Advances in Social Science, Education and Humanities Research, volume 531
Proceedings of the conference on current problems of our time: the relationship of man and society (CPT 2020)

Digital Security of "Smart Cities" as a Factor in the Sustainable Development of the Economy

Viktoria V. Borisova[1], Elena E. Panfilova[1], Hendra Raza[2]

[1]*Department of Management Organization in Engineering, Institute of Industrial Management, State University of Management, Moscow, Russia*
[2]*Faculty of Economics and Business, Universitas Malikussaleh, Aceh Utara, Indonesia*
** Corresponding author. Email: inf@guu.ru*

ABSTRACT
The purpose of the research conducted by the authors is to identify key problems in organizing the digital security of technology parks as prototypes of the "smart city" and points of innovative development of the economy. In the research the authors adhered to the hypothesis that the development in Technopolis's of a single digital platform for the interaction of the management company, residents, government bodies will serve as the basis for the development of the regional economy if key informational cyber threats are considered taking into account the maturity of business processes of organizations and newly involved information technologies.
Within the framework of the article different tasks were solved. They were an analysis of automation efficiency of key business processes in resident companies and the management company; comparison the approaches of leaders in the digital transformation of the business to the choice of information technology / systems to form the "digital layer" of the organization; development of guidelines for the digital security of information systems of representatives in the real sector of the economy on a single digital platform. The empirical material of the research were 169 technology parks of the Russian Federation, which were evaluated in terms of information openness and contribution to the sustainable development of the region. Information openness involved an assessment of the information systems and technologies used by foreign resident companies (including Indonesia).
The methodology of the study is based on statistical methods of research, observation, survey, and comparison. The main result of the study is the identification and ranking of digital security threats for technology parks as prototypes of "smart cities" in terms of importance, development of recommendations for monitoring projects of digital business transformation in an unstable environment. The paper clarifies the features of building information systems of resident companies during their integration into the information system of a Technopolis's and further into a single digital platform.
The authors' basic research area is the digital security of information systems of industrial organizations under the conditions of the development of smart contract technologies, predictive analytics, reverse engineering, and enhanced digital qualified signatures. The authors consider the further research development in this area as improvement of interaction mechanisms of single digital platforms of Technopolis's with state authorities, financial institutions, and fiscal authorities, as well as with investors, both in the Russian Federation and Indonesia.
Keywords: *Digital economy, Information, Cybersecurity, Risk, System, «Smart city», Technopolis, Management, «Smart contracts»*

1. INTRODUCTION

Standards for conducting modern industrial business, which is an integral part of the "smart city", are undergoing major changes. They are primarily driven by the requirements of increasing competitiveness through following the global trends of "Industry 4.0". The development of industrial organizations through a digitalization strategy increases the chances of sustainable development of the country's economy. At the same time, the company's management is facing new threats to digital

security, which are insufficiently studied and systematized.

For Technopolis's, which are the prototype of a "smart city", issues of digital security become doubly relevant due to the high concentration of resident companies in high-tech industries, the specifics of integrating business processes between the management company and public authorities. The scientific novelty of the research results presented by the authors is to consider the issues of digital security of resident companies in relation to the technological infrastructure of the Technopolis and the basic/specialized services of the management company.

The theoretical significance of the research carried out by the authors is to develop the theory and methodology of managing complex socio-economic systems, which include "smart cities" in the context of business digitalization, to determine the information threats / vulnerabilities associated with this process, as well as to identify the degree of dependence of the structural characteristics of "smart cities" on cyber threats. A number of researchers associate the consideration of digital security issues in "smart cities" with the intensity and nature of the use of cloud technologies, data storage when conducting business and interacting with contractors in the framework of technological chains [1]. In the works of other authors managing cybersecurity companies as systemically important core of a "smart city", is considered from the point of view of the information architecture of a company [2]. In this case, there are stages of risk management for the business level (corporate information systems - ERP), production level (MES-systems), technological level (PDM/CAE-systems), design level (CAD-systems) and monitoring system (MDS-systems).

Technopolis's located in special economic zones are defined by some scientists as an ideal place for the formation and development of unified digital platforms for interaction between the Technopolis management company, residents and state authorities [3]. However, Technopolis's as the core of building a "smart city" differ in the degree of state participation in regulating the activities of the management company; the nature of attracting foreign investment; the specialization of enterprises included in clusters; and industry specifics.

Accordingly, the recommendations for ensuring digital security of "smart cities", which include a variety of technopolises, will vary. The stability of economic development for a particular region is determined by the list of key business processes of interaction between representatives of the real economy with government authorities, the degree of their automation and the approaches used to ensure information security when using smart contracts. In this regard, the choice of the topic of digital security of "smart cities" is significant both when doing business in the Russian Federation and abroad (Indonesia).

The idea of using smart contracts in organizing such interaction seems to be productive and is supported by a large number of researchers [4, 5]. It is noted that being essentially self-executing and self-supporting agreements in digital form [6], smart contracts can significantly reduce transaction costs and get positive effects throughout the life cycle of a transaction concluded in the digital space. In General, these effects are implemented in terms of increasing the market efficiency and activity of resident companies and their partners, including the management company itself, provide full verification of the identity of the client and counterparty, facilitate the conclusion of a transaction and the execution of a contract, form accurate information data for accounting, allow you to quickly and regularly create reports [7].

Smart contracts based on blockchain technologies are aimed at significantly changing the business relationships of business structures. They demonstrate a high potential for transforming supply chains, have successful implementation in the financial sector (operations with securities and derivatives), retail (vending machines), insurance (self-fulfilling insurance contracts), transport (car rental agreements), etc. The blockchain platforms used in this process, with their cryptographic and consensus mechanisms, ensure the integrity of transactions and a high degree of protection against unauthorized access [8].

In relation to Technopolis's, the implementation of the "smart city" concept is aimed at ensuring integration interaction not only between resident companies within the Technopolis, but also with society, by creating a unified information and communication environment that provides collaboration of interaction processes of all participants involved in the development and promotion of innovative products and services. Smart contract tools and blockchain technologies that support them become an integral part of such a digital environment, providing their own opportunities and advantages to increase the innovative potential of interacting structures within the framework of "smart cities". Study the build interact to meet needs in a variety of forms of information support the ongoing transaction management structures, like science parks, leads to the need analysis information security as a whole structure and its components, and estimates the degree of influence of models of functioning of science in information technology the implementation of the interaction. In this regard, the issues of digital security of structures such as Technopolis are in the zone of close attention.

2. MATERIALS AND METHODS

When conducting the research, the authors based on statistical research methods covering 169 technoparks operating on the territory of the Russian Federation and including Indonesian resident companies for the period from 2016 to 2019. Sources of obtaining data on information transparency of science as a core build "smart cities", their contribution to sustainable development of

the country were the results of a survey of representatives of management companies, the Association of clusters and science parks of Russia analytical report of the Ministry of industry and trade of the Russian Federation, as well as annual reports on the activities of domestic and foreign Special economic zones in the public domain.

When preparing recommendations for monitoring the implementation of projects in the field of business transformation in the "smart city", Russian and foreign standards for digital security were taken as a basis [9]. When using methods for comparing typical digital threats characteristic of domestic and foreign "smart cities", the classical infrastructure and service component of the interaction model were taken into account [10]. The issues of digital security of "smart cities" were considered taking into account the specifics of the model of functioning of basic technopolises:

infrastructure model (11% of technoparks in the sample) - used when there is a large number of available space for medium-sized businesses;

innovation model (35% of technoparks) - typical for the proximity of enterprises to research centers;

the cooperative model (40% of technoparks) is in demand for localization of high-tech and high-tech products;

the University model (14% of technoparks) is focused mainly on the commercialization of scientific developments.

Also in the study of digital activities of the technopolises in terms of making smart trades taken into the consideration their peculiarities, manifested in the form of transaction on transfer of intellectual property rights, the implementation of the terms of the license agreements, storage and exchange of data about innovation and innovation participants of interaction and monitoring the use of rights and licenses [11].Standard forms of interaction for supply chains and other business operations are considered as basic forms of smart contracts.

Types of models for the functioning of basic technopolises produce the possibility of using smart contracts and are linked to the technologies of blockchain systems for their implementation. Table 1 presents a comparative characteristic of selected blockchain platforms and an expert assessment of comparison with variants of the basic models of technopolises.

Table 1 Summary of blockchain platforms

№	The name of the platform	Key feature	The main orientation	Options for choosing the base model of technopolises *
1	Ethereum	Prevalence, open source, flexibility, wide range of programming languages	Smart contracts	All type
2	Big Chain DB	Open source, sustainability, comprehensive functionality, high speed of data processing	Storing a large amount of data Support for custom digital assets.	Innovative Cooperative
3	Hyperledger Fabric	Flexibility, reliability, scalability	The corporate segment Public blockchains	All type
4	Hyperledger Cello	It is also an operating system	Blockchain-as-a-service (BaaS)	All type
5	Hyperledger Sawtooth Lake	Ability to describe the business logic of contracts using Python	The corporate segment Support for custom digital assets	Infrastructural Innovative Cooperative
6	Hydrachain	Ethereum extension, open source	Creating smart contracts in Python	Infrastructural Innovative Cooperative
7	Chain Core	Open source	Issuance, transfer and management of digital assets	Innovative Cooperative

8	Corda	Open code, development of interoperable blockchain networks	The corporate segment	All type
9	Quorum	Open source, private code functionality blockchain	Financial sector	Innovative Cooperative

* expert evaluation

In this regard, the issues of ensuring the information security of "smart" transactions are tied to the security assessment of the blockchain platforms themselves and, consequently, add additional conditions to the construction of a secure digital environment of technopolises.

The analysis of the mechanisms for implementing smart contracts allowed us to support the position [12] that suggests considering the business processes of interaction between resident organizations of Technopolis with the management company and the external environment as prototypes of smart contracts. This conclusion allows us to include in the analysis of digital security threats and vulnerabilities characteristic of such business processes, taking into account the fact that their specificity will also be determined by a variant of the basic model of functioning of technopolises.

3. DISCUSSION

The authors support the view of researchers that the digital security of a "smart city"consists of a number of components from those in the country standards for information security of cyber-physical systems, policy in the field of geolocation data, usage business of biometric technologies used to format connecting mobile devices to cloud data and the industrial Internet of things [13].

The higher transparency of the Technopark as the core of smart cities, the larger investment management company in the security infrastructure used to store and process big data within a single digital platform for the integration of residents. The key costs in this case are the costs of data encryption, information system administration tools, and network infrastructure [14].

At the same time, it is possible to argue with the opinion of a number of researchers that the digital security of a "smart city" depends solely on the organization of effective protection of the cloud services used in the interaction of the management company, residents and public authorities within a single digital platform [15]. In the context of increasing radical changes in the business model in the "smart city", digital security should be considered in the relationship between the level of maturity of business processes of Technopolis resident organizations and newly introduced innovative information technologies. The completed work is in trend with foreign research carried out about business transformation in accordance with the concept of “industry 4.0”.

Thus, the main research on smart contract threats is focused on the software and technical implementation of such transactions: incompatibility of user interfaces, computer system failures, technical failures of Internet services, code violations, scaling problems, reduced bandwidth, and so on [16]. To a lesser extent, the assessment of direct and/or indirect losses due to errors or improper operation of internal business processes, personnel, or as a result of external events, such as: lack of reliable backup / failover mechanisms in case of any risk events; possible transfer of vulnerabilities of other systems(in case of dependence on them to fulfill the terms of the contract); lack of critical system guarantees and customer protection in the terms of contracts; operational failures or poor management of digital assets, etc. A separate discussion is held on the emerging legal risks of the General plan and compliance risks arising from the implementation of smart contracts [17].

It is worth recognizing that the legal aspect of smart contracts is not sufficiently covered. In connection with the characteristic direction of the parks and resident companies for innovation activity is considered a significant need to bridge the gap between legal semantics smart contract, business semantics and the regulatory semantics of and between semantic translation, performed by a computer and its operating activities, with the assurance and guarantee of the empirical reliability of the information [18, 19]. This requires certain efforts to include semantic security mechanisms in the digital environment of technopolises when concluding smart deals by creating an ontological database of smart contracts containing the semantics of such contracts.

4. RESULTS

Information openness of technoparks as the core of building a "smart city" was evaluated based on the quality of information provided on the management company's website, the results of testing the performance of residents personal accounts when interacting with potential investors, as well as public authorities.

The results of the authors 'study of the relationship between the levels of information openness of Technopolis as the core of building a "smart city" and the development of business processes (in the CMMI ideology-Capability Maturity Model Integrated) are presented below (table 2).

Table 2 The relationship between the levels of information openness of technopolises and the development of business processes

Name of the Technopark (including foreign residents)	Technopolis information openness index and contribution to the sustainable development of the economy	Specialization of Technopolis	Infrastructure of the Technopark	Degree of development of business processes
«IT-park»	1,455	multi-industry, information and communication technologies, aviation, automobile industry, aerospace industry, mechanical engineering, new materials, medical industry	engineering center, prototyping center, data center, center for collective use of equipment, technology transfer center, additive technology center, customs post	optimizable
Technopark “Istok”	1,430			optimizable
"high-tech Technopark”	1,395			optimizable
Technopolis "Moscow”	1,376			optimizable
Technopark "Zhigulevskaya valley”	1,329			integrable
Technopark “ELMA”	1,273			integrable
Technopark «Sarov»	1,250			integrable
Technopark «Mosgormash»	1,250			integrable
Industrial technopark «IKSEl»	1,249			controlled
Technopark «Perm»	1,227			controlled
High-tech technopark «Rameev»	1,221			controlled
«Kuzbass technopark»	1,200			controlled

The study showed that for technoparks that have the highest number of points for information openness, the leaders are those that have the most complete infrastructure, from the presence of engineering centers to technology transfer centers. Technoparks "it", "Istok", "Technopark of high technologies" and "Moscow" scored from 1.376 to 1.455 values of the information openness index. They are characterized by the predominance of business processes classified as "optimized" according to the digital maturity model [20, 21]. Technoparks with an information openness index value from 1,250 to 1,329 (Mosgormash, Sarov, ELMA, Zhigulevskaya Dolina) have" integrated "business processes. And "managed" business processes are typical for the technoparks "Ixel", "Perm", "Rameyev" and "Kuzbass Technopark" (the value

of the information openness index is in the range from 1.2 to 1.249).

"Managed" business processes are characterized by a variety of information systems/technologies that allow residents of Technopolis to automate design, technological preparation of production, production itself, and logistics. The identification of" integrated " business processes allows us to talk about the use of digital duplicates and shadows in the production of high-tech products by resident companies in cooperation with participants from other clusters of the same Technopolis. "Optimized" business processes imply product lifecycle management based on a single digital platform that provides prompt coordination with government authorities on certification issues, preferential taxation, and transfer pricing [22].

Based on the specifics of ongoing business processes in Technopolis, as a prototype of a "smart city", digital security can be provided by using the following tools [23].

1. Enhanced qualified digital signatures of employees responsible for bidding. Corporate data service bus for integration of information systems of participants in transactions and smart contracts.
2. Digital prototyping of products using cloud data storage.
3. data exchange Technology in the mode of permission to open electronic documents from external computer-aided design systems, as well as a" reference model for importing data.
4. A model for filtering the content of participants in a single digital platform.

The degree of development of business processes, taking into account their representation as a prototype of smart contracts for the management company and its residents, ensures the effectiveness of overcoming vulnerabilities and threats of smart contracts themselves in terms of a formal description of the technology for their conclusion and implementation, as well as in terms of preventing various manipulations by insiders in the form of making deliberate errors, implementing software code for reading confidential information, intentionally managing smart contracts by getting a response to certain events or input data, dissemination of distorted information about the intentions of one or more Contracting parties when entering into a contract [24]. The best results in the field of digital security should be expected from technoparks and technopolises with an "optimized" level of business process maturity, and, consequently, the implementation of smart contracts in such structures will be less affected by the risks and threats considered.

The General structure of the digital security components of technopolises, reflecting the approach to their representation through the prototype of a "smart" city with the allocation of a smart contact as an element, is shown in figure 1.

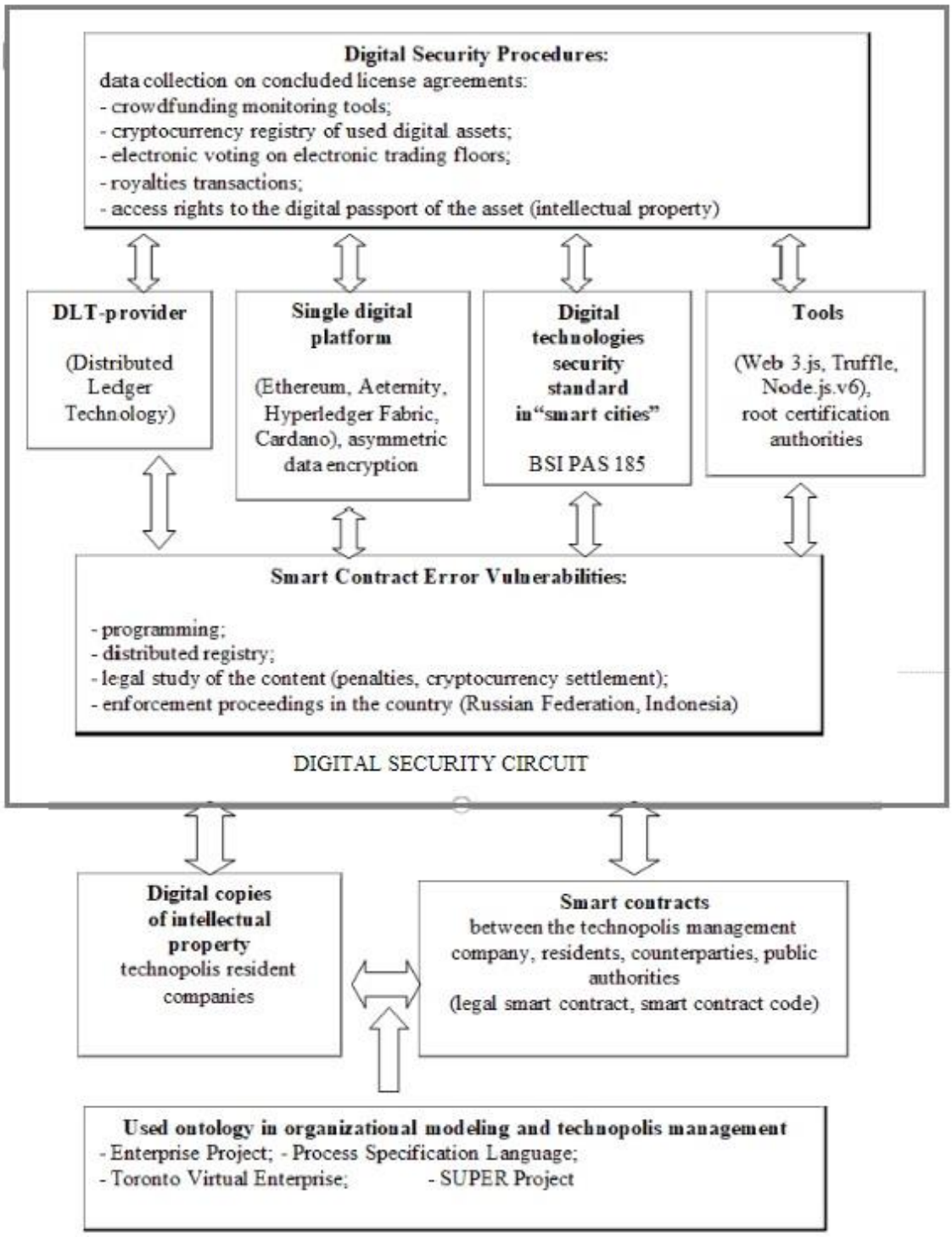

Figure 1 Key components of technopolis digital security as a prototype of a "smart city" (the author's model)

5. CONCLUSION

Digital security of technopolises as a prototype for building a "smart city" is easier to ensure by placing resident companies on Greenfield squares, rather than brownfield. Currently, the focus on organizing effective interaction in the digital environment between the management company of Technopolis, residents and public authorities is shifting to the protection of transactions in the field of specialized, rather than basic services. Services in the field of digital reverse engineering, BIM technology and digital prototyping of products are in demand. The competitiveness of an organization is not in the sphere of automation of internal business processes, but processes related to the external side of the company's activities.

In an unstable external environment, recommendations for monitoring projects of digital business transformation carried out within the framework of the "smart city" are based on a careful selection of information service providers and services, passing certification of the developed digital platform that allows all financial stakeholders to work on it, from investors to government authorities.

The key threats to the digital security of technoparks as prototypes of "smart cities" are: interruptions in the operation of data centers; unauthorized access of individuals to information contained in the personal accounts of resident companies; and industrial espionage against organizations engaged in scientific development and patenting on the territory of Technopolis. Monitoring the effectiveness of digital business transformation carried out within the framework of the "smart city" is based on the use of methods for managing project metrics and digital assets [25].

The study of smart contracts as a characteristic of a "smart city" on the example of technopolises revealed the dependence of potential threats and vulnerabilities on the following aspects:

- software and technical component inherent in smart contracts themselves as software code;
- choosing a blockchain platform that implements smart contracts linked to the basic models of Technopolis;
- implementation of business processes and their degree of development when considering business processes as a smart contract model;
- the semantic component necessary to ensure the empirical validity of legal categories, regulatory categories, and business semantics.

These aspects are more or less inherent in all business structures like Technopolis, which support and implement promising developments of "Industry 4.0". They also do not have a regional, industry, or country attachment. The specifics of an economic entity will be shown in the internal adjustment of elements of the digital security circuit to the actual operating conditions, taking into account the specifics of doing business. From these positions, the authors believe that the proposed model can be considered as an element model of the prototype of the core of systems for the "smart city", ensuring the protection of their information structure and business practices.

6. RESEARCH PROSPECTS

Further development of issues of ensuring digital security of "smart cities" as a factor of sustainable development of the economy of countries is in the development of common interstate standards for interaction of cyber-physical systems, the introduction of blockchain technologies in the public procurement system, as well as improving the competence of middle-level personnel when working with digital assets of the enterprise.

With the development of smart contract intellectualization capabilities and prospects for obtaining a fully intelligent solution, this part will increase attention to the issues of comparability of concluded smart contracts with the norms and legal bases of contract law, which will speed up the development of ontological models and allow identifying new aspects in the study of digital security of smart solutions for a smart city.

REFERENCES

[1] D. Mourtzis, E. Vlachou, Cloud-based cyber-physical systems and quality of services, The TQM Journal 28(50) (2016) 704-733. DOI: 10.1108/TQM-10-2015-0133

[2] V.V. Borisova, E.E. Panfilova, P.V. Zhukov, S.N. Matulis, V.V. Matveev, V.E. Teymurova, Information support in the enterprise risk management, International Journal of Management and Business Research 9(1) (2019) 158-169.

[3] E.E. Panfilova, A.I. Tikhonov, A.V. Savin, Competitive Advantages of Innovative Development of High-Tech Manufactures Based on the Creation of Special Economic Zones, in: Bogoviz A., Ragulina Y. (Eds.), Industry Competitiveness: Digitalization, Management, and Integration, ISCI 2019, Lecture Notes in Networks and Systems, Springer, Cham, vol. 115., 2020, pp. 39-47. DOI: 10.1007/978-3-030-40749-0_5

[4] M. Kaulartz, Smart Contract Dispute Resolution, Smart Contracts (2019) 73-83, Available at: https://www.jstor.org/stable/j.ctvn96h9r.8.

[5] M. Angelidou, Smart city planning and development shortcomings, TeMA - Journal of Land Use, Mobility and Environment 10(1) (2017) 77-94. DOI: 10.6092/1970-9870/4032

[6] K. Werbach, The Promise — and Perils — of 'Smart' Contracts, May 18, 2017, Available at: http://knowledge.wharton.upenn.edu/article/what-are-smart-contracts/.

[7] A Primeron Smart Contracts, CFTC's Lab CFTC Press Releases, 2018, Available at: https://www.cftc.gov/PressRoom/PressReleases/7847-18.

[8] A.M. Rozario, M.A. Vasarhelyi, Auditing with Smart Contracts, The International Journal of Digital Accounting Research 18 (2018) 1-27. DOI: 10.4192/1577-8517-v18_1

[9] Yu.A. Rodichev, The regulatory framework and standards in the field of information security: a training manual, Piter 2017.

[10] I. Karabulatova, Kh. Vildanov, A. Zinchenko, E. Vasilishina, A. Vassilenko, Problems of transformation matrices modern multicultural identity of the person in the variability of the discourse of identity Electronic Information Society, Pertanika Journal of Social Science & Humanities 25(S) (2017) 1-16.

[11] A.G. Finogeev, L.A. Hamidullaev, S.M. Vasin, A.A. Finogeev, V.V. Pronichev, A.M. Lychagin, Smart

contracts as a tool for safe interaction of subjects in the regional innovation system, News of higher educational institutions. The Volga region. Social sciences 3(47) (2018) 139-157.

[12] A.V. Cardonov, Spheres of smart contracts application and risks when working with them, Business education in the knowledge economy 1 (2018) 44-46.

[13] J.R. Gil-Garcia, T.A. Pardo, Taewoo Nam, What makes a city smart? Identifying core components and proposing an integrative and comprehensive conceptualization, Information Polity 20(1) (2015) 61-87. DOI: https://doi.org/10.3233/IP-150354

[14] I.A. Antipin, O.Y. Ivanova, Digitalization as a Direction of Neo-Industrial Transformation of Strategic Urban Development in the Ural Macroregion, in: A. Bogoviz, Y. Ragulina (Eds.), Industry Competitiveness: Digitalization, Management, and Integration, ISCI 2019, Lecture Notes in Networks and Systems, Springer, Cham., vol. 115, 2020, pp. 67-75. DOI: 10.1007/978-3-030-40749-0_8

[15] C. Martinez-Olvera, J. Mora-Vargas, A Comprehensive Framework for the Analysis of Industry 4.0 Value Domains, Sustainability 11(10) (2019) 1-21.

[16] N.A. Naraliyev, D.I. Samal, Review and analysis of standards and protocols in the field of Internet of Things. Modern testing methods and problems of information security IoT, International Journal of Open Information Technologies 7,8 (2019) 94-104.

[17] N.V. Lukoyanov, Legal aspects of the conclusion, amendment and termination of smart contracts, Legal Studies 11 (2018) 25-28. DOI: 10.25136 2409-7136.2018.11.28115

[18] F. Al Khalil, M. Ceci, L. O'Brien, T. Butler, A Solution for the Problems of Translation and Transparency in Smart Contracts, Government Risk and Compliance Technology Centre (2017), Available at: http://www. grctc. com/wp-content/uploads/2017/06/GRCTC-Smart-Contracts-White-Paper-2017.

[19] M. Ko'lvart, M. Poola, A. Rull, Smart Contracts, in: T. Kerikma'e, A. Rull (Eds.), The Future of Law and eTechnologies, Springer International Publishing Switzerland, 2016, pp. 133-147. DOI: 10.1007/978-3-319-26896-5

[20] Mercosur to reduce reliance on foreign technology over spying, Xinhua, 26.01.2020, Available at: http://news.xinhuanet.com/english/world/2013-07/17/c_132548966.htm.

[21] Y. Liu, X. Xu, Industry 4.0 and cloud manufacturing: a comparative analysis, Journal of Manufacturing Science and Engineering 139(3) (2016) 1-8. DOI: 10.1115/1.4034667

[22] E.V. Zenkina, Information transport and Internet communications as part of a modern transport system, Economics and Entrepreneurship 4 (2018) 678-681.

[23] G. Adamson, W. Lihui, M. Holm, P. Moore, Cloud manufacturing – a critical review of recent development and future trends, International Journal of Computer Integrated Manufacturing 30(4-5) (2017) 347-380. DOI: 10.1080/0951192X.2015.1031704

[24] V.V. Borisova, O.V. Demkina, A.V. Savin, Digitalization Risks of Industrial Companies, Innovations and Investments 12 (2019) 294-297.

[25] Sanne van der Lugt, A smart Smart City plan: The importance of controlling the flow and storage of 'the new coal, Oct. 1, Research Report, Clingendael Institute, 2019, Available at: https://www.jstor.org/stable/resrep21326.