CRITICAL INFRASTRUCTURE INFORMATION MANAGEMENT. REQUESTS AND PROPOSALS

Dragoș DANȚIȘ
Bucharest University of Economic Studies, Bucharest, Romania
dragos.dantis@gmail.com

Ana Gabriela ANUȚOIU
Transylvania University of Brașov, Brașov, Romania
gabriela.anutoiu@yahoo.com

Abstract

Latterly the community systems are influenced by disruptive scenarios, in practical terms various factors impacting on the effective running of social processes. Among the actors present in the life cycle of the community processes are enlisted the subjects, with roles in the protection and governance of critical infrastructures. Organizations covering these roles have to act accordingly, gathering information on the background, not only to prevent and mitigate the occurrence of risks, contemporarily to govern the operative behavior of their systems. The information collected can be managed in various modalities, using traditional databases or innovative technologies, like blockchain. Present study puts together some considerations identified in other working papers and practical aspects encountered in the management of information to discuss on requirements and proposals. Furthermore contains a high level assessment among the two existing options for particular critical infrastructures in the administration of the information, traditional databases and blockchain.

Keywords: critical infrastructure, research, finance-cryptocurrencies, environment-brown bear, blockchain.
DOI: https://doi.org/10.24818/beman/2023.13.1-03

1. INTRODUCTION

During their research the authors have seen there are different necessities arising in identifying the sources for data collection, data storage, information analysis, results construction and outcome presentation. These phases can be enrolled in a process of information governance, which can be seen as a backbone for sustaining the decision making process of any researcher or organization.

On the other side data collection, storage and access can be in itself a key factor in arriving to a proper research result. This is not limited only to the modalities in which the researchers manage their data, it extends as well to the original sources for the examination.

The need for availability of proper data has been understood as well for a long time by public authorities in two directions: as a prerequisite for their activity (act of governance) and necessity of other stakeholders, to have access to transparency and build useful knowledge on the open information. Currently are available and could be quoted to sustain the previous mentioned directions the following data sources. The first one has been developed by Romanian state (data.gov.ro), second by European authorities (data.europa.eu), while the last one by international organizations (data.worldbank.org).

In the same time, the act of governance is established on the use of information, which is not available in all the cases, accessible only partially or in an aggregated form to the people, due to the reserved character it has behind. This information is stored in protected environments of public entities, which through the functions empowered by the legislation arrive under the umbrella of critical infrastructures.

Nowadays, in addition to the functions performed by the state agencies, there are numerous examples of private organizations that complete the portfolio of what is understood as critical infrastructures.

Writers of this article accomplish their research in fields closely linked to the range of critical infrastructures, specifically, in finance (impact of cryptocurrencies on monetary system) and environment (status of brown bear in Romania) and have seen the importance of proper information governance. As well, they have the interest to understand if innovation, through one of its elements – blockchain - can sustain above mentioned process.

This interest has materialized in a first instance in a wider manner on the use of blockchain technology in finance (Danțiș, 2021) and advancement of a possible solution for the management of information related to brown bear (*Ursus arctos*) population (Anuțoiu and Danțiș, 2021).

The scope of the study case will be to comprehend if blockchain can be seen as an alternative platform to traditional databases, in the governance of information for critical infrastructures, predominantly, in the research area. This assessment will be performed by analysing two dimensions, the first one containing the characteristics identified by the essayists in their exploration, while the other encompasses a selection of technical attributes, recognized and associated to each database by technical professionals and by the authors.

2. CRITICAL INFRASTRUCTURE

At European level the critical infrastructure area is defined in the Council Directive 2008/114/EC as “an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions”.

Furthermore, the same legislative act indicates that should be evaluated with increased attention the cases when are impacted the critical infrastructures present in two or more countries of European Union and these sectors could be linked among them. Based on this definition can be understood the interdependency principle present among particular functions, especially the ones identified as European Critical Infrastructures or ECI. In this regard, considering the importance of the activity of these organizations has to be highlighted the need to adopt proper measures for their identification and protection.

In performing their roles the critical infrastructures use critical information, which may be linked to another definition provided by the Directive (European Council, 2008). According to it "sensitive critical infrastructure protection related information' means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations".

Considering the progress registered with the enhancement of technology and digital area, at European level, the protection of critical information requires mainly implementation of cybersecurity measures. As a result the European Parliament and the Council advanced the so-called Network and Information Security Directive (2016). This first step was continued by the European Commission (2022), which has announced the launch of the NIS2 Directive, proposed in December 2020. The update of the first NIS Directive has been seen as a required step for the cybersecurity area strengthening, covering a wider range of critical sectors for economy and society.

The efforts in providing better protection have materialized as well in what will be known as the Directive on the Resilience of Critical Infrastructures, which should come into force in the next period. New legislation will reinforce the "physical non-cyber resilience" and will cover eleven sectors like: "energy, transport, digital infrastructure, banking, financial market infrastructure, health, drinking water, wastewater, public administration, space and food" (European Commission, 2022).

In Romania the implementation of Council Directive 2008/114/EC has started in 2010 at national legislation level, with the adoption of Government Emergency Ordinance 98/2010 (Romanian Government, 2010), regarding the identification, designation and protection of critical infrastructures. Based on the regulation has been created the National Centre for the Coordination of Critical Infrastructures Protection or CNCPIC, in the structure of the Ministry of Internal Affairs (CNCPIC, 2022).

Under the definition provided by Emergency Ordinance 61/2019, updating the one from 2010, through national critical infrastructure is understood "an element, a system or a component, present on the national territory, which is essential for maintaining vital functions of society, health, safety, security, social and economic wellbeing of people, which if influenced or destroyed would have a significant impact at national level due to the impossibility to run those functions, or the project of a strategic national objective, which through its construction contributes to the national interest" (Romanian Government, 2019).

The Romanian legislator enforces the definition provided at EU level and mentions the functions seen as European Critical Infrastructure. Furthermore, critical information is seen as information related to the protection of the domain, which if breached would impact on the activity or destruction of critical infrastructure. For each national domain are identified several public responsible authorities to govern the organization and functioning of the critical infrastructures.

During the last years, the perimeter has extended and several updates have been registered compared to the initial version. Going through the content of the legislation (Romanian Government, 2021) and website of CNCPIC the following selection of areas and public responsible authorities has been identified (Table 1). It has to be highlighted that during the time some Ministries may have changed their naming, having a possible impact on the list of titles.

TABLE 1. NATIONAL CRITICAL INFRASTRUCTURES DOMAINS

Domain	Public Responsible Authority
Energy	The General Secretariat of Government; Ministry of Energy
Information Technology and Communication	Ministry of Research, Innovation and Digitalization
Water, Forest and Environment	Ministry of Health; Ministry of Water, Forests and Environment
Food and Agriculture	Ministry of Agriculture and Rural Development; National Authority for Animals and Food Safety; Ministry of Health
Health	Ministry of Health; Ministry of National Defence
National Security	The General Secretariat of Government; Ministry of National Defence; Ministry of Internal Affairs; Ministry of Economy; Ministry of Justice
Administration	Ministry of Development, Public Works and Administration
Transportation	Ministry of Transportation and Infrastructure
Industry	Ministry of Economy; Ministry of Energy

Space and Research	Romanian Space Agency; Ministry of Research, Innovation and Digitalization; Ministry of Education
Finance and Banking	Ministry of Public Finance; National Bank of Romania
Culture and National Cultural Heritage	Ministry of Culture

Source: amended by the authors based on national legislation and CNCPIC website content

What can be noticed from the above table is the fact that at national level there are numerous public responsible authorities, which are governing the activity of various organizations in public and/or private sector. Considering the hypothesis that most of these entities, if not all of them, perform their activities using critical information, may result an increased complexity level in managing it. The complexity may be given by various factors and may be linked to the size and nature of each organization, level of automation, skills of employees, level of security measures, portfolio of applications used, maintenance of ICT landscape and organizational resilience.

The last factor represents a core characteristic of any critical infrastructure and may have several meanings. In synthesis it represents the capability of an entity to respond to disruptive elements through integration, flexibility or transformation (Manca et al., 2017).

3. RESEARCH QUESTION

The main question of this paper is to understand if can be identified an alternative technology aside the traditional database, to support the management of critical information used by the organizations covering the functions of critical infrastructures.

4. RESEARCH METHODS

Writers of this article will choose as field to test their hypothesis the research area, indicated in the perimeter of the Romanian legislation as critical infrastructure. The foundations for the construction of the assessment case will be provided by the experience gathered by the authors inside their study process.

In a first instance information has been obtained by performing online research to have an understanding of the situations where have been identified issues in information governance, including data attacks or data breaches towards the portfolio of critical infrastructures at European level.

From what has been seen in most of the cases the issues in governance of information are linked to its protection from cyber-attacks, addressing in this case to the documents made available by European Union Agency for Cybersecurity (ENISA, 2021).

The paper indicated has been constructed by the EU agency using online collection of information from various sources and other ENISA capabilities. The organization has tried to map the content under a common framework, representing the incidents identified for the period April 2020 – July 2021.

The mapping and depiction of information under various clusters has been used afterwards to link it with the list of existing critical infrastructures in general, and research area in particular.

The case study performed consists in analyzing the following dimensions:

- characteristics of information governance identified by each writer in individual area of research: finance (cryptocurrencies) and environment (brown bear) and a brief evaluation of few business intelligence-data source platforms;
- selection of technical attributes acknowledged by specialists in the field for blockchain and features identified by the authors for traditional databases.

5. RESULTS AND DISCUSSIONS

5.1. Considerations On The Research Perimeter

According to the evaluation performed by ENISA (2021) and represented in Figure 1 can be seen that the range of cyber-attacks has been quite diverse, extensive and happened in each month of the evaluated perimeter.

More or less all the areas considered as critical infrastructures have been targeted by incidents.

The highest impact has been observed on government/public administration - 198, digital service/providers - 152, healthcare/medical - 143, finance/banking - 97 and transport - 54.

The same report mentions that cyber criminals are interested to target the critical infrastructures to disrupt their normal functioning and hiding their real objectives (ENISA, 2021).

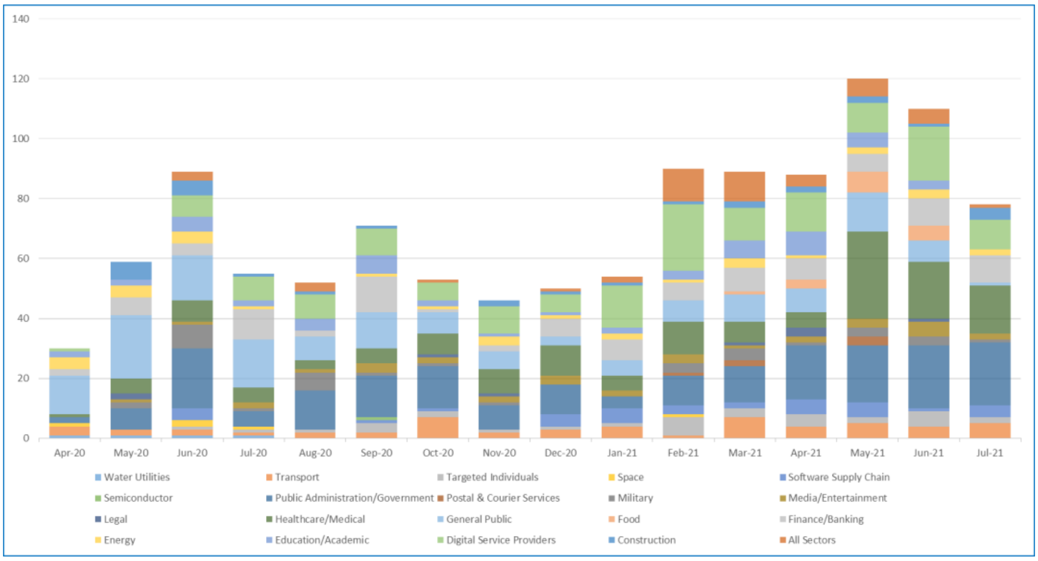


FIGURE 1. TIMELINE OF OBSERVED INCIDENTS RELATED TO PRIME ETL THREATS IN TERMS OF THE IMPACTED SECTOR

Source: created by authors based on ENISA ETL Report (2021), p. 12

It can be noticed that area of education and academic reaches a total of 52 incidents (Figure 2), which represents 4,59% in the total number of events. Even though the percentage may be seen as marginal compared to other fields, has been decided to direct the attention in this area as the education/academic or research serve as foundation for the activities of other critical infrastructures.

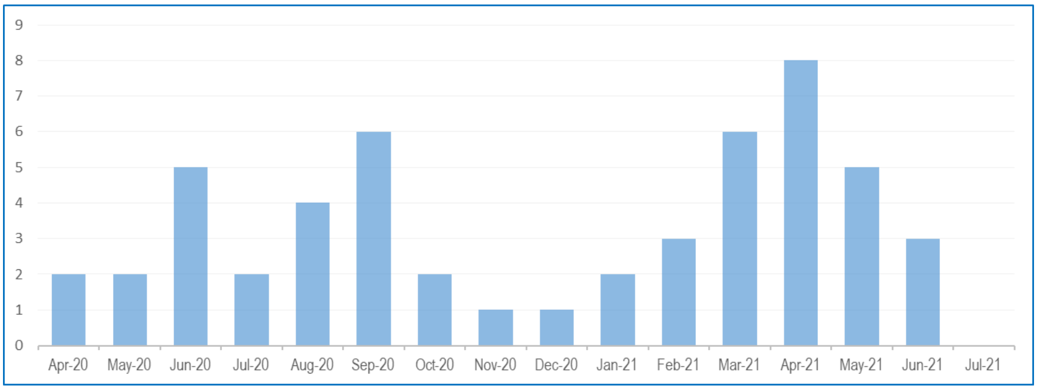


FIGURE 2. TIMELINE OF OBSERVED INCIDENTS RELATED TO PRIME ETL THREATS TOWARDS EDUCATION/ACADEMIA

Source: created by authors based on ENISA ETL Report (2021), p. 12

Having in mind the technological threats with impact on the perimeter of research, the authors performed an evaluation of the current AS-IS process, detailing some:

- characteristics necessary for information governance in their area of study, ideas expressed in Table 2;
- Business Intelligence (BI) platforms – data sources used in data/information scrutiny.

TABLE 2. CHARACTERISTICS OF INFORMATION GOVERNANCE IN RESEARCH PROCESS

Finance (cryptocurrencies)	Environment (brown bear)
- process is quite dynamic and in continuous evolution, new coins and businesses emerging and influencing data collection;	- information is available in various data sources, characterised by enlarged number;
- there are constant updates and communication from public authorities regarding the phenomenon impacting on the legislative and juridical status and indirectly on data collection and representation;	- there is a considerable effort in centralization of data;
- crypto is being used in various fields of economics and creates new socio-economic realities, contributing to the extension of the analysed perimeter;	- complexity is given by the fact that brown bear number is difficult to collect;
- data collected should be quantitative and qualitative;	- data collected should be quantitative and qualitative;
- centralised information can be used for other fields of research;	- centralised information can be used for other fields of research;
- centralised information should be trust worthy as it can be developed for decision making process, in public and private area;	- centralised information should be trust worthy as it can be developed for decision making process, in public and private area;
- there is needed an increased storage capacity option;	- data storage capacity does not require increased capacity;
- historical evolution of the phenomenon can be seen on dedicated BI platforms available online;	- should be kept a historical tracking of the centralised data for future scenario analysis;
- data analysis implies, increased system	- should be kept a registry on the changes of the

requirements options and usually is being done on dedicated BI platforms available online.	archive regarding the attributes of the data;
	- information once collected should be stored in a safe environment to prevent data loss;
	- information structure should be robust and flexible to allow quick queries and answers to incoming questions, given the notoriety of the subject at national level.

Source: created by authors based on the knowhow gathered in their research

Regarding the situation of cryptocurrencies are available several platforms where people can perform evaluation on the price quotations, historical evolution and link the development with different news present in private websites or communications from public authorities.

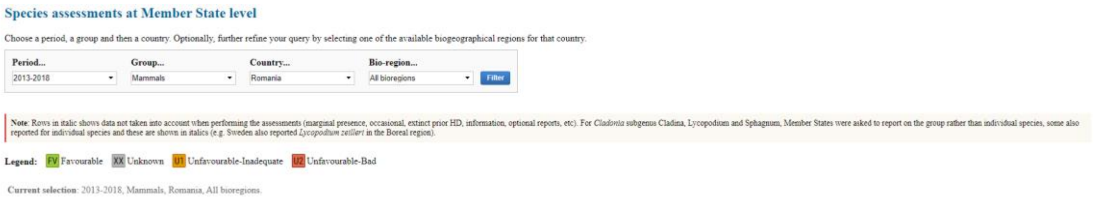
Analysis of the phenomenon is supported by the application of principles in data management, automated workflows, digital input and use of Business Intelligence dashboards.

What can be highlighted is the fact that the understanding of cryptocurrencies and their link to the international financial system is available to everyone, interested in examining the phenomenon.

It is advisable to perform a critical observation on the content displayed and a cross check assessment from multiple sources before deciding on the information to be used. In the same time the platforms are evaluated using various criteria by external parties, so users may have a good starting point for their analysis.

For the second area of research, the status of the brown bear (*Ursus arctos*) in Romania, the authors will extend some of the findings mentioned briefly in a previous article (Anuțoiu and Danțiș, 2021).

At the level of EU can be used the European Environment Information and Observation Network or EIONET (2022). Launched in 1994, it is a partnership network of European Environment Agency - EEA (2022). Researchers have the options to update their examination using various criteria having access to quantitative and qualitative data, indicators or other supportive material (Figure 3) regarding environment and wildlife.



Species assessments at Member State level

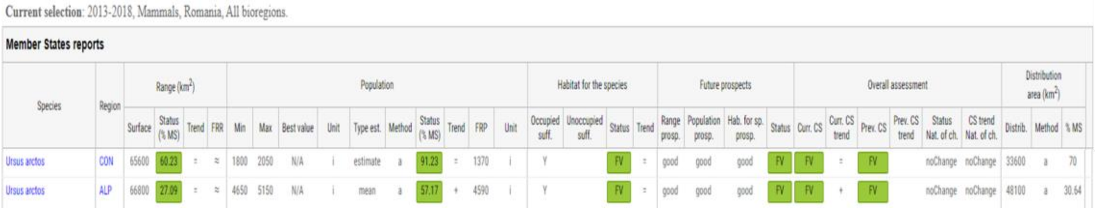
Choose a period, a group and then a country. Optionally, further refine your query by selecting one of the available biogeographical regions for that country.

Period...: 2013-2018
Group...: Mammals
Country...: Romania
Bio-region...: All bioregions

Note: Rows in italic shows data not taken into account when performing the assessments (marginal presence, occasional, extinct prior HD, information, optional reports, etc). For *Cladonia* subgenus Cladina, Lycopodium and Sphagnum, Member States were asked to report on the group rather than individual species, some also reported for individual species and these are shown in italics (e.g. Sweden also reported *Lycopodium zeilleri* in the Boreal region).

Legend: FV Favourable XX Unknown U1 Unfavourable-Inadequate U2 Unfavourable-Bad

Current selection: 2013-2018, Mammals, Romania, All bioregions.



Current selection: 2013-2018, Mammals, Romania, All bioregions.

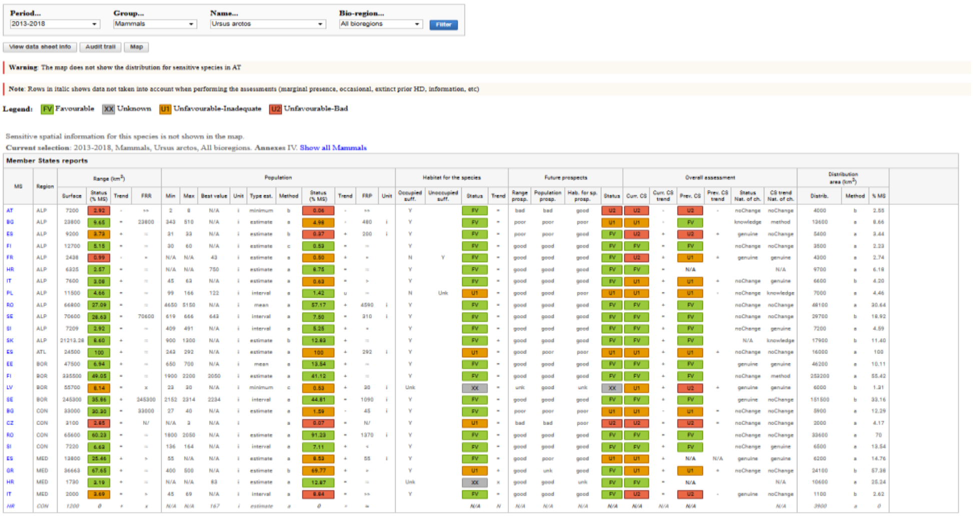
Member States reports

Species	Region	Range (km²)				Population										Habitat for the species				Future prospects				Overall assessment						Distribution area (km²)		
		Surface	Status (% MS)	Trend	FRR	Min	Max	Best value	Unit	Type est.	Method	Status (% MS)	Trend	FRP	Unit	Occupied suff.	Unoccupied suff.	Status	Trend	Range prosp.	Population prosp.	Hab. for sp. prosp.	Status	Curr. CS	Curr. CS trend	Prev. CS	Prev. CS trend	Status Nat. of ch.	CS trend Nat. of ch.	Distrib.	Method	% MS
Ursus arctos	CON	65600	60.23	=	≈	1800	2050	N/A	i	estimate	a	91.23	=	1370	i	Y		FV	=	good	good	good	FV	FV	=	FV		noChange	noChange	33600	a	70
Ursus arctos	ALP	66800	27.09	=	≈	4650	5150	N/A	i	mean	a	57.17	+	4590	i	Y		FV	=	good	good	good	FV	FV	+	FV		noChange	noChange	48100	a	30.64

FIGURE 3. REPRESENTATION ON EIONET PLATFORM REGARDING BROWN BEAR IN ROMANIA

Source: sample taken from EIONET PLATFORM

Information presented contains guidelines and insights to allow the user to familiarize with terms, which could be more technical. The content can be shaped based on the needs of each researcher and various perspectives can be displayed. Readers are being provided with titles of papers for various species, so the platform, can be seen as well as a codex. The tool itself can be used for a cross check with other data sources, which may indicate partial or complete number of brown bear individuals. This can be quite useful as a guideline for the development of analysis or future scenarios even on a greater area (Figure 4).



Period... 2013-2018
Group... Mammals
Name... Ursus arctos
Bio-region... All bioregions

Warning: The map does not show the distribution for sensitive species in AT

Note: Rows in italic shows data not taken into account when performing the assessments (marginal presence, occasional, extinct prior HD, information, etc)

Legend: FV Favourable XX Unknown U1 Unfavourable-Inadequate U2 Unfavourable-Bad

Sensitive spatial information for this species is not shown in the map.
Current selection: 2013-2018, Mammals, Ursus arctos, All bioregions. Annexes IV. Show all Mammals

Member States reports

MS	Region	Range (km²)				Population										Habitat for the species				Future prospects				Overall assessment						Distribution area (km²)		
		Surface	Status (% MS)	Trend	FRR	Min	Max	Best value	Unit	Type est.	Method	Status (% MS)	Trend	FRP	Unit	Occupied suff.	Unoccupied suff.	Status	Trend	Range prosp.	Population prosp.	Hab. for sp. prosp.	Status	Curr. CS	Curr. CS trend	Prev. CS	Prev. CS trend	Status Nat. of ch.	CS trend Nat. of ch.	Distrib.	Method	% MS
AT	ALP	7200	2.92	-	>>	2	8	N/A	i	minimum	b	0.06	-	>>		Y		FV	=	bad	bad	good	U2	U2	-	U2	-	noChange	noChange	4000	b	2.55
BG	ALP	23800	9.65	=	23800	343	510	N/A	i	estimate	a	4.98	-	480	i	Y		FV	=	poor	poor	poor	U1	U1	-	FV		knowledge	method	13600	a	8.66
ES	ALP	9200	3.73	+	≈	31	33	N/A	i	estimate	b	0.37	+	200	i	Y		FV	=	poor	poor	good	FV	U2	+	U2	+	genuine	noChange	5400	a	3.44
FI	ALP	12700	5.15	=	≈	30	60	N/A	i	estimate	c	0.53	=	≈		Y		FV	=	good	good	good	FV	FV	=	FV		noChange	noChange	3500	a	2.23
FR	ALP	2438	0.99	-	=	N/A	N/A	43	i	estimate	a	0.50	+	=		N	Y	FV	=	good	good	good	FV	U2	+	U1	+	genuine	genuine	4300	a	2.74
HR	ALP	6325	2.57	=	≈	N/A	N/A	750	i	estimate	a	8.75	=	≈		Y		FV	=	good	good	good	FV	FV	=	N/A			N/A	9700	a	6.18
IT	ALP	7600	3.08	+	≈	45	63	N/A	i	estimate	a	0.63	=	>		Y		FV	=	good	good	good	FV	U1	+	U1	+	noChange	genuine	6600	b	4.20
PL	ALP	11500	4.66	=	≈	99	166	122	i	interval	a	1.42	u	≈		N	Unk	U1	=	good	good	poor	U1	U1	=	U1	-	noChange	knowledge	7000	a	4.46
RO	ALP	66800	27.09	=	≈	4650	5150	N/A	i	mean	a	57.17	+	4590	i	Y		FV	=	good	good	good	FV	FV	+	FV		noChange	noChange	48100	a	30.64
SE	ALP	70600	28.63	=	70600	619	666	643	i	interval	a	7.50	=	310	i	Y		FV	=	good	good	good	FV	FV	=	FV		noChange	noChange	29700	b	18.92
SI	ALP	7209	2.92	=	≈	409	491	N/A	i	interval	a	5.25	+	=		Y		FV	=	good	good	good	FV	FV	+	FV		noChange	genuine	7200	a	4.59
SK	ALP	21213.28	8.60	+	≈	900	1300	N/A	i	estimate	b	12.83	+	≈		Y		FV	+	good	good	good	FV	FV	+	FV		N/A	knowledge	17900	b	11.40
ES	ATL	24500	100	+	≈	243	292	N/A	i	estimate	a	100	+	292	i	Y		U1	=	good	poor	poor	U1	U1	+	U1	+	noChange	noChange	16000	a	100
EE	BOR	47500	6.94	+	≈	650	700	N/A	i	mean	a	13.54	+	≈		Y		FV	=	good	good	good	FV	FV	+	FV		genuine	genuine	46200	a	10.11
FI	BOR	335500	49.05	=	≈	1900	2200	2050	i	estimate	a	41.12	+	≈		Y		FV	=	good	good	good	FV	FV	+	FV		noChange	method	253200	a	55.42
LV	BOR	55700	8.14	=	x	23	30	N/A	i	minimum	c	0.53	+	30	i	Unk		XX	=	unk	good	unk	XX	U1	+	U2	+	genuine	genuine	6000	b	1.31
SE	BOR	245300	35.86	+	245300	2152	2314	2234	i	interval	a	44.81	=	1090	i	Y		FV	=	good	good	good	FV	FV	+	FV		genuine	noChange	151500	b	33.16
BG	CON	33000	30.30	=	33000	27	40	N/A	i	estimate	a	1.59	-	45	i	Y		FV	=	poor	poor	poor	U1	U1	-	U1	=	noChange	noChange	5900	a	12.29
CZ	CON	3100	2.85	=	N/	N/A	3	N/A	i		a	0.07	=	N/		Y		U1	=	bad	bad	poor	U2	U2	=	U2	=	noChange	noChange	2000	a	4.17
RO	CON	65600	60.23	=	≈	1800	2050	N/A	i	estimate	a	91.23	=	1370	i	Y		FV	=	good	good	good	FV	FV	=	FV		noChange	noChange	33600	a	70
SI	CON	7220	6.62	=	≈	136	164	N/A	i	interval	a	7.11	+	<		Y		FV	=	good	good	good	FV	FV	+	FV		noChange	genuine	6500	a	13.54
ES	MED	13800	25.46	+	>	55	N/A	N/A	i	estimate	a	8.53	+	55	i	Y		FV	=	good	poor	good	U1	U1	+	N/A	N/A	genuine	genuine	6200	a	14.76
GR	MED	36663	67.65	+	≈	400	500	N/A	i	estimate	b	69.77	+	>		Y		U1	+	good	unk	good	FV	U1	+	U1	+	noChange	noChange	24100	b	57.38
HR	MED	1730	2.19	+	≈	N/A	N/A	83	i	estimate	a	12.87	=	≈		Unk		XX	x	good	good	unk	FV	FV	=	N/A			N/A	10600	a	25.24
IT	MED	2000	3.69	=	>	45	69	N/A	i	interval	a	8.84	=	>>		Y		FV	=	good	good	good	FV	U2	=	U2	-	genuine	noChange	1100	b	2.62
HR	*CON*	*1200*	*0*	*+*	*x*	*N/A*	*N/A*	*167*	*i*	*estimate*	*a*	*0*	*=*	*≈*				*N/A*	*N*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*			*N/A*	*3900*	*a*	*0*

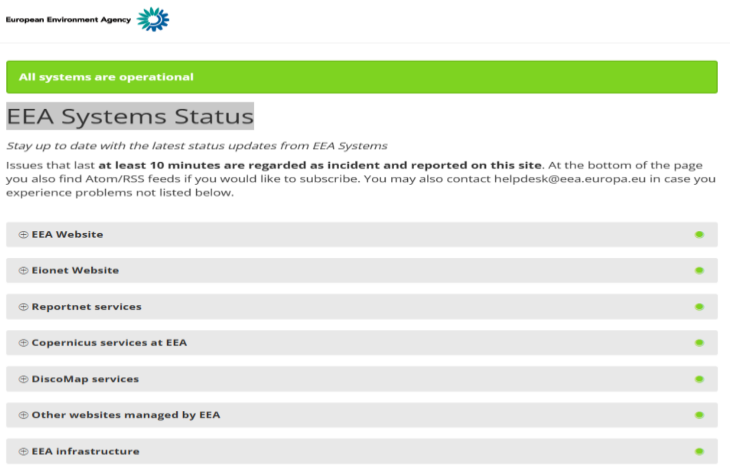
FIGURE 4. REPRESENTATION ON EIONET PLATFORM REGARDING BROWN BEAR IN EU

Source: sample taken from EIONET PLATFORM

The content identified in the above mentioned sources is analyzed and integrated by the researchers in other databases or in excel tables.

Reasoning on possible developments, if a technical issue appears in the functioning of the original data-source, having as root cause an ICT incident or an external threat, the collection and analysis of information can be interrupted, with results on the research process.

Referring to an ICT undesirable event the EEA is providing a dashboard where users have an overview on the status of the website and receive guidelines on the management of ICT incidents and the service position (EEA, 2022) as it is displayed in Figure 5. In addition visitors have a historical presentation of the incidents, which can be quite helpful for the general utilization of the platform.



European Environment Agency

All systems are operational

EEA Systems Status

Stay up to date with the latest status updates from EEA Systems

Issues that last **at least 10 minutes are regarded as incident and reported on this site**. At the bottom of the page you also find Atom/RSS feeds if you would like to subscribe. You may also contact helpdesk@eea.europa.eu in case you experience problems not listed below.

- ⊕ **EEA Website** ●
- ⊕ **Eionet Website** ●
- ⊕ **Reportnet services** ●
- ⊕ **Copernicus services at EEA** ●
- ⊕ **DiscoMap services** ●
- ⊕ **Other websites managed by EEA** ●
- ⊕ **EEA infrastructure** ●

FIGURE 5. DEPICTION OF EEA SYSTEM STATUS

Source: sample taken from EEA website

The possible impact of ICT disruption on the research process is taken into account even by the Romanian authorities in the national legislation. In this regard, will be mentioned a selection of the criteria/indicators applied to evaluate the impact on research as critical infrastructure:

- ICT criteria – systems linked to data calculation, analysis and storage; infrastructures, components or networks associated to communication services (Official Monitor, 2011);
- research criteria – percentage in which a Research & Development domain is impacted; percentage of Research & Development staff impacted by an event; Local and distributed computing capability – number of nodes, computing speed, computing power, number of projects, number of research institutes (Official Monitor, 2011).

As it can be noticed the research area represents a key component in the running of other systems and have been taken various actions to monitor its functional resilience. Based on the selected criteria, many of the indicators have an ICT footprint, providing the authors the idea to advance the blockchain as a possible solution for critical information management.

5.2. Blockchain Model. Brief Comparison With Traditional Database Characteristics

The indication for the testing or the use of blockchain technology in key areas or critical parts of society is not something completely new. Currently there are several initiatives on-going at European level to evaluate the suitability of this technology in different settings. Among them can be mentioned the European Blockchain Partnership, followed by European Blockchain Services Infrastructure or EBSI. The latter is an initiative of the public sector to create its own infrastructure, linking it afterwards with private sector (European Commission, 2022).

One of the use cases of the technology is linked to the education, as it is happening in Malta, where blockchain supports academic credentials verification (Allessie et al., 2019).

In Romania, the National Institute for Research & Development in Informatics - ICI Bucharest, is already part of the EBSI project and runs at national level one of the nodes of the infrastructure. The portfolio of ICI Bucharest in activities linked to the new technology includes Executive Blockchain Laboratory and European Center for Excellence in Blockchain (ICI, 2022).

Regarding blockchain or distributed ledger technology there are numerous studies available offering definitions on the technology and on its use. Turning point has been the paper of Satoshi Nakamoto and the launch of first unit of bitcoin (Nakamoto, 2008). This technology uses a typology of database diverse of classical one, being characterized by decentralization, saving information in data blocks linked and protected by cryptography.

The European Commission is defining blockchain as a "technology for promoting user trust. It makes it possible to share on-line information, agree on and record transactions in a verifiable, secure and permanent way" (European Commission, 2018).

ENISA (2016) is associating following characteristics and functioning model (Figure 6) to the technology:

- "all participants share a consistent copy of the database, there is no central server;
- network connections are peer-to-peer;
- participants must comply with ledger rules (permissionless or permissioned);
- using a type of consensus protocol, to agree on validity of a given transaction;
- transactions – could be financial and/or exchanging of assets and/or services;
- uses digital signatures (private/public key) to sign and/or encrypt transactions on the ledger;
- represents a temporal order of how assets evolve over time".

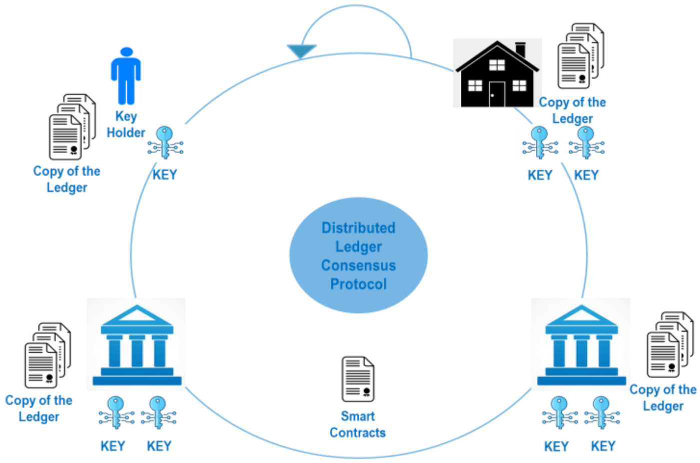


FIGURE 6. DISTRIBUTED LEDGER ECOSYSTEM

Source: created by authors based on ENISA Distributed Ledger Technology & Cybersecurity. Improving information security in the financial sector report (2016), p. 09

The European Commission is dedicating a particular interest to the blockchain, developing a strategy in this area and mentioning several attributes for this technology (European Commission, 2022).

In 2018 the Commissioner for Digital Economy and Society was indicating that blockchain will support the public services, the information systems will be reviewed and personal data will be better safeguarded (European Commission, 2018).

Among the attributes mentioned by the Commission the authors consider that the following ones may be useful for the use of blockchain in the governance of critical information (including research): data protection, cybersecurity, interoperability, environmental sustainability.

Performing a theoretical synthesis (not an exhaustive one) on the points of view expressed above by the specialists, the technical features to be linked to the blockchain technology may be the following:

- the decentralization and the lack of central authority;
- data protection and security through cryptography;
- data protection through the existence of different typologies of blockchain;
- can be seen the amendments done to the data;
- availability of data even if one node of the network is closed.

Contemporarily with the theoretic evaluation, below will be advanced the characteristics for the traditional databases. These ideas will be based on the experience gathered by the essayists in the implementation and utilization of Business Intelligence applications, founded on this technology:

- central storage of data;
- it is required a principal function for the management of data;

- protection requires implementation of different access profiles provided by a central authority;
- information once modified is displaying the last update;
- if the server is not available the services are not accessible.

Having these initial starting points in mind, a high level SWOT analysis (Table 3) can be performed to understand even more the adaptability level of each technology in the governance of critical information in general, research associated one, in particular.

TABLE 3. SWOT ANALYSIS

Strong Points	Weak Points
• traditional databases are used for a longer time in various environments; • are known and understood most of the behavioural characteristics of the classical technology; • there is an increased number of users familiarised with the implementation, usage and maintenance of traditional databases; • researchers have easier access to the applications based on traditional databases; • blockchain can function even if one of the network nodes is not available, sustaining the organizational resilience.	• blockchain is a relatively new technology and has a smaller perimeter of application; • if the server of the traditional database is not available, the services are not accessible; • if the central function governing the traditional database is not available, some requests may not be fulfilled.
Opportunities	**Threats**
• blockchain may be more safe as data is protected through cryptography; • blockchain is still in itself a research area; • blockchain has at European level strategic sponsorship in testing and implementation; • traditional databases have been subjects to numerous cyber-attacks and most of their vulnerabilities are known and can be revised; • needs of each research domain are different	• traditional databases have been subjects to numerous cyber-attacks and most of their vulnerabilities are known and can be exploited; • blockchain has to be tested even more to see how it behaves in governance of critical information and how it responds to cyber-attacks; • needs of each research domain are different

and influence the necessity for development.	and may impact on the standardization option (traditional database versus blockchain); • the human factor needs training in the use of the new technology, especially if it will be used on a large scale in public services.

Source: created by authors based on the knowhow gathered in their research

What can be noticed is that each database has different functioning principles and is characterized by different operative scenarios.

Blockchain may represent some advantages regarding data protection and data availability, still needs to prove its effectiveness on larger scale in use and cyber-attacks.

The different functioning principles of each database may adjust in a different manner to the scope and objectives of each research, as these direct the information governance process. What can be relevant for one area may have different outcomes for another one.

The level of variability present in the research area is impacting on the standardization decision, requiring the presence of alternatives for available technologies.

Equally, in practice, there may be organizations covering the function of critical infrastructure, where a central authority for the management/security of information is necessary. In this case a traditional database may adapt better to the requirements of that organization, compared to a blockchain.

CONCLUSIONS

The authors are aware on the limitations of the current content, as it does not cover all the cases linked to the management of the critical information used by the functions, seen as critical infrastructures.

As it emerges from the case study the necessities of the research are different in each field, impacting on the technical requirements of the technology to be used.

Considering the portfolio of critical infrastructures and the range of activities performed materializes a comprehensive image, marked by different necessities and market realities.

The decision to perform an assessment for the implementation and use of a classical database or blockchain solution should be evaluated at the level of each critical infrastructure.

Can be endorsed that each organization should assess the level of technical maturity, have a clear image of internal realities, future requirements and ways of development to understand which of the two scenarios is better for the management of critical information. In practical terms the testing on the use of blockchain can be experienced in a proof of concept, in a particular area of an organization and have a starting point for further enlargement of the perimeter.

What can be expressed even more is that blockchain based on the future developments and on the data stored, may fulfil itself the function of critical infrastructure, even one across various sectors. Based on the definitions provided at the beginning could be even seen as an European Critical Infrastructure and this may be linked to the strategic sponsorship existing at European level through various initiatives. In addition, this should be linked with the following considered factors:

- strategic objectives set by the organizations covering the role of critical infrastructure;
- level of complexity associated to the functioning scenarios of each critical infrastructure;
- successful implementation cases and experiences;
- prevention of data breaches or large scale cyber-attacks and organizational continuity;
- costs associated to the technology;
- joint projects between academia, public entities and private organizations;
- compliance with confidentiality, integrity and availability of data triad (Sosin, 2018).

In conclusion, can be highlighted that blockchain technology offers potential in development, still may be seen as an early platform compared to traditional databases. The decision to implement it has to be linked to the context of each organization after an internal assessment and understanding if such a solution can support the resolution of existing functional topics (Nascimento et al., 2019).

REFERENCES

Allessie, D., Sobolewski, M., Vaccari, L., Pignatelli, F. (Editor). (2019). Blockchain for digital government, EUR 29677 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-00581-0, doi:10.2760/942739, JRC115049, (pp 22 – 25)

Anutoiu, A.G., Dantis, D. (2021). Brown Bear Population Management in Romania: Pilot Project Using the Benefits of Technology. Proceedings of the 38th International Business Information Management Association (IBIMA), 23-24 November 2021, Seville, Spain, ISBN: 978-0-9998551-7-1, ISSN: 2767-9640

Dantis, D. (2021). Possible Directions of Evolution for Banking Activity in European Union under the Impact of Blockchain Technology. The Romanian Economic Journal. Year XXIV no. 80. June 2021, (pp 59 – 69)

EIONET (2022). Article 17 web tool on biogeographical assessments of conservation status of species and habitats under Article 17 of the Habitats Directive. Retrieved December 17, 2022 from https://nature-art17.eionet.europa.eu/article17

European Commission. Press Release (2022). Commission welcomes political agreement on new rules on cybersecurity of network and information systems. Retrieved November 10, 2022 from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2985

European Commission (2018). Shaping Europe's digital future. European countries join Blockchain Partnership. Retrieved November 15, 2022 from https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership

European Commission. Press Release (2022). Critical Infrastructure: Commission accelerates work to build up European resilience. Retrieved November 12, 2022 from: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238

European Commission. (2022). European Blockchain Services Infrastructure. Retrieved November 15, 2022 from https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure

European Commission. (2022). Shaping Europe's digital future. Blockchain Strategy. Retrieved November 16, 2022 from https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy

European Environment Agency. (2022). Retrieved December 17, 2022 from https://www.eea.europa.eu/

European Environment Agency. (2022). EEA Systems Status. Retrieved December 17, 2022 from https://status.eea.europa.eu/

European Union Agency for Cybersecurity. ENISA (2021). ENISA Thread Landscape 2021. (pp 29 – 30). Retrieved September 22, 2022 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Union Agency for Cybersecurity. ENISA (2021). ENISA Thread Landscape 2021. (pp 12 – 13). Retrieved September 22, 2022 from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

European Union Agency for Cybersecurity. ENISA (2016). Distributed Ledger Technology & Cybersecurity. Improving information security in the financial sector. Retrieved November 25, 2022 from https://www.enisa.europa.eu/publications/blockchain-security

European Union. Council Directive 2008/114/EC. Retrieved November 10, 2022 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=RO

European Parliament and the Council. Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Retrieved November 09, 2022 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1667416866889&from=EN

European Union. Data.Europa.Eu. Retrieved November 05, 2022 from https://data.europa.eu/

Manca, A.R., Benczur, P., Giovannini, E. (2017), Building a scientific narrative towards a more resilient EU society, Part 1: a conceptual framework, EUR 28548 EN, doi:10.2760/635528, (pp 4 – 5)

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System

Nascimento, S. (ed), Pólvora, A. (ed), Anderberg, A., Andonova, E., Bellia, M., Calès, L., Inamorato dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F., Spirito, L. (2019). Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies, EUR 29813 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-08977-3, doi:10.2760/901029, JRC117255, (pp 6)

National Centre for the Coordination of Protection of Critical Infrastructures. (2022). Retrieved November 15, 2022 from https://cncpic.mai.gov.ro/

National Institute for Research & Development in Informatics - ICI Bucharest. (2022). Services based on Blockchain technologies. Retrieved November 17, 2022 from https://ici.ro/en/blockchain-based-services/

Romanian Government. Data.Gov.Ro. Retrieved November 05, 2022 from https://data.gov.ro

Romanian Government. Decision 656/2021. Retrieved November 11, 2022 from https://legislatie.just.ro/Public/DetaliiDocument/243722

Romanian Government. Emergency Ordinance 98/2010. Retrieved November 10, 2022 from https://legislatie.just.ro/Public/DetaliiDocument/123547

Romanian Government. Emergency Ordinance 61/2019. Retrieved November 11, 2022 from https://legislatie.just.ro/Public/DetaliiDocumentAfis/217572

Official Monitor. (2011). Ministry of Research, Innovation and Digitalization Order 610/2011 and Ministry of Education Order 4380/2011 on the establishment of sectorial criteria and related critical thresholds for the identification of national critical infrastructures in the information and communication technology sector. MONITORUL OFICIAL 847/29th of November 2011

Official Monitor. (2011). Ministry of Education Order 4587/2011 on the establishment of sectorial criteria and related critical thresholds for the identification of national critical infrastructures in space and research domain. MONITORUL OFICIAL 530/27th of July 2011

Sosin, A. (2018). HOW TO INCREASE THE INFORMATION ASSURANCE IN THE INFORMATION AGE. Journal of Defence Resources Management 9:1(2018), (pp 45-57)

World Bank. Data.WorldBank.Org. Retrieved November 05, 2022 from https://data.worldbank.org/