regulation in order to eliminate potential problems.

Summing up, we can state that the technological implementation of smart contracts should be done according to the following technological and legal requirements:

- Impossibility to change a contract content without consent of all participants, however, if such consent is granted, the contract can be changed. Immutability of contract’s content is often guaranteed by the use of Blockchain technology; still, this is just one of the possible options enabling smart contract content immutability and its execution.
- Technological invariance. For example, when processing technology is updated or changed for a new one, available smart contracts should remain valid.
- Legally binding. The contract must be duly supported by the norms and regulations in force guaranteeing its execution by the parties involved and providing protection in case of rights violation. However, excessive regulation that impedes the development, should be avoided.
- Compliance with regulations concerning data processing procedures, for instance with the legislation on personal data processing [9].
- Verifiability and possibility to check the contract by the parties.
- Resistance to fraudulent activities, such as hack of software, insufficient information about parties to the contract withheld intentionally with mercenary intentions etc.
- User-friendly design of smart contracts, possibility to present smart contract in a convenient form.
- Clear procedures on all stages of contract preparation and execution.
- Possibility to combine digital and traditional display, i.e. availability of software enabling to convert smart contract into the format suitable for both automated application and perception by people.
- No high requirements towards resources of the infrastructure, possibility to scale the system processing smart contracts. .
- Possibility to work bypassing intermediaries in the process of contract negotiation and execution.
- Availability of interstate agreements on the acknowledgement of contracts made by persons belonging to different jurisdictions.
- Standardization of information processing procedures with the use of smart contracts.

Obviously, available smart contract implementation solutions do not meet all these requirements. This technology is still in the process of methodological interpretation and development. However, it is integrated by both commercial enterprises and state regulation authorities of some countries. In the United States, the use of smart contracts is still regulated on the states level [10].

In Russia the use of smart contracts and related technologies is still not enough regulated with regards to legal framework. However, the adoption of some relevant norms and regulations is expected in March 2020 [11].

Legislative framework around smart contracts should be implemented considering the widespread use of automated devices. It should be developed taking into account smart contracts use cases in ordinary routine situation in order to guarantee that the new means of communication are understood by a general user, that they do no cause discomfort and tensions in society.

It may be assumed that the legal system supporting digital environment will function similar to the traditional legal system because despite of new means of life cycle implementation it attends to the same subject domain and supports the same activities but with the help of a new technology. For example, a promising IoT infrastructure will became a formalized and programmed subdomain of the traditional infrastructure. In the context of IoT infrastructure smart contracts may include for instance the following content:

- Service Level Agreements (SLA) in a special format allowing to control and assess the fulfillment of mutual obligations by devices and their owners at the technological cooperation.
- Settlement and cooperation terms in a broader context not covered by SLA .
- Requirements towards service access, formats, volumes of data exchange and other parameters specific to the system consisting of certain devices.

The contents of smart contracts should be available for the wide application by users who do not have professional experience in digital technologies. It is crucial to address the challenges of interface usability and use cases for the implemented technologies.

Figure 1 demonstrates types of smart contract users and the goals they plan to achieve using this contractual instrument. Citizens get a convenient automated tool to process personal information. The state controls and regulates the sphere in order to minimize risks for citizens and social and economic system in general. Besides, the state provides infrastructure services enabling smart contracts implementation. These include up-to-date manuals and classifiers enabling standardization of smart contracts content.

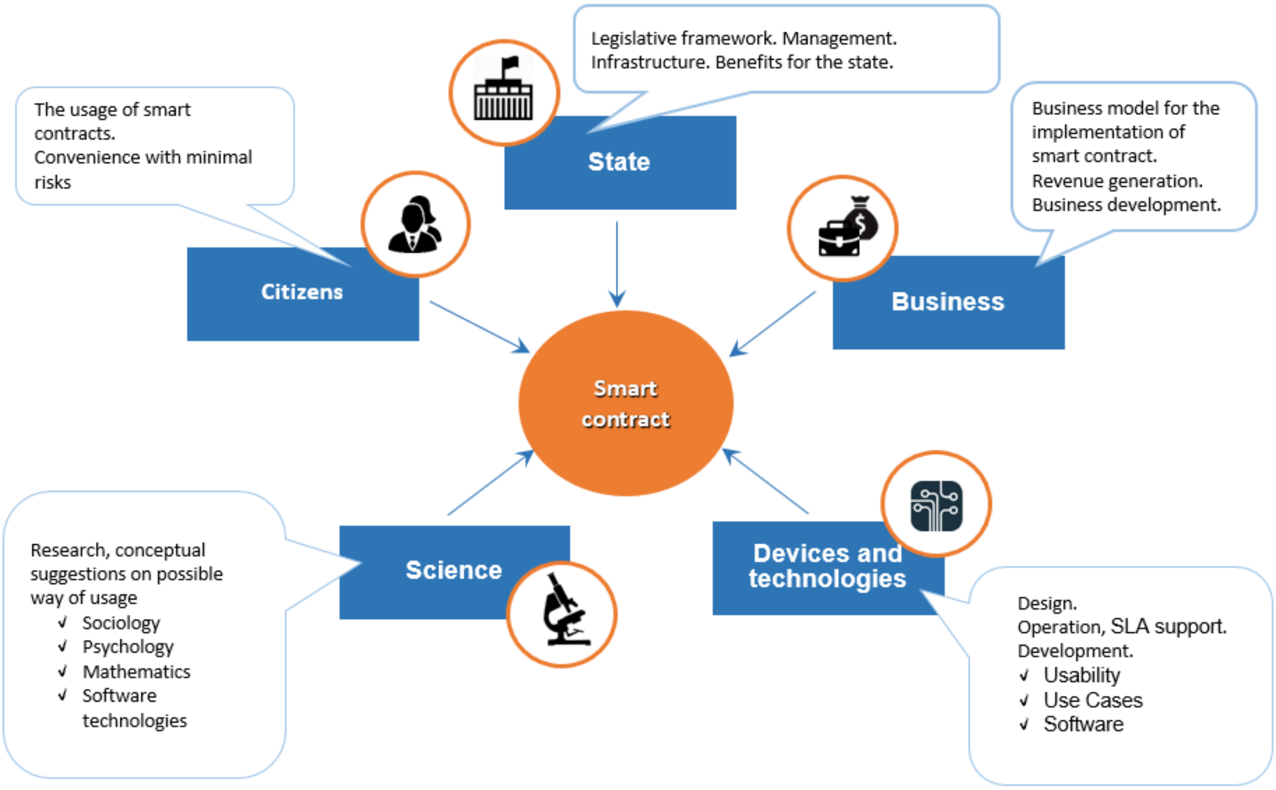
Legislative framework. Management. Infrastructure. Benefits for the state.
State
The usage of smart contracts. Convenience with minimal risks
Citizens
Business model for the implementation of smart contract. Revenue generation. Business development.
Business
Smart contract
Research, conceptual suggestions on possible way of usage
√ Sociology
√ Psychology
√ Mathematics
√ Software technologies
Science
Devices and technologies
Design.
Operation, SLA support.
Development.
√ Usability
√ Use Cases
√ Software

Fig. 1. Types of smart contract users and their goals

Businesses suggest a smart contract business model of a certain type and implement it. Throughout the life cycle of the implemented system businesses strive for profitability of the system, provide its modernization and development.

Design, operation and technological development of this type of smart contract providing sufficient SLA for the chosen business model is supported by technical and technological solutions. The developed software is focused on citizens; they should understand clearly how to work with smart contracts. Special attention is paid to the usability and friendliness of the system interfaces.

Progress in the humanities and natural science is used for the research of smart contracts development tendencies, of best ways to incorporate this technological trend into the social and economic system; it also helps to address the challenges of technology performance. Ensuring immutability of smart contract content providing sufficient operation flexibility is one of these developing trends.

Digital infrastructure object features related to smart contracts such as those of IoT devices can be considered as a type of virtual assets in addition to other types described in [12].

It should be noted that objects of the legislative framework have its own life cycle – from the adoption to the termination or change for new objects. Life cycle of a norm or a regulation is shortening due to the rapid emergence of the new types of digital infrastructure objects, change in their functionality during operation. The acceleration of changes affects the use of digital technologies in everyday life. Emergence and rapid general adoption of digital technologies by social and economic system created a new situation in the society impending the loss of control and collisions due to the development of unexpected emergent features. Preventive development of legislative framework, regulation of digital technologies usage will allow eliminating possible negative situations.

5. Conclusion

Digital devices owned by citizens have become a critical element of infrastructure in the modern society. These are personal communication devices, e.g. smartphones, and IoT objects, e.g. home management solutions, utility resources consumption solutions etc. Traditional communication channels and a significant part of object environment are substituted by functionally similar digital devices. New types of violations and technological risks arise along with positive results.

In these conditions, it is essential to preventively implement new legislative framework, new technologies such as smart contracts that meet the requirements of the changed environment and allow to provide effective management mechanisms for the society and eliminate negative situations.

It is also needed to develop and implement norms and regulations that precede the development of new technologies and allow to guarantee efficient operation of social and economic system in new conditions.

Acknowledgment

This paper was supported by the Russian Foundation for basic Research (RFBR) via projects 18-29-16200.

References

[1] Federal Law of July 26, 2017 N 187-ФЗ "On the Safety of Critical Information Infrastructure of the Russian Federation" (available at http://static.kremlin.ru/media/acts/files/0001201707260023.pdf July 2017).

[2] Grin O.S., Grin E.S., Solovyov A.V. The Legal Design of the Smart Contract: The Legal Nature and Scope of Application. Lex Russica. 2019;(8):51-62 Lex russica. 2019;(8):51-62.] (In Russian).

[3] Reinhold L.A., Slavin O.A. Socio-economic technologies as a generalization of trends in socio-economic development // Proceedings of the Institute for System Analysis of the Russian Academy of Sciences. Intelligent information technology. Applied aspects. M .: 2005.p. 40-55.

[4] Volos A.A. Smart contracts and principles of civil law // Russian Justice. 2018. No. 12. P. 5-7 [Volos A.A. Smart-kontrakty i printsipy grazhdanskogo prava // Rossiyskaya yustitsiya. 2018. № 12. pp. 5-7].

[5] Smart Contracts and Distributed Ledger — A Legal Perspective // ISDA Linklaters. — August 2017. (available at https://www.isda.org/a/6EKDE/).

[6] Gaëtan Guerlin. Considerations sur les smart contracts. Dalloz IP/IT. Droit de la propriete intellectuelle et du numerique. 2017. № 10. pp. 512 - 513.

[7] What Is Uber and How Do You Use it? (available at https://www.uber.com/ee/en/ride/how-it-works/).

[8] Smart-Contract: is the Law ready? (available at https://digitalchamber.org/smart-contracts-whitepaper).

[9] Federal Law of July 27, 2006 No. 152-FZ On Personal Data (available at http://www.kremlin.ru/acts/bank/24154).

[10] Arizona State Law of March 29, 2017. Arizona House Bill 2417. (available at https://legiscan.com/AZ/text/HB2417/id/1588180).

[11] In March, the State Duma may adopt a law on digital financial assets (available at https://versia.ru/gosduma-mozhet-v-marte-prinyat-zakon-o-cifrovyx-finansovyx-aktivax February 2020).

[12] Bogdanova E. E. Problems of the use of smart contracts in transactions with virtual property. Lex russica (Russian law). 2019.No 7 (152). pp. 108-118.

About the autors

Reingold Leonid A., consultant, LLC DIAVER, Candidate of Technical Sciences. E-mail: leonidrein@gmail.com.

Solovyev Alexander V., Chief Researcher, Department 94 ISA FRC CSC RAS. Doctor of Technical Sciences. E-mail: soloviev@isa.ru.

Reingold Elena A., lead consultant, LLC MCD PARTNERS, PhD in Economics, docent. E-mail: l_r@mail.ru.

Oleg S. Grin, Civil Law Chair, Kutafin Moscow State Law University, Moscow, Russia, E-mail: osgrin@msal.ru