Shifting towards Antifragile Critical Infrastructure Systems

Hind Bangui[a], Barbora Buhnova[b] and Bruno Rossi[c]
Faculty of Informatics, Masaryk University, Brno, Czech Republic

Keywords: Critical Infrastructure Systems, Antifragility, Resilience, Security.

Abstract: Antifragility, which is an evolutionary understanding of resilience, has become a predominant concept in academic and industrial fields as the criticality of vital infrastructures (like healthcare and transportation) has become more flexible and varying due the impact of digitization and adverse circumstances, such as changing the prioritization of industrial services while accelerating IoT (Internet of Things) deployment during the COVID-19 pandemic. The crucial role of antifragility is to enable critical infrastructures to gain from disorder to foster their adaptability to real unexpected environmental changes. Thus, this paper aims to provide a comprehensive survey on the antifragility concept while clarifying the difference with the resilience concept. Moreover, it highlights how the COVID-19 crisis has revealed the fragility of critical infrastructures and unintentionally promoted the antifragility concept. To showcase the main concepts, we adopt the blockchain as an example of an antifragile system.

1 INTRODUCTION

The modern society depends on Critical Infrastructures (CI). Safety, security, health, social well-being of everyone are bound to critical infrastructures for the provision of crucial services such healthcare and energy provision services. Societies have thus become increasingly vulnerable to disruptions in these infrastructures. Concretely, the criticality of infrastructures can be assessed in the event of a disturbance or disruption that can have dramatic consequences.

There are many definitions of CIs. For the European Union, *"critical infrastructure means 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"* (EU, 2008). In general, all the definitions of CIs place the emphasis on the importance of systems and assets that are part of CIs, so that any interference can have a debilitating impact on national security, public health or safety (Jarmon, 2019).

Despite different definitions of CIs that emerged in the literature (Engels, 2018), CIs have a common key concept, which is **"criticality"** that reflects the **"vitality and priority"** of service to enable and keep the functioning of modern society. Moreover, criticality of infrastructures is flexible and varying over-time to enable a society to develop. Meanwhile, criticality reflects the acceptance of a society to deal with consequences of service flaws, weaknesses, and disruptions. Thus, criticality is simultaneously synonymous of vitality and risk in the literature (Engels, 2018).

Actually, disasters and crises are the major CI concerns as they are disruptive to their interdependent structures and functions. CIs adopt the resilience concept to deal with disruptive events while keeping their desired original state. Indeed, resilience enhances the ability of a system to confront with disruptions by using mainly and successively the following capacities:

- Absorption: It is the ability to reduce or prevent the severity of a crisis,
- Recoverability: It is the ability to rebound to its original state,
- Ex Post Adaptability: It is the ability to bounce forward to a new state based on planning for the expected and unexpected situations.

However, the COVID-19 pandemic has challenged the effectiveness of these resilience capacities by accelerating uncertain circumstances and preventing CIs from using the possible and preventive resilient measures to rebound and continue as normal, such

[a] https://orcid.org/0000-0003-2689-0382
[b] https://orcid.org/0000-0003-4205-101X
[c] https://orcid.org/0000-0002-8659-1520

Bangui, H., Buhnova, B. and Rossi, B.
Shifting towards Antifragile Critical Infrastructure Systems.
DOI: 10.5220/0011086400003194
In *Proceedings of the 7th International Conference on Internet of Things, Big Data and Security (IoTBDS 2022)*, pages 78-87
ISBN: 978-989-758-564-7; ISSN: 2184-4976

as forcing employees to self-isolate and work from their homes due to the closure of industries. Consequently, this health crisis has obliged CIs to learn and adapt to real unanticipated situations. Furthermore, it has forced infrastructures to change increasingly the vitality and priority of their services and functions, such as shifting from in-person to distance learning in the education sector. Actually, these sudden changes experienced during COVID-19 reflect unintentionally the antifragility concept that was introduced by Taleb to ***"adapt and change continuously by learning from the environment and being, sort of, continuously under pressure to be fit"*** *(Taleb, 2012).*

Therefore, the goal of this paper is to spark a debate about the antifragility concept by shedding light on how CIs can benefit from disorder to evolve overtime while enhancing their adaptability to real unexpected situations. We use COVID-19 as an example of crises that shows up how survived CIs (like healthcare) have gained from disorder unintentionally to acquire new knowledge and strengthen their adaptability to real unforeseen circumstances. Moreover, we cite blockchain as an example of antifragile systems (Sahdev et al., 2021; Nicholas Taleb, 2021) that has attracted attention in CIs (Kendzierskyj and Jahankhani, 2019) due to its ability to become antifragile with every disorder it has suffered, which is proven with cryptocurrencies, particularly Bitcoin (Ammous, 2018; Nicholas Taleb, 2021).

This paper is structured as follows. Section 2 aims to introduce the antifragility concept. Section 3 highlights how the COVID-19 crisis has revealed the fragility of CIs and unintentionally promoted the antifragility concept. Section 4 illustrates the blockchain as an example of antifragile systems. Section 5 concludes the survey.

2 WHAT IS ANTIFRAGILITY?

In 2012, Nassim Taleb introduced antifragile concept in his book "Antifragile: things that gain from disorder". He represented this concept as: *"Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors and love adventure, risk, and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile.* ***Let us call it antifragile****"*(Taleb, 2012). From that time, antifragility has been shown considerable interest in academic and industrial fields. Within the context of digital CIs, the main idea of antifragility is to enable a system to gain from volatility and disorder and learn how to improve its behaviour when subjected to implausible changes in parameters (Gheorghe et al., 2018; Taleb, 2012).

Actually, antifragility is an evolutionary understanding of the resilience that not simply enables a system to tolerate adverse events, but rather allows to strengthen in the process its self-learning ability to respond to future possible threatening situations, which was clarified in Taleb's book (Taleb, 2012) as follows: *"Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better"*. Thus, antifragility is a property of *"systems able to learn while enacting elastic and resilient strategies"* (De Florio, 2014). In other words, as it is impossible to predict all future circumstances with a large negative impact in the digital era, antifragility looks at enabling an autonomous system to self-learn from shocks, resulting in creating a complex adaptive-autonomous system that is antifragile to negative incidents. Thus, Antifragility has been considered as an important step in safety evolution (Martinetti et al., 2019), exemplifying the digital era. Table 1 and Figure 1 provide more clarification concerning the antifragility concept.

Table 1: Other Antifragility Definitions.

Papers	Definitions
(Taleb, 2012)	"It not only survive disturbance and disorder but actually develop under pressure"
(Karadimas et al., 2014)	"Being antifragile means being able to grow despite the crises that might arise"
(Taleb, 2012)	"The robust or resilient is neither harmed nor helped by volatility and disorder, while the antifragile benefits from them."
(Taleb, 2012)	"The antifragile loves randomness and uncertainty, which also means—crucially—a love of errors, a certain class of errors. Antifragility has a singular property of allowing us to deal with the unknown, to do things without understanding them—and do them well".

3 WHY DO WE NEED ANTIFRAGILE SYSTEMS?

Given the stark reality that dynamic CIs would face increasingly multiple changes as well as multiple risks, in this section, we discuss the need for considering the antifragility concept in CIs. To do this, we use the COVID-19 crisis as a realistic scenario that reflects the need of gaining from disorders to adapt to

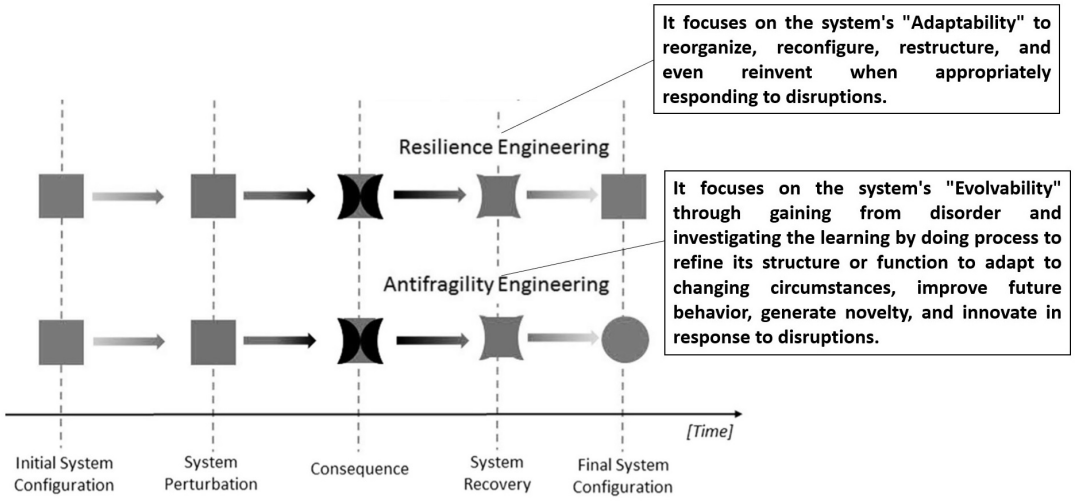

Figure 1: Antifragility vs Resilience (Adapted from (Martinetti et al., 2019)).

Table 2: Health Organizations that Reported Cyberattacks/Data Breaches during the COVID-19 Outbreak.

Health Institutions	Date of Reported Issues	Attacks Detected/ Data Breach
Brno University Hospital[1]	March 13, 2020	Unspecified attack
UK Healthcare Workers[2]	April 4, 2020	Ransomware attack
Spanish Healthcare Workers[3]	April 4, 2020	Ransomware attack
Paris Hospital Authority[4]	March 22, 2020	Unspecified attack
Hammersmith Medicines Research Group[5]	March 14, 2020	Ransomware attack
Babylon Health[6]	June 10, 2020	Data Breach due to software vulnerability
United States Health and Human Services Department[7]	March 16, 2020	Unspecified attack

1 https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/
2 https://www.digitalhealth.net/2020/04/neither-covid-19-nor-cyber-criminals-care-who-gets-infected-and-suffers/
3 https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware
4 https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says
5 https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus
6 https://www.mobihealthnews.com/news/emea/babylon-health-admits-gp-hand-app-data-breach-caused-software-issue
7 https://techmonitor.ai/security/us-health-human-services-department-cyber-attack

the dynamic change of infrastructures criticality.

3.1 Fragility of Critical Infrastructures

While it seems that resilience is able to recover and restore any impaired CI system due to perturbations (like cybersecurity incidents), the rapidly spreading COVID-19 pandemic has shown the deficiency of resilience to mitigate its adverse effects, which makes CI systems more fragile to downtime caused by this unexpected crisis. Indeed, resilience focuses mainly on rebounding a system to its previous state and then reorganizing it afterwards to prevent unexpected events, which could not serve shocked CI systems during COVID-19 that are looking for acquiring new knowledge to learn how to adapt their components and become antifragile against downtime.

Healthcare is an example of critical infrastructures that could not rebound to their previous original state after being exposed to uncertain and unstable conditions caused by COVID-19, which pushes to envisage new potential strategies for tackling the challenges arising in several ways. For example, many health organizations have reported cyberattacks and data breaches during COVID-19 crisis (Table 2). Likewise, hospitals were overcrowded and disabled to meet the demands on COVID-19 patients due to non-specialized doctors, poor technical skills, and limited human resources to deal with the COVID-19 epidemic. Therefrom, healthcare systems have perceived the potential of Internet of Medical Things (IoMT) to handle and control digitally critical medical cases during the ongoing pandemic. Thus, IoMT is having a huge impact on helping healthcare systems to improve their reliability and the quality of life of COVID-19 patients. Moreover, the collected information-based IoMT services undertake to guide medical professionals in envisaging new healthcare

opportunities and fighting against this pandemic, such as forecasting in advance medical resource requirements and conducting forensics readiness to learn how to avoid cyberattacks and implement security mechanisms adequately.

Meanwhile, other critical infrastructures followed the same path of healthcare to tackle COVID-19 crisis due to their inability to act proactively and reactively in response to pre and during disruptive changes caused by this pandemic. Yet, this leads to radical changes to the way CIs cope with adversarial perturbations that threaten their reliability, security and stability. For example, work from home (or remote working), online services, and acceleration of using automation and autonomous operations are adopted to deal with the enterprises and industrial closure, which restructures toward a future digital workplace environment.

We can notice that the global transformation caused by COVID-19 crisis across different CIs represents a starting point of an evolutionary resilience, which is antifragility. Indeed, CIs have realised the importance of considering learning as part of their process to adapt to real unexpected events (like closure of retail shopping or educational institutions). Moreover, CIs get benefits from disturbances and then they become able to improve their performance and reliability.

Therefore, antifragility has shown explicitly and implicitly its ability to cope with the pandemic as it *"has a singular property of allowing us to deal with the unknown, to do things without understanding them—and do them well"* (Taleb, 2012). Thus, antifragility can support digital technologies-oriented CI systems that operate in adversarial environments as they could proactively learn how to adapt their function and advance their cyber defense approaches, such as IoT (Internet of Things) and AI (Artificial Intelligence) technologies.

3.2 The Need for Adapting IoT to Real CI Requirements

After the outbreak of COVID-19, academic and industrial researchers across various domains are coming together to put forward IoT solutions to support CIs in coping with the fallbacks. IoT has been leveraged in different vital infrastructures to entirely rely on digital and mitigate this pandemic, such as smart workplace technologies, smart lockdowns, and smart classroom teaching.

Despite the considerable IoT advancements, its applications are still lacking reliability and are susceptible to overwhelming traffic, failures, and cyberattacks (Chamola et al., 2020). Indeed, during the outbreak, the main goal of software engineering is to build and maintain high-quality IoT systems that focus mainly on mitigating this pandemic. The best practice is to exploit reference IoT architectures to develop new versions of IoT systems or adapting the current versions to deal with this epidemic. However, the time necessary for identifying the best set of test cases is very short, which does not help developers to deliver high-quality IoT applications and services. Besides, the lack of simulators of epidemic risk management and the absence of realistic datasets to test and validate the research outcomes decrease further the robustness of IoT services (Chamola et al., 2020).

Yet, the adoption of antifragility concept in IoT technologies could enable learning from the bad experiences (e.g., technical mistakes and failures), which can lead to acquire new knowledge to defence the increasing threats against IoT services. Likewise, it allows to get more expertise in modeling and testing and then adapt IoT services to real CI requirements, resulting in fostering IoT deployment in CIs.

3.3 The Need of Data Analysis in CIs

AI (Artificial Intelligence) applications will play a crucial role in analyzing the high volume and complexity of big data in CIs (Sakhnini et al., 2020). In fact, AI applications will extract actionable information required for supporting CI operations. This extraction is usually done at centralized platforms. However, the impact of moving from centralized to decentralized edge computing platforms will be progressively accelerating the requirements of using AI in distributed environments, namely federated learning (Liu et al., 2020). As a result, AI applications benefit from data streaming to satisfy the real-time needs of CIs, such as decision-making. Moreover, AI applications investigate the massive volume, variety, and the velocity of data streaming to enhance the protection of a system and avoid such scenarios causing huge cascading effects on its other dependent infrastructures.

Nevertheless, the deployment of efficient AI applications in CIs may also bring various data security, privacy, and trust concerns due to the threat of active adversarial attacks (Ibitoye et al., 2019) that seek to exploit the vulnerability of learning models and then confuse them into making wrong decisions. Yet, it is necessary to consider risk analysis to mitigate existing risks and find ways to prevent inducing wrong prediction outcomes from learning models (Ibitoye et al., 2019).

Antifragility could tackle these challenges as high

"risk" related to positive improvements and high performance for an antifragile system (Aven, 2015) that should be exposed to uncertainties to gain from them, resulting in improving future performance while reducing negative risks. Thus, the implication of antifragility for AI could be used as a defense mechanism against adversarial attacks.

4 ANTIFRAGILITY EXAMPLE

In this section, we select blockchain technology as a typical example of antifragile systems (Johnson and Gheorghe, 2013) that would tackle the scalability of CI services towards improving data storage, data security, and data trust (Kendzierskyj and Jahankhani, 2019).

The antifragility of blockchain has been discussed in several studies (Ammous, 2018; Nicholas Taleb, 2021; Pérez-Marco and Journée, 2016; Nicholas Taleb, 2021). Moreover, the blockchain characteristics reflect clearly the antifragile properties (Johnson and Gheorghe, 2013), such as redundancy, efficiency versus risk, absorption of serious threats, and non-monotonicity (e.g., Bitcoin platforms (Ammous, 2018) learn from mistakes to evolve). However, blockchain is also partially fragile as all cyber security attacks could not be detected 100% nor prevented (Boireau, 2018).

Therefore, in this section we survey briefly the application of blockchain in CIs. Notably, we point out substantially its application for supporting some CI properties. Beside, from the antifragility perspective, we highlight some blockchain limitations that could be used to acquire the knowledge necessary to build antifragile CIs.

4.1 Blockchain for CIs

As critical infrastructure systems are getting more and more dependent on sensitive information, a number of critical infrastructure properties are grappling with moving forward in sustainable infrastructure development while ensuring the availability of information in a consistent way. Therefrom, blockchain (Pérez-Marco and Journée, 2016; Nicholas Taleb, 2021) has been adopted in different CI domains due to its ability to ensure sustainable development of many applications by managing and securing sharing information. Particularly, blockchain has received much interest in the most significant CI properties, which are: reliability, resilience, and forensic readiness. These CI properties are highlighted in (Klein, 2020; Alcaraz and Zeadally, 2015) as the main key requirements to achieve a sustainable critical infrastructure through digitalization in face of unpredictable disruptions. Blockchain plays the role of being liable in the context of these properties and the functionality of CIs to prevent the manipulation of data and ensure the availability of CI services. For a summary of blockchain applications linked to these CI properties see Tables 3, 4, and 5.

4.1.1 Blockchain for Resilience

Resilience is an aspect that can face this crucial challenge by resisting to disturbances safeguarding critical infrastructures while recovering and returning to an acceptable state. There are many definitions of resilience, for example, it is defined in (Henry and Ramirez-Marquez, 2012) as: *"the ability of a system to bounce back from a failure"*. Likewise, in (Kahan et al., 2009), resilience is defined generally as: *"the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner through the preservation and restoration of its essential basic structures and functions"*. While in supply chain domain (Swafford et al., 2006) resilience is defined as: *"the ability of a supply chain to fulfill end customer demand to the desired level within an acceptable period of time after any pre or post-disruption mitigation efforts"*.

In (Thompson et al., 2016), the differences between security and resilience have been clarified and have made a point to state that *resilience is maintained if and only if a security breach is detected, contained and resolved*. Thereby, resilience has adopted blockchain to reach its full potential across different domains (Table 4) by strengthening a system in resisting detrimental effects and safeguarding its dependent systems.

4.1.2 Blockchain for Reliability

Using reliable infrastructure services is crucial to assure the continuity of our daily activities. *A conventional definition of software reliability is the probability that software will not fail in a specified period of time in a given operational environment* (Miller et al., 1992). In other words, reliability is a concept that models the probabilistic behavior of a system to investigate its correct function during exposure to common failures within a specified period. It is usually confused with resilience that is mainly related to the consequences of disturbances without considering the probability of their occurrence (Mahzarnia et al., 2020; Panteli and Mancarella, 2015). It is worth noting that the reliability of a system can be evaluated

Table 3: Examples of Blockchain Application Domains for Reliability.

Paper	Description
Agriculture Domain	
(Pincheira et al., 2021)	Cost-effective IoT devices as trustworthy data sources for a blockchain-based water management system in precision agriculture
(Song and Li, 2021)	Blockchain-enabled relay-aided wireless networks for sustainable e-agriculture
(Alkahtani et al., 2021)	E-Agricultural Supply Chain Management Coupled with Blockchain Effect and Cooperative Strategies
(Rocha et al., 2021)	Blockchain Applications in Agribusiness
Healthcare Domain	
(Aggarwal et al., 2021)	Blockchain-Based UAV Path Planning for Healthcare 4.0
(Nguyen et al., 2021)	A Cooperative Architecture of Data Offloading and Sharing for Blockchain-based Healthcare Systems
(Musamih et al., 2021)	A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain
Transportation Domain	
(Zhang et al., 2020)	BSFP: Blockchain-Enabled Smart Parking with Fairness, Reliability and Privacy Protection
(Jian et al., 2021)	Blockchain-Empowered Trusted Networking for Unmanned Aerial Vehicles in the B5G Era
(Alsamhi et al., 2021)	Blockchain for Decentralized Multi-Drone to Combat COVID-19
Energy Domain	
(Guan et al., 2021)	Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid
(Wang et al., 2021)	Blockchain-based IoT device identification and management in 5G smart grid
(Patil et al., 2021)	Study of blockchain based smart grid for energy optimization
(Ahmad et al., 2021)	Blockchain based Secure Energy Trading Mechanism for Smart Grid

Table 4: Examples of Blockchain Application Domains for Resilience.

Paper	Description
Agriculture Domain	
(Vannucci et al., 2021)	Climate change management: a resilience strategy for flood risk using Blockchain tools
(Gils and Frison, 2020)	Blockchain Technology for Food Security? Resilience Potential and Risk Identification for the Multilateral System of the International Treaty on Plant Genetic Resources for Food and Agriculture
Energy Domain	
(Mylrea and Gourisetti, 2017)	Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security
(Nallapaneni and Chopra, 2020a)	Blockchain-based Online Information Sharing Platform for Improving the Resilience of Industrial Symbiosis-based Multi Energy Systems
(Nallapaneni and Chopra, 2020b)	Enhancing the Resilience of Urban Networked Community Microgrids: Blockchain-enabled Flexible Energy Trading Strategy
(Jetley, 2019)	Blockchain implementation for smart grid resilience
(Vishwakarma and Singh,)	Smart Grid Resilience and Security Using Blockchain Technology
Transportation Domain	
(Gupta et al., 2020)	Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review
Healthcare Domain	
(Frison et al., 2020)	Blockchain Technology for IP Management & Governance: Exploring its Potential to Restore Trust and Resilience in the Plant and Biomedical Sectors

without identifying the threats, while the concept of resilience is tied to cope with one or more specific threats.

Table 3 illustrates blockchain-based reliability frameworks across domains, where blockchain has been used in effective ways to improve the reliability of several applications, such as the unmanned aerial vehicle (UAV) that has become a big research topic due to its various applications in various domains, such as UAVs (or drones) for medical applications (Egala et al., 2021), multi-drone to combat COVID-19 (Alsamhi et al., 2021), and UAV-assisted connected vehicle networks (Álvares et al., 2021).

Table 5: Examples of Blockchain Application Domains for Forensics Readiness.

Paper	Description
Energy Domain	
(Kotsiuba et al., 2018)	Blockchain evolution: from bitcoin to forensic in smart grids
(Mbarek et al., 2020)	Blockchain used for energy readings data tampering detection
(Sanseverino et al., 2017)	Blockchain used for data tampering detection during energy transactions
Healthcare Domain	
(Malamas et al., 2019)	A forensics-by-design management framework for medical devices based on blockchain
(Nuzzolese, 2020)	Electronic health record and blockchain architecture: forensic chain hypothesis for human identification
(Lusetti et al., 2020)	A blockchain based solution for the custody of digital files in forensic medicine
Transportation Domain	
(Billard and Bartolomei, 2019)	Digital forensics and privacy-by-design: Example in a blockchain-based dynamic navigation system
(Obimbo, 2020)	Towards Vehicular Digital Forensics from Decentralized Trust: An Accountable, Privacy-preservation, and Secure Realization
(Hossain et al., 2017)	Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV)
(Cebe et al., 2018)	Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles

4.1.3 Blockchain for Forensics Readiness

Forensics readiness aims mainly to conduct a comprehensive analysis to identify the root causes and involved individuals after disturbances have occurred (Daubner et al., 2020), resulting in digital evidence admissible at court. It is defined as: *"The extent to which computer systems or computer networks record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations"* (Mohay, 2005).

The storage and processing of data with secu-

Table 6: Examles of Blockchain Security Threats (Cheng et al., 2021; Bhushan et al., 2021; Saminathan et al., 2021).

Category of Security Threats	**General Description**	**Attack Vectors**
Spending Threats	It takes place where a consumer uses a single cryptocurrency for processing multiple transactions.	Race Attack, 51% Attack, Finney Attack, Vector 76 Attack, Alternative History Attack
Network Threats	Considering the peer-to-peer nature of the blockchain network that needs to use protocols to provide network services, attackers exploit this network requirement to trick victims, for example, making them believe that a transaction has failed and then asking for the transaction to be repeated.	Transaction Malleability Attack, Sybil Attack, Eclipse Attack, DDoS Attack, Timejacking Attack, Partition Routing Attack, Delay Routing, Refund Attack, Balance Attack Punitive and Feather forking Attack
Mining-Pool Threats	Mining pools are created by a group of miners to work collaboratively. Next, it pools their resources for contributing to the generation of a block, and then sharing the block reward according to the added processing power. the pool vulnerabilities are exploited by attack vectors to launch both internal and external attacks on a mining pool.	Selfish Mining/Block-discard Attack, Block Withholding Attack, Fork-After Withholding Attack, Bribery Attack, Pool Hopping Attack
Wallet Security Threats	A wallet is a type of paid account that stores users' financial information, using public and private keys to make transactions in the blockchain. Attackers exploit the weakness in wallets that lead to exposure of private keys. As a result, they can steal money and transfer the stolen funds to different addresses and hide the fund traceability after stealing money.	Vulnerable Signature, Flawed Key Generation, Lack of Address Control Creation, Collison and Pre-Image Attack, Bugs and Malware
Smart Contract Threats	A smart contract is executed automatically when certain conditions are met. Once it is added to the blockchain, it cannot be altered due to the immutable property of blockchain. Attackers exploit smart contract codes' weaknesses to control all the user's incoming and outgoing transactions.	Vulnerabilities in Contract Codes, Vulnerabilities in EVM Bytecode, Vulnerabilities in Blockchain, Eclipse Attack on Smart Contract, Low-level attacks

rity is needed in forensic applications across different domains (Table 5) to produce an efficient investigation. Blockchain facilitates forensic readiness by being incorporated into critical systems to ensure the availability and integrity of data used for determining stress sources. Thus, using blockchain for digital forensics can serve as a starting secured and trusted point for understanding and identifying the critical needs to anticipate future stresses and protect different dependent and interdependent critical infrastructures through realistic examples and scenarios.

4.2 Blockchain Vulnerabilities

Despite the positive influence of blockchain in different domains, blockchain implementations are also vulnerable (Wang et al., 2019; Boireau, 2018; Cheng et al., 2021; Bhushan et al., 2021; Saminathan et al., 2021). Many studies have focused on identifying vulnerabilities that could threaten the data integrity in blockchain-based systems (Wang et al., 2019; Bhushan et al., 2020; Shrivas et al., 2020; Samanta et al., 2021). In fact, the blockchain is like any software application, not invulnerable. Table 6 shows specific vulnerabilities that can be used by potential attackers, such as mining-pool threats that exploit miners to launch attacks (e.g., Pool Hopping (Singh et al., 2019)). Likewise, in wallet security threats (Table 6), encrypted data on blockchain is not guaranteed since it may deteriorate over time due to the lost or compromised key, which means permanent loss of control over a blockchain (Mosakheil, 2018).

4.3 Gaining from Blockchain Vulnerabilities

Owning to the fact that vulnerabilities would have significant negative effects on CIs, there is a big need for understanding how blockchain could deal with the dependency and inter-dependency in CIs as it is unreasonable to assume that blockchain is capable of adapting and tolerating attacks (Table 6). Consequently, the dependency analysis (Alcaraz and Zeadally, 2015) would be very crucial to deal with cascading and common-cause failures/attacks by identifying and classifying potentially risk dependencies. Also, this analysis should include methods for measuring fragility to find proactively alternative mitigation measures that can proceed with automated actions to decrease/prevent the spread of negative events in CIs. Thus, it is necessary to conduct a deep analysis

to trace the dependency between blockchain and CIs while learning how to gain from blockchain threats (Table 6), leading to defense CI mechanism evolution.

To sump up, the blockchain could be the perfect real-world testbed to understand better how we can shift effectively from resilience to antifragility, which entails further future research to reach the maturity level of blockchain that would promote truthfulness and trustworthiness of digital-antifragile CIs.

5 CONCLUSIONS

The major lesson learned from this study is that the COVID-19 pandemic has pushed CIs to acknowledge their vulnerability and fragility, which are often overlooked. This crisis has become a challenge that CIs (like healthcare) have managed to use as an opportunity for change, which unintentionally leads to adopting an evolutionary understanding of resilience (antifragility) to learn how to curb the tragic effects of this crisis and foster their digital transformation. Likewise, the real impact of this health crisis has exposed the CI properties in a new way, mainly criticality that is fully changed due to the mutable CI resource prioritization (like using car parks as hospitals).

Finally, this study is a thorough review of antifragility literature that necessitates a detailed research investigation to understand better how to gain from disorder and advance the body of knowledge on constructing antifragile CIs, which has already been started with the COVID-19 pandemic and will continue in the following decades.

ACKNOWLEDGEMENTS

The work was supported from ERDF/ESF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

REFERENCES

Aggarwal, S., Kumar, N., Alhussein, M., and Muhammad, G. (2021). Blockchain-based uav path planning for healthcare 4.0: Current challenges and the way ahead. *IEEE Network*, 35(1):20–29.

Ahmad, R. F., Siddique, M., Riaz, K., Hussain, M. M., and Bhatti, M. (2021). Blockchain based secure energy trading mechanism for smart grid. *Pakistan Journal of Engineering and Technology*, 4(2):100–107.

Alcaraz, C. and Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, 8:53–66.

Alkahtani, M., Khalid, Q. S., Jalees, M., Omair, M., Hussain, G., and Pruncu, C. I. (2021). E-agricultural supply chain management coupled with blockchain effect and cooperative strategies. *Sustainability*, 13(2):816.

Alsamhi, S., Lee, B., Guizani, M., Kumar, N., Qiao, Y., and Liu, X. (2021). Blockchain for decentralized multi-drone to combat covid-19. *arXiv preprint arXiv:2102.00969*.

Álvares, P., Silva, L., and Magaia, N. (2021). Blockchain-based solutions for uav-assisted connected vehicle networks in smart cities: A review, open issues, and future perspectives. In *Telecom*, volume 2, pages 108–140. Multidisciplinary Digital Publishing Institute.

Ammous, S. (2018). *The bitcoin standard: the decentralized alternative to central banking*. John Wiley & Sons.

Aven, T. (2015). The concept of antifragility and its implications for the practice of risk analysis. *Risk analysis*, 35(3):476–483.

Bhushan, B., Sinha, P., Sagayam, K. M., and Andrew, J. (2020). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, page 106897.

Bhushan, B., Sinha, P., Sagayam, K. M., and Andrew, J. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering*, 90:106897.

Billard, D. and Bartolomei, B. (2019). Digital forensics and privacy-by-design: Example in a blockchain-based dynamic navigation system. In *Annual Privacy Forum*, pages 151–160. Springer.

Boireau, O. (2018). Securing the blockchain against hackers. *Network Security*, 2018(1):8–11.

Cebe, M., Erdin, E., Akkaya, K., Aksu, H., and Uluagac, S. (2018). Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Communications Magazine*, 56(10):50–57.

Chamola, V., Hassija, V., Gupta, V., and Guizani, M. (2020). A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact. *Ieee access*, 8:90225–90265.

Cheng, J., Xie, L., Tang, X., Xiong, N., and Liu, B. (2021). A survey of security threats and defense on blockchain. *Multimedia Tools and Applications*, 80(20):30623–30652.

Daubner, L., Macak, M., Buhnova, B., and Pitner, T. (2020). Verification of forensic readiness in software development: a roadmap. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pages 1658–1661.

De Florio, V. (2014). Antifragility= elasticity+ resilience+

machine learning models and algorithms for open system fidelity. *Procedia Computer Science*, 32:834–841.

Egala, B. S., Pradhan, A. K., Badarla, V. R., and Mohanty, S. P. (2021). Fortified-chain: A blockchain based framework for security and privacy assured internet of medical things with effective access control. *IEEE Internet of Things Journal*.

Engels, J. I. (2018). *Key Concepts for Critical Infrastructure Research*. Springer.

EU (2008). Council directive 2008/114/ec on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection. *L345*, 3:0075–0082.

Frison, C., van Zimmeren, E., and Gils, T. (2020). Blockchain technology for ip management & governance: Exploring its potential to restore trust and resilience in the plant and biomedical sectors. *Current Opinion in Environmental Sustainability*.

Gheorghe, A. V., Vamanu, D. V., Katina, P. F., and Pulfer, R. (2018). Critical infrastructures, key resources, and key assets. In *Critical Infrastructures, Key Resources, Key Assets*, pages 3–37. Springer.

Gils, T. and Frison, C. (2020). Blockchain technology for food security? resilience potential and risk identification for the multilateral system of the international treaty on plant genetic resources for food and agriculture. *Resilience Potential and Risk Identification for the Multilateral System of the International Treaty on Plant Genetic Resources for Food and Agriculture (September 1, 2020). IUCN AEL Proceedings*.

Guan, Z., Lu, X., Yang, W., Wu, L., Wang, N., and Zhang, Z. (2021). Achieving efficient and privacy-preserving energy trading based on blockchain and abe in smart grid. *Journal of Parallel and Distributed Computing*, 147:34–45.

Gupta, R., Tanwar, S., Kumar, N., and Tyagi, S. (2020). Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Computers & Electrical Engineering*, 86:106717.

Henry, D. and Ramirez-Marquez, J. E. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety*, 99:114–122.

Hossain, M. M., Hasan, R., and Zawoad, S. (2017). Trustiov: A trustworthy forensic investigation framework for the internet of vehicles (iov). In *ICIOT*, pages 25–32.

Ibitoye, O., Abou-Khamis, R., Matrawy, A., and Shafiq, M. O. (2019). The threat of adversarial attacks on machine learning in network security–a survey. *arXiv preprint arXiv:1911.02621*.

Jarmon, J. A. (2019). *The New Era in US National Security: Challenges of the Information Age*. Rowman & Littlefield Publishers.

Jetley, H. (2019). Blockchain implementation for smart grid resilience. In *Proceedings of the International Annual Conference of the American Society for Engineering Management.*, pages 1–9. American Society for Engineering Management (ASEM).

Jian, X., Leng, P., Wang, Y., Alrashoud, M., and Hossain, M. S. (2021). Blockchain-empowered trusted networking for unmanned aerial vehicles in the b5g era. *IEEE Network*, 35(1):72–77.

Johnson, J. and Gheorghe, A. V. (2013). Antifragility analysis and measurement framework for systems of systems. *International Journal of Disaster Risk Science*, 4(4):159–168.

Kahan, J. H., Allen, A. C., and George, J. K. (2009). An operational framework for resilience. *Journal of Homeland Security and Emergency Management*, 6(1).

Karadimas, A., Hewig, E., Behera, S., and Kotisi, T. (2014). Case study of black swans and antifragility. *Semantic Scholar*, pages 1–17.

Kendzierskyj, S. and Jahankhani, H. (2019). The role of blockchain in supporting critical national infrastructure. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, pages 208–212. IEEE.

Klein, L. (2020). Governing critical infrastructure in digital futures. In *Sustainable Development and Resource Productivity*, pages 182–192. Routledge.

Kotsiuba, I., Velykzhanin, A., Biloborodov, O., Skarga-Bandurova, I., Biloborodova, T., Yanovich, Y., and Zhygulin, V. (2018). Blockchain evolution: from bitcoin to forensic in smart grids. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 3100–3106. IEEE.

Liu, Y., Yuan, X., Xiong, Z., Kang, J., Wang, X., and Niyato, D. (2020). Federated learning for 6g communications: Challenges, methods, and future directions. *China Communications*, 17(9):105–118.

Lusetti, M., Salsi, L., and Dallatana, A. (2020). A blockchain based solution for the custody of digital files in forensic medicine. *Forensic Science International: Digital Investigation*, 35:301017.

Mahzarnia, M., Moghaddam, M. P., Baboli, P. T., and Siano, P. (2020). A review of the measures to enhance power systems resilience. *IEEE Systems Journal*.

Malamas, V., Dasaklis, T., Kotzanikolaou, P., Burmester, M., and Katsikas, S. (2019). A forensics-by-design management framework for medical devices based on blockchain. In *2019 IEEE World Congress on Services (SERVICES)*, volume 2642, pages 35–40. IEEE.

Martinetti, A., Chatzimichailidou, M. M., Maida, L., and van Dongen, L. (2019). Safety i–ii, resilience and antifragility engineering: a debate explained through an accident occurring on a mobile elevating work platform. *International journal of occupational safety and ergonomics*, 25(1):66–75.

Mbarek, B., Chren, S., Rossi, B., Pitner, T., et al. (2020). An enhanced blockchain-based data management scheme for microgrids. In *AINA Workshops*, pages 766–775.

Miller, K. W., Morell, L. J., Noonan, R. E., Park, S. K., Nicol, D. M., Murrill, B. W., and Voas, M. (1992). Estimating the probability of failure when testing reveals no failures. *IEEE transactions on Software Engineering*, 18(1):33.

Mohay, G. (2005). Technical challenges and directions for digital forensics. In *First International Workshop on*

Systematic Approaches to Digital Forensic Engineering (SADFE'05), pages 155–161. IEEE.

Mosakheil, J. H. (2018). Security threats classification in blockchains.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., and Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access*, 9:9728–9743.

Mylrea, M. and Gourisetti, S. N. G. (2017). Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In *2017 Resilience Week (RWS)*, pages 18–23. IEEE.

Nallapaneni, M. K. and Chopra, S. S. (2020a). Blockchain-based online information sharing platform for improving the resilience of industrial symbiosis-based multi energy systems. In *Actionable Science for Urban Sustainability 2020, AScUS-2020: AScUS Unconference*.

Nallapaneni, M. K. and Chopra, S. S. (2020b). Enhancing the resilience of urban networked community microgrids: Blockchain-enabled flexible energy trading strategy. In *Actionable Science for Urban Sustainability 2020, AScUS-2020: AScUS Unconference*.

Nguyen, D. C., Pathirana, P. N., Ding, M., and Seneviratne, A. (2021). A cooperative architecture of data offloading and sharing for blockchain-based healthcare systems. *arXiv preprint arXiv:2103.10186*.

Nicholas Taleb, N. (2021). Bitcoin, currencies, and fragility. *Quantitative Finance*, 21(8):1249–1255.

Nuzzolese, E. (2020). Electronic health record and blockchain architecture: forensic chain hypothesis for human identification. *Egyptian Journal of Forensic Sciences*, 10(1):1–5.

Obimbo, C. (2020). Towards vehicular digital forensics from decentralized trust: An accountable, privacy-preservation, and secure realization.

Panteli, M. and Mancarella, P. (2015). The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine*, 13(3):58–66.

Patil, H., Sharma, S., and Raja, L. (2021). Study of blockchain based smart grid for energy optimization. *Materials Today: Proceedings*, 44:4666–4670.

Pérez-Marco, R. and Journée, S. (2016). What is a blockchain.

Pincheira, M., Vecchio, M., Giaffreda, R., and Kanhere, S. S. (2021). Cost-effective iot devices as trustworthy data sources for a blockchain-based water management system in precision agriculture. *Computers and Electronics in Agriculture*, 180:105889.

Rocha, G. d. S. R., de Oliveira, L., and Talamini, E. (2021). Blockchain applications in agribusiness: A systematic review. *Future Internet*, 13(4):95.

Sahdev, N. K., Ahluwalia, G., and Durrie, M. (2021). The antifragility effect: Deploying emerging tech in medical device supply networks to rebuild better. *University College London Centre for Blockchain Technologies*.

Sakhnini, J., Karimipour, H., Dehghantanha, A., and Parizi, R. M. (2020). Ai and security of critical infrastructure.

Samanta, A. K., Sarkar, B. B., and Chaki, N. (2021). Quantified analysis of security issues and its mitigation in blockchain using game theory. In *International Conference on Computational Intelligence in Communications and Business Analytics*, pages 3–19. Springer.

Saminathan, K., Kondaveeti, H. K., and Karunanithi, S. (2021). Structure, security attacks, and countermeasures in the blockchain network. In *Convergence of Blockchain Technology and E-Business*, pages 61–84. CRC Press.

Sanseverino, E. R., Di Silvestre, M. L., Gallo, P., Zizzo, G., and Ippolito, M. (2017). The blockchain in microgrids for transacting energy and attributing losses. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 925–930. IEEE.

Shrivas, M. K., Yeboah, T., and Brunda, S. S. (2020). Hybrid security framework for blockchain platforms. In *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*, pages 339–347. IEEE.

Singh, S. K., Salim, M. M., Cho, M., Cha, J., Pan, Y., and Park, J. H. (2019). Smart contract-based pool hopping attack prevention for blockchain networks. *Symmetry*, 11(7):941.

Song, K. and Li, C. (2021). Blockchain-enabled relay-aided wireless networks for sustainable e-agriculture. *Journal of Cleaner Production*, 281:124496.

Swafford, P. M., Ghosh, S., and Murthy, N. (2006). The antecedents of supply chain agility of a firm: scale development and model testing. *Journal of Operations management*, 24(2):170–188.

Taleb, N. N. (2012). *Antifragile: Things that gain from disorder*, volume 3. Random House Incorporated.

Thompson, M. A., Ryan, M. J., Slay, J., and McLucas, A. C. (2016). A new resilience taxonomy. In *INCOSE International Symposium*, volume 26, pages 1318–1330. Wiley Online Library.

Vannucci, E., Pagano, A. J., and Romagnoli, F. (2021). Climate change management: a resilience strategy for flood risk using blockchain tools. *Decisions in Economics and Finance*, pages 1–14.

Vishwakarma, A. K. and Singh, Y. N. Smart grid resilience and security using blockchain technology.

Wang, D., Wang, H., and Fu, Y. (2021). Blockchain-based iot device identification and management in 5g smart grid. *EURASIP Journal on Wireless Communications and Networking*, 2021(1):1–19.

Wang, S., Wang, C., and Hu, Q. (2019). Corking by forking: Vulnerability analysis of blockchain. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pages 829–837. IEEE.

Zhang, C., Zhu, L., Xu, C., Zhang, C., Sharif, K., Wu, H., and Westermann, H. (2020). Bsfp: Blockchain-enabled smart parking with fairness, reliability and privacy protection. *IEEE Transactions on Vehicular Technology*, 69(6):6578–6591.