Smart City Ecosystem Using Blockchain Technology

Carmen ROTUNĂ, Alexandru GHEORGHIȚĂ, Alin ZAMFIROIU, Dragoș SMADA
ANAGRAMA
carmen.rotuna@anagrama.ro, alexandru.gheorghiță@anagrama.ro,
alin.zamfiroiu@anagrama.ro, dragos.smada@anagrama.ro

Given the continuous development of urban areas, integrated policies are needed to improve the lives of urban residents by implementing integrated, interoperable and secure electronic services. Public administrations recognize the potential of blockchain in solving the problems of local communities. Blockchain, initially perceived through its association with cryptocurrency bitcoin, offers an innovative perspective on how smart cities can be organized and a more transparent economic model for resource management. This study analyses how blockchain technology-based services can contribute to the development of smart cities and proposes a Smart City ecosystem model based on SSI (Self-Sovereign Identity) authentication model and smart contracts between entities, citizens and administrations. It also overviews the domains in which this technology can be used. The results can be a starting point for the development of local initiatives for using the blockchain as a platform for communications and transactions in the public sector.
Keywords: *Blockchain, Smart City, SSI, IoT, Smart Contracts*

1 Introduction

Worldwide, the number of inhabitants in urban areas is increasing, so 68% of the world's population is expected to live in urban areas by 2050 [1]. As cities continue to grow, sustainable development is increasingly dependent on the successful management of urban growth, especially in low- and middle-income countries, where urbanization is expected to be the fastest. Most countries will face challenges in providing services to the population, including housing, transportation, energy systems, infrastructure, employment, as well as basic services, such as healthcare and education. Integrated policies are needed to improve the lives of urban and rural residents, while strengthening the links between urban and rural areas, based on existing economic, social and environmental links.

Smart cities based on IoT technologies can contribute to improving the quality of life, but this "smart" urban landscape, with numerous connected devices and a large communications network, creates new security challenges - challenges that cannot be easily addressed by conventional cyber security solutions.

1.1 Smart Cities

The Smart City concept is defined in the literature in different ways. Komninos defines smart cities and regions as environments with a high capacity for learning and innovation, incorporating the creativity of population and institutions with digital infrastructures to operate in the physical, institutional and digital spaces of cities. The ambiguity of this concept causes difficulties in understanding how the adoption of information technology influences the development of smart cities. [2][3][4].

Smart City is a collection of paradigms spread across different domains: economy, people, government, mobility, environment and life [5] [6] and addresses a variety of use cases : environmental monitoring, traffic analysis, utility monitoring, smart public transport, electronic voting system, e-commerce, jobs, local events, real-time incident reporting, medical services, etc. The analysis of data collected from the above-mentioned domains allows the city administration to improve the infrastructure and optimize its services. A smart city is also an environment with integrated information and communication technologies that creates interactive spaces

that bring computational capabilities to the physical world. [7].

A Smart City must include key components that allow data centralization, components that can take many forms, starting from a simple website to complex applications, supported by specialized hardware. The accessibility of the data should be guaranteed in a way that the system can be freely accessed by citizens, allowing them to propose changes and corrections in an interactive way.

To ensure that the benefits of urbanization are fully exploited, urban growth management policies must ensure access to electronic infrastructure and services for all residents. The acquisition of sensitive data through the Internet of Things is one of the primary objectives of smart cities, which means that ensuring the security of this data is of utmost importance.

For this reason, most administrations invest consistently in the development of smart cities with many facilities for inhabitants. The modern city is already a massive network of interconnected technologies, and according to Cisco [8], 500 billion devices are expected to be connected to the Internet by 2030. Gartner says that about 10 billion interconnected objects will be used by smart cities by 2020. [9]

1.2 Blockchain Technology

Blockchain technology first appeared in a publication by Haber and Stornetta in 1991 [10]

To understand the blockchain technology it is necessary to define some basic concepts [11]:

- **Nodes:** are the most rudimentary elements of the Blockchain. The blockchain is made up of a network of nodes. In reality the nodes are computers;
- **Transactions:** Each share in a Blockchain represents a transaction. If you want to change a value on the Blockchain a new transaction will be created, sending the virtual currency from one account to another which is also a transaction. For a transaction to be accepted, it must be approved by at least 50% +1 of the existing nodes [12];

- **Block:** represents how a blockchain holds data. A block contains data from several transactions. Each block is linked to the previous block by a cryptographic hash. All these blocks are stored in each node;
- **Account:** Blockchain accounts are made up of two variables, a private key and a public key. The account is owned by the private key holder. Unlike other centralized technologies, in Blockchain if the private key was lost there is no possibility to claim the account, there is no way "I forgot the password";

Blockchain features are [13]:

- **Decentralized**, the data is in several places, as many nodes are in the network [14];
- **Scalable,** there may be an infinite number of nodes in the network;
- **Safe / Secure,** with current technology a Blockchain is theoretically impossible to break. As already mentioned, for a transaction to be approved half plus one of the nodes in the network must accept it. If an attacker manages to modify a blockchain or alter one piece of data, a new block is created, which must be verified by all the devices within the blockchain network. Half data plus one node should be modified for a fraudulent transaction to be accepted and all should be broken at the same time. If one node has responded differently from the others, the cryptographic hash of the node is checked and node will be ignored by the network until it returns to a real data version [15].
- **Intelligent**, beyond the basic Blockchain technology it is possible to write custom code for each application separately, thus leaving room for various rules and use cases;
- **Auditable,** because each block is linked to the previous block through a hash, the Blockchain allows to navigate through all the blocks up to the "Genesis" block, the starting block of the Blockchain, thus enabling chronological tracking of all changes.

1.3 Smart Contracts

Smart Contracts are automatically executed digital contracts that require tasks to be performed by two entities to initiate a transaction. In the blockchain, a smart contract cannot be modified by either party and its terms are continuously monitored, simultaneously with the execution of the necessary steps for its fulfilment. If changes are needed, a completely new contract must be created. Smart contracts were originally conceived by Nick Szabo, as a possible method of formalizing business relations and commercial agreements in an online context, in an efficient way, compared to the classical method of paper contracts [16].

Smart Contracts are small programs, identified by an address and stored in the blockchain like any other transaction, which execute automatically when predefined conditions are met. The source code of the contracts is written in a specific programming language such as Solidity, an object-oriented, high-level language, designed for the Ethereum Virtual Machine (EVM) model. [17]

2 Blockchain Technology for Smart Cities

Initially, Blockchain technology was perceived through its association with bitcoin, but in recent years, it's possible uses have been explored in other fields of activity such as smart contracts, logistics and the management of systems comprising many actors. By harnessing the potential of Blockchain, researchers and developers are aiming to increase people's trust in digital communities, as well as local ones [18]. This can be easily accomplished by Blockchain systems through their decentralized and open nature, providing a single source of truth and a single starting point for new initiatives.

In [19] domain and applications of using blockchain technology in cybersecurity are presented. These are shown in Figure 1.
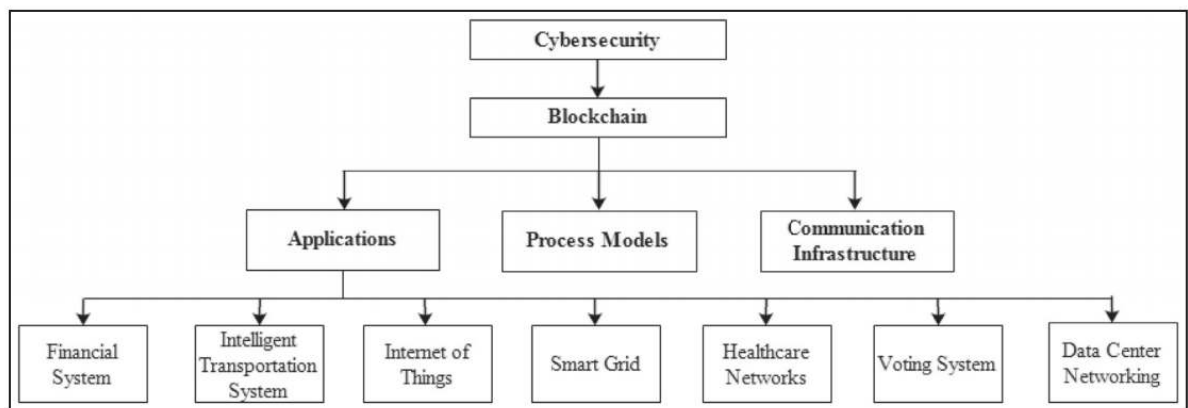
Fig. 1. Domains of using the blockchain technology [19]

Blockchain technology has the capacity to increase the transparency of local and regional institutions, while facilitating the communication of sensitive data without compromising security and confidentiality. In this sense, blockchain can be used in the development of smart cities as an interoperable platform that allows citizens to actively participate in the decision-making processes that affect the communities they belong to. It can also serve as a tool for managing the reputation of companies in relation to the activity related to the environment.

The administration of a smart city through its systems, generates a considerable volume of sensitive data that requires an oversized storage environment on which to intervene in a secure way and according to a predetermined policy of accessing this data. According to recent data, cyber-attacks are still a real security issue when it comes to online transactions. To mitigate the effects of these phenomena, blockchain technology uses a distributed model that increases the degree

of entropy, implicitly reducing the vulnerability of the systems it supports.

The technology-based cryptography architecture makes it unlikely that transactions will be reversed or altered. Whenever a new transaction is broadcast on the network, the nodes have the obligation to validate and include it in the copy of the distributed ledger and in case of invalidation, it must ignore it. When most of the participants that make up the network decide on a single state, a consensus is reached. In addition, all participants in the system have a personal key or signature that is used when creating a transaction. This key allows the association between the user who created a particular transaction and the recipient of that transaction. At the same time, because the ledger is distributed and validated by the entire network, a transaction is associated with a single user and cannot be registered multiple times on the blockchain. [20] [21]

3 Blockchain Use Cases for the Development of Smart Cities

A smart city offers its citizens the facility to interact with public administration and local communities, using digital technologies for increased efficiency and security. By its persistent and at the same time distributed storage, blockchain allows the development of a large number of new interaction models, which could not be designed within a centralized model.

Public administrations are beginning to recognize the potential of the blockchain model as a platform for communication and transactions in the implementation of electronic services for local communities. The following study analyses the areas where this technology can be implemented for smart cities development.

3.1 Digital Identity and SSI

Digital identity is the information about an entity, used by information systems to represent an external agent, which can be a person, an organization, an application or a device. ISO 24760-1 defines identity as an "entity-related set of attributes". [22] Digital identity data allows the automatic authentication of a user interacting with a system and enables the access to the services provided by the system.

Self-Sovereign Identity (SSI) is a type of digital identity that allows the user complete and final control of his identity. Through SSI, users or companies can store their identity data on their devices and can effectively provide them to those who need to validate them. Thus, the user manages through an application, on mobile or computer, the elements that make up the identity and controls the access to this set of information. Identity data may include: birth dates, citizenship, university diplomas or licenses. [23]

Within the application, the user is initially assigned a self-generated identification number derived from the public key and a corresponding private key. This key pair is different from the combination of username and password, because after it is created by the user, automatic mathematical calculations are performed over it, which makes decryption almost impossible.

Fig. 2. Classical identification vs SSI [24]

This type of identity can be implemented to identify the citizens of a smart city using blockchain technology which ensures storage, secure timestamping and decentralized hosting. This model eliminates the need for passwords and guarantees authentication with a high degree of security.

An example of successful implementation is the Estonian e-Residency program which allows users outside the EU to create a digital identity that can be used to set up a business in Estonia [4].

3.2 Security of IoT Devices
The implementation of an IoT system involves the operation and management of a large number of decoupled and distributed smart devices, which communicate securely. Current solutions are largely based on centralized infrastructures that have the disadvantages of high maintenance costs, low interoperability and susceptibility to cyber attacks.

Blockchain technology can be used to protect IoT systems and devices such as temperature sensors, security cameras, air quality sensors, etc., from possible attacks, as it enables devices to make security decisions without relying on a central authority.

The implementation of a blockchain platform can ensure secure data transmission between IoT devices located tens or hundreds of kilometers away, in a smart city, in real time,

in the absence of a central authority that controls all transferred data.

Decentralizing an IoT solution brings benefits, including reducing the amount of data transferred to the cloud for processing and analysis, and improving data security and confidentiality. In this scenario an eventual attack would be much harder to implement. The blockchain platform can ensure the interconnection of smart devices from several areas of activity such as:

- public lighting systems that enable remote control and operation of lighting in public spaces and can be adjusted according to predetermined parameters, such as weather or time.
- intelligent waste management systems that monitor the level of waste in containers and recommend optimal collection routes, thus ensuring fuel savings for waste collection trucks.
- municipal fleet systems with sensors that allow real-time tracking of vehicles and remote management of efficient routes.
- systems for monitoring the operational capabilities of the infrastructure components for municipal utilities which alert the assistance personnel whenever a problem is detected.
- rapid emergency response systems that can be automated to improve response time and resources distribution.
- systems for detecting environmental parameters that use sensors to measure

pollutant levels and contribute to maintaining a healthy environment for residents.

3.3 Security in Private Messages

Private messages are an important type of data in a smart city as it facilitates the interaction of citizens with the public administration to report incidents, receive clarifications regarding administrative procedures, announce cultural events etc.

Currently, most messaging applications lack a standard set of security protocols and a framework to enable communications between them. A blockchain-based communication system that will allow data exchange and connection between different messaging platforms can solve this problem. The essential capability of the blockchain in this context is decentralization as a method of cyber security. When access control, network traffic and even data itself are no longer held in one location, it becomes much more difficult for attackers to exploit the system.

3.4 Autonomous Vehicles

Artificial intelligence in the automotive domain is constantly developing and self-driving cars are seen as cars of the future, given that big manufacturers are already investing large amounts in their research and development. At this point, semi-autonomous systems that require the presence of the driver are already being used, but it is expected that in the near future the autonomous car technology will be widespread.

In order to operate, an autonomous vehicle is dependent on information about the surroundings, such as route information used by the navigation system, traffic information, availability of power/fuel services, driver license validity, road taxes, speed controls, parking places and parking reservation, etc.

The transfer of this data can be done in a secure way through blockchain technology. It has the potential to enable interaction between users of autonomous cars and local electronic services, highway and traffic management systems, local police, parking systems etc., in a Smart City ecosystem. At the same time, information regarding the user's behaviour of an autonomous vehicle such as the driver's behaviour, the actions of the vehicle and the ability of the driver to comply with the traffic rules can be recorded. At the same time, makes it possible to record information regarding the behaviour of the user of an autonomous vehicle such as the driver's behaviour, the actions of the vehicle and the ability of the driver to comply with traffic rules.

4 Blockchain Architecture for Smart City

Smart cities use different technologies and infrastructure to ensure a better quality of life for urban residents, a good environment for business development, optimization of resource use and transparency for public administration. These goals can be achieved by using blockchain that acts as a tool for decentralized and distributed ecosystems. Features as security and transparency, shared information, common updating of the database and information validation, provided by blockchain technology, empowers all smart city use cases.

Blockchain technology allows interactions between citizens and local government without the need for a central authority, in a distributed manner. Smart contracts optimize the functioning of the smart community through their ability to automatically execute transactions without the intervention of an operator.

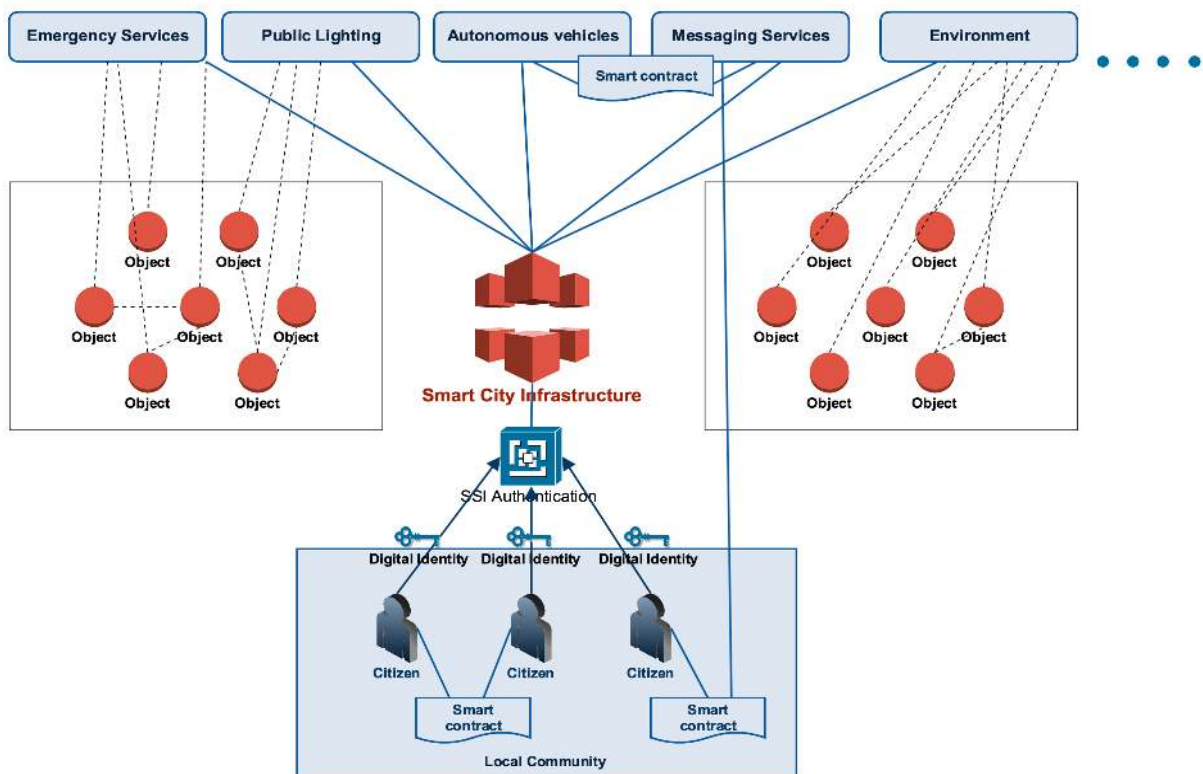A blockchain-based Smart City model using SSI is illustrated in Figure 3.

Fig. 3. Blockchain Model for a Smart City

Blockchain infrastructure connects the local community with public administration. The access to the ledger is allowed to all community members and each member has their own synchronized copy of the common ledger. Also, every participant has a Digital Self-Sovereign Identity that is used to authenticate the person in transactions. The use of central authorities is replaced by a community of peers in the form of an interconnected network where each peer has his own identity. The ecosystem comprises IoT devices located in different locations, which record and transmit securely real-time data about city environment. Also, different types of Smart contracts can be defined between citizens, between public authorities and between citizens and public authorities for services. Smart contracts are stored on the blockchain which reduces fraud attempts.

5 Conclusions
Rapid urban growth raises new infrastructure problems for public administrations. As cities develop and expand their services, governance and management are becoming more and more complex. Consequently, cities must adapt to address the economic, social, engineering and environmental challenges of these transformations. Cities must become smart to face the challenges properly [25].

Although it was originally created as a digital platform for cryptocurrencies and financial transactions, blockchain has many other potential applications in various areas, including city management.

A Smart City relies on components that allow data collection and storage, supported by specialized hardware infrastructure. An important aspect to consider is ensuring the interoperability of new applications with existing ones, so it is reused existing infrastructure, where possible.

A smart city uses digital technologies to improve the quality and performance of urban services for citizens. Citizens' access to Smart City applications must be guaranteed in an interactive way, so that they can access and transmit, as the case may be, real-time information. City officials and local administrations of a smart city based on a blockchain would benefit from a completely new way of connecting with citizens and visitors.

Studies show that the increased rate in urbanization is putting pressure on the nowadays infrastructures. In order to support the growing population in the big cities, a new type of smart infrastructure is needed, capable of supporting both efficiency of services and quality of life. Blockchain is a promising solution for a wide range of challenges faced by a smart city, but the implementation depends on the city administration and the needs of the community. A blockchain based Smart City infrastructure has the advantages of increased efficiency due to the automated interactions with its citizens, optimized distribution of resources and fraud reduction.

References
[1] United nations Organization (ONU), Revision of world urbanization prospects, 2018 https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html
[2] Komninos, Nicos. (2006). The Architecture of Intelligent Cities.
[3] Komninos, N., Intelligent Cities: Innovation, knowledge systems and digital spaces, London and New York, Spon Press, 2002.
[4] Nasulea, Christian & Mic, Stelian-Mihai. (2018). Using Blockchain as a Platform for Smart Cities. Journal of E-Technology. 9. 37. 10.6025/jet/2018/9/2/37-43.
[5] Gori P, Parcu PL, Stasi ML (2015) Smart Cities and Sharing Economy, vol 96, Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS
[6] Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. Journal of Urban Technology, 22(1), 3-21.
[7] Steventon, A., and Wright, S. (eds), 2006, Intelligent spaces: The application of pervasive ICT, London, Springer.
[8] Cisco, Internet of things at-a-glance, 2016, https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf
[9] Gartner, Smart Cities Will Include 10 Billion Things by 2020, 2015, https://www.gartner.com/en/documents/3004417
[10] Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.
[11] 6 Key Features of Blockchain: This is what makes Blockchain so exciting! Online: https://thefintechway.com/6-key-features-of-blockchain/. Accessed: October 2019
[12] Pal, O., Alam, B., Thakur, V., & Singh, S. (2019). Key management for blockchain technology. ICT Express.
[13] Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. Journal of Industrial Information Integration, 13, 32-39.
[14] Lee, J. Y. (2019). A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. Business Horizons, 62(6), 773-784.
[15] Hebert, C., & Di Cerbo, F. (2019). Secure blockchain in the enterprise: A methodology. Pervasive and Mobile Computing, 101038.
[16] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," EXTROPY: The Journal of Transhumanist Thought, vol. 16, 1996.
[17] Boncea, R., Petre, I., & Vevera, V. Building trust among things in omniscient Internet using Blockchain Technology,

Romanian Cyber Security Journal, Spring 2019, No. 1, vol. 1

[18] Tapscott Don and Alex, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World, ISBN 0241237858, Toronto, Penguin 2016.

[19] Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K. K. R., & Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications.

[20] Beck, Roman & Müller-Bloch, Christoph. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization. 10.24251/HICSS.2017.653.

[21] Swan, M. Blockchain: Blueprint for a new economy, O'Reilly Media Inc, Sebastopol, CA, 2015

[22] ISO 24760-1: A framework for identity management - Part 1: Terminology and concepts", ISO, 2019, https://www.iso.org/standard/77582.html

[23] Smolensky N, Identity and Digital Self-Sovereignty, 2016, https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3 - .3jcgvnbok

[24] Paul Payam Almasi, 2019, The Identity Revolution - Self Sovereign Powered by Blockchain https://blog.goodaudience.com/how-blockchain-could-become-the-onramp-towards-self-sovereign-identity-dd234a0ea2a3

[25] Vranken Jan, Social Challenges of Cities of Tomorrow, Centre OASeS, 2011, https://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/citiesoftomorrow/citiesoftomorrow_social.pdf

Carmen ROTUNĂ has graduated the Faculty of Mathematics and Computer Science, University of Bucharest Database and web technologies Master program. Currently she works as a Scientific Researcher with expertise in Software engineering, eHealth, eServices, eGovernment, IoT, Big data I.C.I Bucharest and Anagrama. She was a team member in several international and Romanian research projects, three of them in the eServices domain: "Simple Procedures Online for Cross-border Services (SPOCS)", Electronic Simple European Networked Services(e-SENS) and The once only principle project(TOOP), where she is currently the WP2 leading architect for the Romanian team and piloting coordinator. She published several articles, co-authored project deliverables and collaborates as a reviewer for scientific publication

Cristian-Alexandru GHEORGHIȚĂ graduated the Faculty of Informatics in 2013. He is a PhD student at Politehnica University of Bucharest, Faculty of Computer Science and Automatics. Currently he works as Researcher at I.C.I Bucharest and Anagrama. His main areas of interest are Cyber Security, Big Data, Cloud Computing, blockchain, software engineering, machine learning, digital libraries. He is involved in research projects specific to the Information Society. His research was published in journal articles and proceedings of conferences.

Alin ZAMFIROIU has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2009. In 2011 he has graduated the Economic Informatics Master program organized by the Bucharest University of Economic Studies and in 2014 he finished his PhD research in Economic Informatics at the Bucharest University of Economic Studies. Currently he works like a university lecturer at Bucharest University of Economic Studies and like a Senior

Researcher at I.C.I Bucharest and Anagrama. He has published as author and co-author of journal articles and scientific presentations at conferences.

Dragoș SMADA graduated the Faculty of Electronics, Telecommunications and Information Technology at the Polytechnic University of Bucharest. He has a Master's Degree in Information and Documents Management at the University of Bucharest. He is currently a scientific researcher at ICI Bucharest and Anagrama. His main areas of interest are Big Data, Internet of Things, software engineering, information security, software architecure. He participated in both national and international research projects in the IT&C. He published as author and co-author of journal articles and scientific presentations at conferences.