Blockchain Patterns in Critical Infrastructures: Limitations and Recommendations

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

Keywords: Critical Infrastructures, Blockchain Patterns, Security, Antifragility, Resilience.

Abstract: The widespread adoption of data-driven applications in critical infrastructures has arisen with security and privacy concerns. Blockchain has received considerable attention to protect critical infrastructures (e.g., healthcare and transportation) that could be subjected to intentional and unintentional cyberattacks. Blockchain patterns as reusable solutions have been used in critical infrastructure software to fulfill security requirements while delivering reliable and trusted services to citizens. Thus, this work provides a comprehensive review of blockchain patterns to examine how they can steer the advancement of critical infrastructures. Through a critical analysis of existing blockchain pattern literature, we identify realistic limitations, lessons learned and open research issues entirely dedicated to advancing blockchain-based antifragile critical infrastructures.

1 INTRODUCTION

The digitization of critical infrastructures (CIs) has gained increasing attention from academic and industrial communities to improve the quality of citizens' life through digital services. However, a digital CI is not a simple technological concept that would only merge between digital elements and physical space to get the information and then convert it into actions for gaining smart capabilities. Instead, it also covers the economic, social, and environmental aspects (Jang and Gim, 2021) that accept the digitization only if it fulfills the protection requirements, such as the absence of unacceptable failures in vital services (like healthcare). In this regard, the different CI definitions have mainly pointed out the importance of protecting CIs. For example, the EU Directive 2008/114/EC (Directive, 2008) has defined CIs as followed: *"A critical infrastructure means an asset, system or part thereof located in Member States that 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"*.

In the digital era, the fundamental problem of CIs centers around the protection of their information to guarantee the continuity and quality of their vital services (Silva et al., 2018). Thus, the application of blockchain technology has been extended recently to CIs (Vance and Vance, 2019) as a trusted security solution to protect sensitive CI information. Thanks to the blockchain characteristics, e.g., transparency, trust, integrity, and redundancy (Vance and Vance, 2019), blockchain (Vance and Vance, 2019) has received positive sightings in CIs due to its capability to enhance their properties, such as resilience and reliability (Gheorghe et al., 2018). However, due to the significant blockchain impact on controlling the CI information and the apparition of security concerns entirely dedicated to blockchain technology (Boireau, 2018), a critical question has been raised in academic and industrial communities on whether the blockchain is capable of supporting the development of CIs (Venkatesh et al., 2020).

Therefore, in this paper, we contribute to the body of knowledge on blockchain and its effective adoption for CI development by examining blockchain patterns as reusable solutions in improving the design qualities of CIs (like transportation). To this end, we focus on studying only the blockchain patterns that have been deployed in real-world scenarios in order to examine convincingly the positive and negative realistic effects of blockchain. Accordingly, we outline a research agenda for blockchain patterns to meet the requirements of CIs that are paving the way for constructing

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

Bangui, H. and Buhnova, B.
Blockchain Patterns in Critical Infrastructures: Limitations and Recommendations.
DOI: 10.5220/0011278500003266
In *Proceedings of the 17th International Conference on Software Technologies (ICSOFT 2022)*, pages 457-468
ISBN: 978-989-758-588-3; ISSN: 2184-2833
Copyright © 2022 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

Table 1: Blockchain Application Examples in Healthcare and Transportation.

Paper	Description
Healthcare Domain	
(Nguyen et al., 2021)	A Cooperative Architecture of Data Offloading and Sharing for Blockchain-based Healthcare Systems
(Chelladurai and Pandian, 2021)	A novel blockchain based electronic health record automation system for healthcare
(Alzubi, 2021)	Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare
(Soni and Singh, 2021)	Blockchain-based security & privacy for biomedical and healthcare information exchange systems
(Rajput et al., 2021)	A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition
Transportation Domain	
(Zhang et al., 2020)	BSFP: Blockchain-Enabled Smart Parking with Fairness, Reliability and Privacy Protection
(Ge et al., 2020)	A semi-autonomous distributed blockchain-based framework for UAVs
(Bera et al., 2021)	Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment
(Gupta et al., 2021)	Blockchain-assisted secure UAV communication in 6G environment
(Alsamhi et al., 2021)	Blockchain for Decentralized Multi-Drone to Combat COVID-19
(Álvares et al., 2021)	Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities

a sustainable digital world.

The remainder of the paper is structured as follows. Section 2 briefly illustrates some blockchain application examples in CIs. Section 3 carries out a literature review on blockchain patterns that have been applied in real-world blockchain-based applications. Moreover, it discusses the pros and cons of blockchain patterns from the critical infrastructure perspective. Sections 4 illustrates an advanced integration of blockchain in CIs. As blockchain patterns would be merged with CIs, Sections 5 highlights some recommendations that could help in dealing with the negative impacts associated with reusing blockchain patterns. Finally, Section 6 concludes the work and outlines the future research.

2 BLOCKCHAIN APPLICATION IN CIs

Blockchain has been adopted in different CI domains thanks to its ability to ensure preventative security measures necessary to sustain the development of their applications. Table 1 illustrates some of the vital domains where the blockchain has received considerable interest. Indeed, blockchain has been used in effective ways to improve the reliability of numerous applications, such as the unmanned aerial vehicles (UAV) that have become a big research topic thanks to their 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). Indeed, blockchain offers trust and security to UAVs that are necessary to resist potential cyber-attacks (e.g., Sybil and GPS spoofing attacks), which may lead to the destruction of available information among the whole UAV system. Blockchain also enhances the coordination between distributed UAVs by solving the computation and storage overhead issues while maintaining its reliability and security benefits.

Despite the positive influence of blockchain in different domains, blockchain is vulnerable to several threats (Wang et al., 2019; Boireau, 2018), such as mining-pool threats that exploit miners to launch attacks (e.g., Pool Hopping (Singh et al., 2019)). Thus, the next section we focus more on examining blockchain patterns as reusable solutions in CIs while pointing out their limitations to determine what kind of blockchain issues that may impact CI protection.

3 BLOCKCHAIN PATTERNS

Due to the importance to provide a proven blockchain design for CIs, blockchain patterns are used to aid in offering best practices for blockchain solutions and addressing common software engineering problems. Furthermore, patterns facilitate the design of a distributed ledger system that is a crucial part of the dependability of CIs. In this respect, the aim of this section is to study how the properties and limitations of blockchain patterns could affect CIs.

3.1 Selection of Blockchain Patterns

From the perspective of software and systems engineering, we conducted a survey of blockchain-patterns literature, spanning from 2008 to the time of writing this paper. Different combination of keywords were used to find relevant studies, such as “Blockchain” and ”design pattern”, ”Blockchain” and ”architectural patterns”, “Blockchain patterns”, and ”blockchain-based patterns”. Furthermore, for each paper, the title and abstract were examined during the initial search to ensure that the paper pertained to blockchain patterns. Overall, 77 articles

Table 2: Selected Blockchain Pattern Studies.

Ref	Category of Patterns	Sub-Category of Patterns	What kind of real-world case study is discussed?	The major issues detected and discussed
(Xu et al., 2018)	Smart Contract Patterns	N/A	General Examples of Real-World Known Uses of Patterns	Limited upgradability, extra cost, lack of flexibility and adaptability
(Zhang et al., 2017)			A Case Study on a Real-World Blockchain-based Healthcare Applications	Extra Cost, latency,leaked Data
(Wohrer and Zdun, 2018; Marchesi et al., 2020; Wöhrer and Zdun, 2018; Bartoletti and Pompianu, 2017)	Ethereum Smart Contract Patterns	N/A	A Case Study on a Real-World Ethereum Blockchain-based Application	Harmful callbacks, adverse circumstances on how and when functions are executed, uncontrollably high financial risks at stake, Untrusted external interactions, data sharing,cascading failures (Other platforms face similar issues as Ethereum)
(Liu et al., 2018)	Smart Contract Patterns	Creational Patterns	A Case Study on a Real-World Blockchain-based Traceability Applications	Extra cost, latency, complexity, steal of digital secret key
		Structural Patterns		
		Inter-behavioral Patterns		
		Intra-behavioral Patterns		
(Xu et al., 2018)	Security Patterns	N/A	General Examples of Real-World Known Uses of Patterns	Dishonest users, compromised Key, latency, extra cost, lack of flexibility and adaptability
(Xu et al., 2018; Weigold et al., 2020; Xu et al., 2021)	Interacting with the External World Patterns	N/A	General Examples of Real-World Known Uses of Patterns	Trust, delay, extra cost, uncertainty, performance, transparency, lack of flexibility and adaptability
(Ladleif et al., 2020)			A Case Study on a Real-World Blockchain-based Weather Warning Applications	Performance
(Xu et al., 2018)	Data Management Patterns	N/A	General Examples of Real-World Known Uses of Patterns	Compromised Key, compromising data integrity, trustworthiness, extra cost, immutable data may be subject to brute force decryption attacks
(Weber et al., 2019)			A specific Study for Multi-Tenant Blockchain-Based Systems	Compromising data integrity
(Eberhardt and Tai, 2017; Chao et al.,)			Specific Studies Focusing on Computation and Data Off-Chaining and Maintaining the Key properties of misused Blockchains	Extra Cost, compromising data integrity, unavailable Data due to malicious intent, leaked Data, trustless computation
(Liu et al., 2020)	Self-Sovereign Identity Patterns	Key Management Patterns	General Examples of Real-World Known Uses of Patterns	Lost or compromised master-key, data loss, extra cost, data integrity, trustworthiness, privacy, Latency, Lack of flexibility and adaptability
		DID management Patterns		
		Credential design Patterns		
(Bandara et al., 2020)	Data Migration Patterns	N/A		
(Xu et al., 2018)	Deployment Patterns	N/A		
(Lu et al., 2021)	Payment Patterns	Token Design Patterns	A Case Study on a Real-World Blockchain-based Payment Applications	Extra cost, privacy, upgradability, data integrity, lack of liquidity, lack of traceability, lack of flexibility and adaptability
		Seller Management Patterns		
		Payment Management Patterns		

were retrieved from academic databases and well-known publishers such as IEEE Xplore Digital Library, ScienceDirect, ACM Digital Library, Springer, and Google Scholar. After that, we examined each work based on full-text read. Then, we identified the primary studies that fulfilled the following criteria:

- Providing detailed blockchain pattern descriptions for developers.
- Describing how to make good use of blockchain patterns in real-world applications.

- Listing blockchain pattern benefits.
- Listing real-world blockchain pattern drawbacks.

Due to the immaturity of software engineering for blockchain (Hakak et al., 2020), we found only 16 comprehensive blockchain pattern studies that provide details of 102 blockchain patterns and meet our engineering perspective views. Table 2 provides more details about the identified blockchain pattern studies.

3.2 Comparison of Blockchain Patterns from CI Perspective

In this section, we aim to review the adaptation and suitability of blockchain patterns for CIs. To avoid overlapping conflict, the 102 blockchain patterns are classified into 9 categories based on real-world blockchain applications (Table 2), which are as follows: Smart contract patterns, ethereum smart contract patterns, security patterns, interacting with the external world patterns, data management patterns, self-sovereign identity patterns, data migration patterns, deployment patterns, payment patterns. After that, we focused on examining the drawbacks cited in each work. The importance of this step is to highlight the major blockchain pattern limitations without focusing only on promoting the benefits of blockchain properties, such as decentralization, transparency, and immutability. Figures 1, 2, and 3 summarize the findings of the major limitations of blockchain patterns to explore whether blockchain patterns would live up to their CI expectations or not.

Findings on the Pattern Benefits. There is no doubt that blockchain has the potential to promote the development of CI systems due to its ability to change the way to store and secure sensitive information effectively against adversaries trying to access data to control or disrupt systems, resulting in boosting the capabilities of CI properties (Gheorghe et al., 2018). For example, thanks to the redundancy and traceability offered by blockchain, resilience and forensic readiness can retrain data from every step of the data generation process in CI systems. Moreover, these CI properties have built trust in blockchain as a distributed database technology that can endorse the data quality and guarantee the correctness of data analysis necessary for making resilient CI systems.

Findings on the Patterns Limitations. Based on reviewing blockchain patterns, we found that the maturity of blockchain is still facing many limitations not yet solved. The major blockchain pattern challenge is maintaining security (Figure 1). Notably, we found that the key compromise is the root cause of security issues in blockchain and its dependent systems as losing this unique and secret key assigned to each user may make sensitive information accessible to unauthorized parties. Moreover, since the blockchain network is decentralized to prevent a single point of security failure, it is hard to identify the behavior of a malicious user who gets the private key of an authorized user. In this critical case, blockchain technology cannot fulfill the requirements of CI properties, such as self-healing resilience that needs accurate data to aid a system to respond rapidly and recover effectively from unexpected setbacks. Likewise, the vulnerable codes in smart contract patterns may cause malicious behaviors of blocks and leave CI systems seriously vulnerable in real circumstances. For example, the invocation of callback functions in Ethereum smart contract patterns (Wohrer and Zdun, 2018; Marchesi et al., 2020; Wöhrer and Zdun, 2018; Bartoletti and Pompianu, 2017) may result in giving a chance to attackers to exploit security bugs and deteriorate CI systems. Equally, privacy and trust are not guaranteed in some blockchain patterns (Figure 1) due to the lack of security countermeasures against such steal of the digital key and leak data. Yet, there is a big need to maintain the security in blockchain patterns, particularly, we need to fix the vulnerabilities of smart contract and find a secured way to share a key over blockchain networks, while guaranteeing and centering CI systems around the promising properties of blockchain technology, such as decentralisation, authentication, confidentiality, integrity, and transparency.

On the other hand, flexibility, adaptability, and upgradability of blockchain patterns (Figure 2) are accompanied with significant limitations that affect the fusion of blockchain within CI systems. For example, in the case of the public blockchain, all smart contracts by default have no owner. As a result, all participants can access all the information and code stored on blockchain without any special privilege. For example, the embedded permission pattern (Xu et al., 2018) is used to restrict access to the invocation of the functions defined in smart contracts. However, the specified permissions cannot be updated or removed once they are issued, which can be considered as a lack of flexibility and adaptability in CI systems. Yet, a mechanism should be proposed to support the flexibility and adaptability of the embedded permission pattern.

Long time to synchronize a large volume of transactions is another gap in blockchain patterns (Figure 2) that may affect data transmission between CI systems, resulting in compromising security concerns as well as reducing the scalability and per-

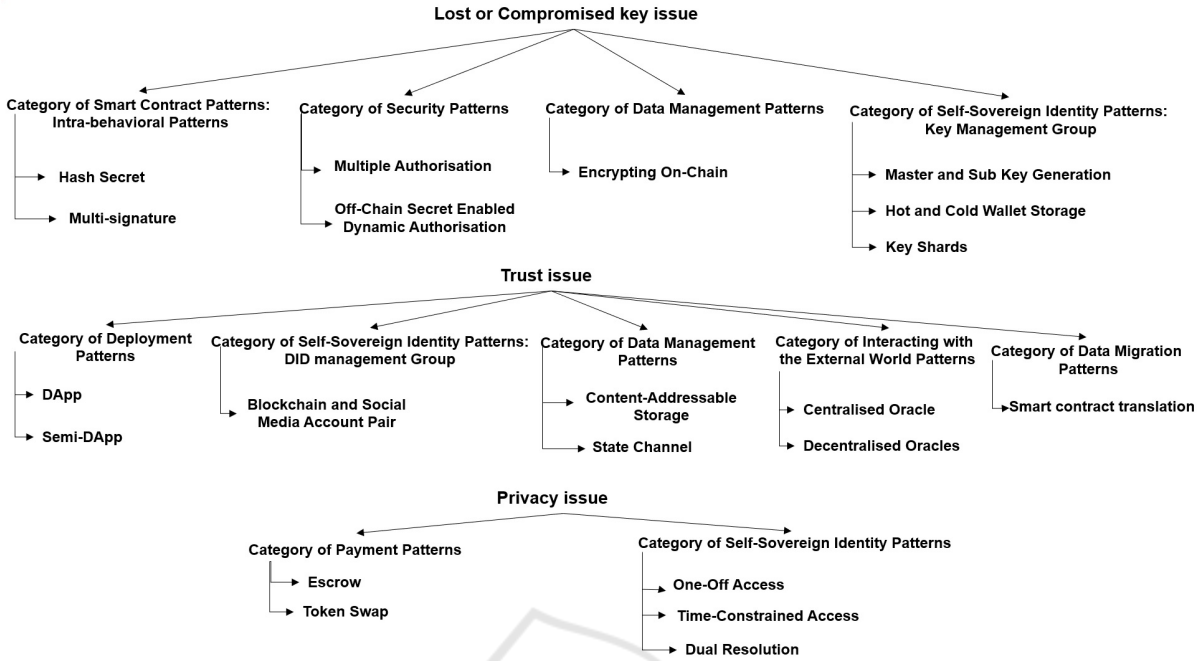

Figure 1: Roadmap of Blockchain Patterns with Compromised Key, Trust, and Privacy Issues.

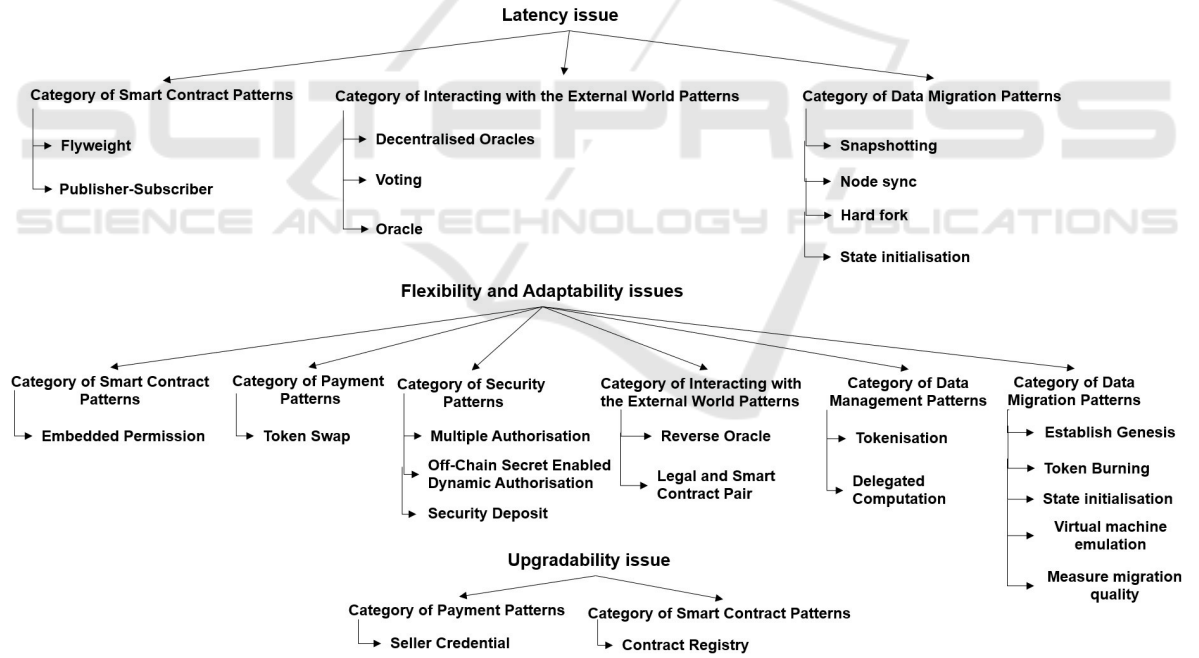

Figure 2: Roadmap of Blockchain Patterns with Latency, Flexibility-Adaptability, and Upgradability Issues.

formance of CI systems. Double-spending (Iqbal and Matulevičius, 2021) is an example of attacks in blockchain that reflects the negative impact of delay between the initiation and confirmation of two transactions. Indeed, double-spending is possible with any attacker who wants to benefit from time-lapse to get the first transaction results before other blocks announce the invalidation of the second transaction. Consequently, blockchain would not be the best security solution that could manage and synchronize real-time sensitive information flow over CIs. Thus, realistic case studies are required to understand how blockchain may process, maintain, and manage transactions over different CIs. Also, experimental studies

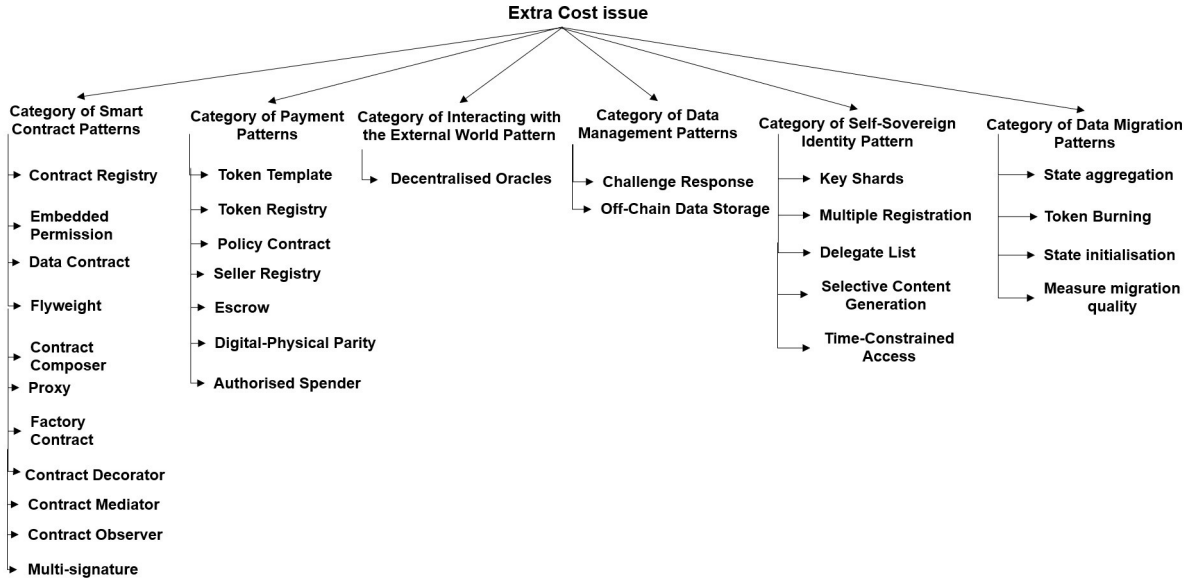

Figure 3: Roadmap of Blockchain Patterns with Extra Cost Issue.

are required to identify in what cases blockchain may cause significant delays, resulting in defining the best practices of blockchain development and supporting data transmission that is the main key for advancing resilient CIs.

Meanwhile, we found that sustainability is still a key barrier to adopt blockchain in CI systems. Indeed, the rising cost of maintaining ledgers and managing data is of extreme concern (Figure 3). For example, the "Off-Chain Data Storage" pattern requires extra communication mechanisms and storage platforms to ensure data sharing (Xu et al., 2018), which can cause significant extra cost for interdependent CIs. Likewise, some blockchain patterns still need qualified and experienced personnel to ensure the correctness of their implementation within a system, such as Learning Curve is mandatory steep for users of DApp Pattern (Xu et al., 2018) to understand the functionality of smart contracts and know-how to verify transactions.

On the other hand, it is expected that data propagated over blockchain would be increased to meet the needs of CI systems. As a result, the computing resources of blocks would be increased, resulting in increased CI energy use. Actually, the current blockchain patterns focus mainly on preventing unauthorized access that is essential for securing any vulnerable system; however, they are not prepared to deal with intensive data storage related to the exponentially increasing complexity of dependent CI system interactions. For example, in (Zhang et al., 2017), a study have been conducted to determine the benefits of the application of patterns to address interoperability in blockchain-based health applications. However, this work has pointed out the major limitations of realizing patterns on the blockchain, which are: high computation delay, extra computation cost, and storage overhead. Thus, there is a necessity to shape an efficient and sustainable blockchain that would control and manage the data generated by smart devices while minimizing the undesirable computation and energy cost impact in CIs.

3.3 Observations

In this section, we summarize lessons learned from the previous section, structured into beneficial properties that can be useful in reconstructing upcoming blockchain patterns and supporting the fusion of blockchain technology within complex CIs. From CI perspective, the beneficial properties of blockchain patterns include:

- The pattern shows its simplicity for non-qualified and experienced personnel to support its wide implementation.
- The pattern shows its trustworthiness through measuring its reputation when CI system participants access to information.
- The pattern shows its dependability through fault-tolerance and resilience in CI systems.
- The pattern shows its flexibility and efficiency through managing large datasets without development overheads.
- The pattern shows its agility through responding to the increasing complexity of CI system interac-

tions and dealing rapidly with their related unexpected circumstances.

- The pattern shows its interpretability and interoperability through comparing and measuring alternative responses to automate the transformation of interdependent and dependent CI systems.
- The pattern shows its adaptability through learning over experience and accommodating new requirements imposed by the ever changing nature of CIs (like need of using further storage space) with minimum cost, energy, and time.

4 ADVANCED BLOCKCHAIN APPLICATION IN CIs

Despite the blockchain pattern limitations, they can be reused to improve the design of CIs. Thus, in this section, we highlight an example of advanced application of blockchain that can support the moving beyond resilience by considering antifragility in CIs (Sartorio et al., 2021; Martinetti et al., 2019). Besides, we try to clarify why we should care about the limitations of blockchain patterns and implications related to them.

4.1 Data Management for Antifragile CIs

Moving towards digitization is not an easy task for CIs since it brings new security concerns (Sartorio et al., 2021; Martinetti et al., 2019). Thus, CIs are looking for strategies that enable them to learn how to autonomously readjust and evolve their function and structure while boosting their robustness.

Nassim Nicholas Taleb in his book "Antifragile: Things That Gain from Disorder" (Taleb, 2012) has introduced the concept of antifragility as 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. Figure 4 provides more clarification concerning the antifragility concept.

4.2 Impact of Blockchain Pattern Limitations in Antifragile CIs

Learning from disorder is the main key in antifragile systems to boost self-improvement and autonomous data-driven decisions (Sartorio et al., 2021; Martinetti et al., 2019). Thus, learning process should be done through truthful information sources to satisfy the requirements of antifragility concept. Therefrom, blockchain is considered as the best security solution that can manage data necessary for realizing truly antifragile systems while addressing their data requirements in terms of trust, transparency, security, immunity, redundancy, and decentralisation.

There is no doubt that blockchain can bring significant security enhancement to antifragile CI systems. However, the fusion of blockchain and antifragile CI systems is a big challenge as blockchain patterns need to address carefully their limitations. For example, due compromised key and immutable data issues, Encrypting on-Chain Data Pattern (Xu et al., 2018) may produce undesirable impact for antifragile systems that center around their informational part.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

5 RECOMMENDATIONS

Blockchain patterns have been merged with CIs to support their digital transformation. However, the blockchain pattern limitations may hinder this fusion as any failure or attack leads to serious interdependent cascading effects.

Therefore, in this section, we list below some potential recommendations that could help in avoiding or minimizing the negative impact of blockchain pattern limitations that may affect CIs.

5.1 Distributed Trust Models for Protecting Private CI Information

5.1.1 Description of the Challenge

Considering the limitations of blockchain patterns detected through realistic scenarios, the users' trust would be affected before and after interactions with blockchain. For example, data leakage is one of the major privacy concerns of blockchain that pushes

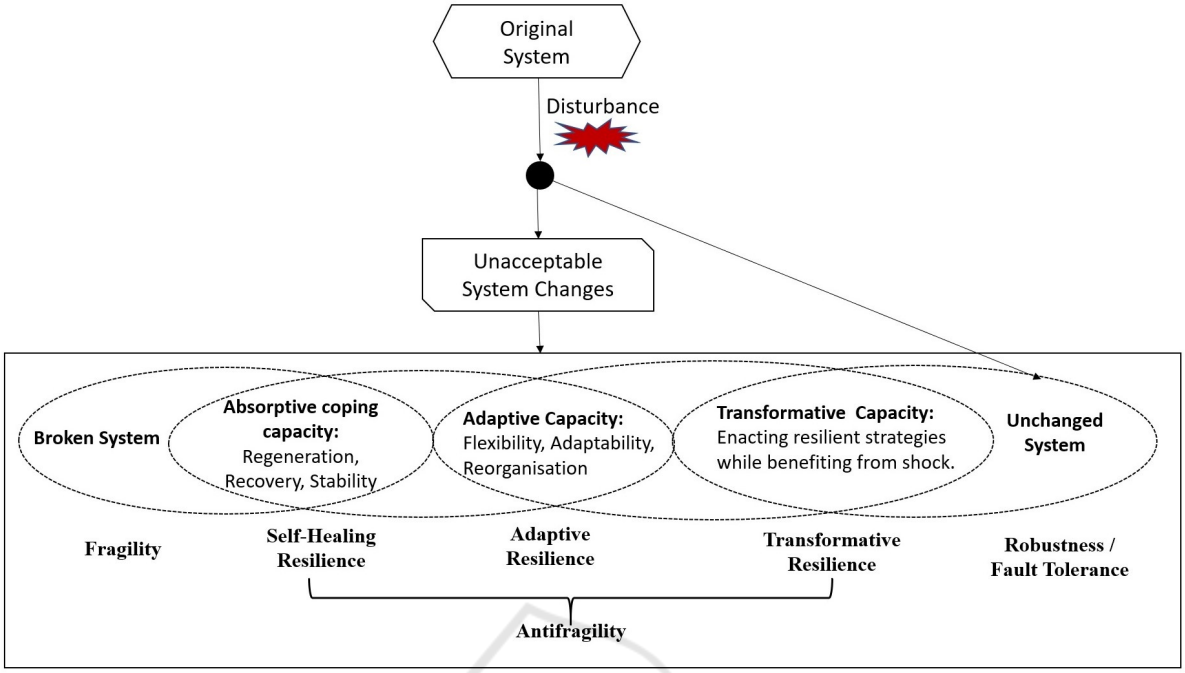

Figure 4: Antifragility Concept.

the owners of sensitive data stored in blocks to switch from overtrust to undertrust blockchain (Zhu et al., 2018). Indeed, in case of information leaking, blockchain can guarantee its trustworthiness property as stored data in blocks are unaffected and still immutable, transparent, and decentralized. However, the ledger cannot guarantee data owners' trust as their personal data can be disclosed without their awareness and misused by unauthorized parties. The data leakage issue could be exacerbated in CIs due to the dependability of a set of functional services on information. In other words, serious security issues can result in the disclosing of information and effect across interdependent CI systems. Yet, ensuring users' trust through blockchain is still a big deal in CI facilities, which are driven by the growing demand for access to information over smart devices.

Some studies have tried to propose methodologies for deciding the suitability of blockchain in industrial areas (Pedersen et al., 2019; Bavassano et al., 2020). However, they have not provided a comprehensive guidelines on how to assess user trust who would be willing to place data on blockchain. Moreover, they have not discussed how to use the existing scales that have been developed to measure user trust in various systems, such as human-computer trust scale(Gulati et al., 2019) and the measurement of the propensity to trust in automation (Jessup et al., 2019).

5.1.2 Recommendation

There is a big need for proposing distributed trust models to empower the blockchain reputation in CIs by representing the trust level of qualitative and quantitative system properties, mainly privacy and safety.

5.2 Other Alternative Distributed Ledger Technologies for CIs

5.2.1 Description of the Challenge

Despite the blockchain advantages in addressing the correctness and trustworthiness of shared information while preserving CI security objectives (Alcaraz and Zeadally, 2015), the blockchain pattern drawbacks may prevent this ledger from compelling its adoption in CIs. To tackle these limitations, some studies have focused on examining the suitability of each blockchain implementation based on the characteristics of a given application (Pedersen et al., 2019). However, blockchain is not the only DLT (Distributed Ledger Technology) that can ensure security and advanced protection against threats in CIs. There are also other DLTs that can be used as alternative solutions for protecting CIs, such as Tangle that is one of the most popular directed acylic graph instances for ensuring high transaction volumes in smart environments (Singh et al., 2021).

Table 3: Comparison of Different Distributed Ledger Technologies (DLTs).

	Blockchain	**Tangle**	**HashGraph**	**HoloChain**	**Tempo**
Licence	Open Source	Open Source	Patented	Open Source	Open Source
Platform(s)	Bitcoin, Litecoin, Ripple, Ethereum, etc.	IOTA	Swirlds	Holo	Radix
Initial Release	2008	2017	2016	2018	2017
Popularity	Very well know	Low	Low	Low	Low
Maturity	Been used	Experimental	Experimental	Experimental	Experimental
Scalability	Low	High	High	High	High
Decentralized	Yes	Semi-Centralized	Semi-Centralized	Yes	Yes
Energy consumption	High	Low	Low	Low	Low
Mining required	Yes	No	No	No	No
Transaction fees	High	Low	Low	Low	Low
Transaction per second	4 to 7	500 to 800	More than 200.000	More than millions	More than 25.000
Latency	High	Low	Subject to Gossiping	Subject to Gossiping	Subject to Gossiping
Security in terms of Availability, Integrity, and Fault Tolerance	High	High	High	High	High

Table 3 provides a comparison between the most popular DLTs in terms of popularity, maturity, scalability, decentralization, energy consumption, latency, transaction fees, mining process, transaction fees per second, and security. As shown in Table 3, there are multiple DLTs but they are still in the infancy stage except blockchain that has been proven and used widely in digital currency security (Singh et al., 2021), which encourages its acceptance in CIs (Georgescu and Cîrnu, 2019).

5.2.2 Recommendation

There is a big need for proposing recommended model approaches to select the best alternative ledger (Table 3) that can assist blockchain in case of poor performance or security and privacy concerns, resulting in supporting the sustainable development of digital CIs.

5.3 Blockchain Checklists for Designing CIs

5.3.1 Description of the Challenge

Blockchain has revolutionized decentralized software architectures and become a fundamental building block of CI designs. However, to date there are no accepted laws and standards that could be followed to unify DLTs in terms of interoperability, architecture, and software design. There are some checklists that can be used to facilitate the integration of blockchain with CIs. Generally, a checklist is a strategic understanding that aims to facilitate the software development process by efficiently instructing and guiding developers. It has been defined as (Singhal and Uthappa, 2019): "A comprehensive formal list of essential actions to be taken in a specific fashion". Thus, a standard checklist can provide a detailed explanation on how integrate blockchain design while fostering dramatically the blockchain adoption in interdependent CIs.

Due to the infancy stage of blockchain development, there are very few studies (Table 4) that are targeted for evaluating blockchain before its implementation. However, they have not devised a standard blockchain model that can be recommended as a mature DLT to fulfill the burst CI needs effectively and elastically. For example, a CI system may request a considerable amount of blockchain resources; simultaneously, its demand may significantly affect the quality of service of its dependable CI systems. Thus, it is necessary to provide an appropriate guideline on monitoring blockchain resource utilization to fulfill the dynamic demands of dependable CIs. Likewise, the related checklist solutions have not dealt well with the compatibility issue between private and public blockchain transactions to fit CI needs (Gheorghe et al., 2018). Furthermore, they have not described how a checklist can contribute in avoiding or minimizing security vulnerabilities and threats of blockchain that may cause severe consequences in CIs, such as data leakage.

5.3.2 Recommendation

Due to the diversity of CIs and the importance of keeping them protected against cyber-attacks (Gheorghe et al., 2018), it is necessary to put forward an institutional model for blockchain that can describe clearly the relations between different DLTs (Table 3) and determine in which case it is recommended to use another DLT instead of blockchain. Furthermore, it is necessary to collect real-world blockchain applications within different contexts to help developers to learn how to make good use of blockchain in CI designs as well as learn how to select a suitable type of blockchain (Andreev et al., 2018), while determining its right technical parameters for each specific CI use case (Gheorghe et al., 2018).

Table 4: Checklists for evaluating the implementation of Blockchain.

Paper	Description
Crypto 2.0 'Lenses' (Jaffrey, 2015)	Develop an evaluation framework specific for the financial applications.
Greenspan (Greenspan, 2015)	Propose a general industrial framework containing eight conditions that should be verified before the implementation of Blockchain.
METI (MET, 2017)	Evaluate the comparability between conventional system and a Blockchain-based systems.
Consensus (Seibold and Samman, 2016)	Propose a questionnaire for evaluating distributed consensus mechanisms.
BLOCKBENCH (Dinh et al., 2017)	Propose a framework for evaluating the performance of private Blockchain components in terms of fault-tolerance, throughput, latency, and scalability.
Case study checklist (Treiblmaier, 2020)	Propose a checklist for writing Blockchain case studies.

6 CONCLUSION

In this work, we investigate the state-of-the-art literature on blockchain patterns to identify the real-world blockchain limitations that could make barriers in adopting the blockchain technology in CIs (like transportation systems). Accordingly, a list of lessons learned is highlighted to facilitate the fusion of blockchain within CIs. This is followed with the discussion of the implications and future directions of blockchain research roadmap, following the trends of distributed trust models, antifragile systems, checklists, and other alternative distributed ledger technologies.

Understanding that the use of digital technologies is becoming a fact in our life and every digital system is vulnerable, the management of disturbances has become a top-priority concern for creating sustainable CI systems. Thus, as a future work, we plan to assess the degrees of blockchain criticality, and investigate how to further advance blockchain integration within CIs.

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

(2017). Evaluation forms for blockchain-based system.

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.

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.

Alzubi, J. A. (2021). Blockchain-based lamport merkle digital signature: Authentication tool in iot healthcare. *Computer Communications*, 170:200–208.

Andreev, R., Andreeva, P., Krotov, L., and Krotova, E. (2018). Review of blockchain technology: Types of blockchain and their application. *Intellekt. Sist. Proizv.*, 16(1):11–14.

Bandara, H. D., Xu, X., and Weber, I. (2020). Patterns for blockchain data migration. In *Proceedings of the European Conference on Pattern Languages of Programs 2020*, pages 1–19.

Bartoletti, M. and Pompianu, L. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns. In *International conference on financial cryptography and data security*, pages 494–509. Springer.

Bavassano, G., Ferrari, C., and Tei, A. (2020). Blockchain: How shipping industry is dealing with the ultimate technological leap. *Research in Transportation Business & Management*, 34:100428.

Bera, B., Das, A. K., and Sutrala, A. K. (2021). Private blockchain-based access control mechanism for unauthorized uav detection and mitigation in internet of drones environment. *Computer Communications*, 166:91–109.

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

Chao, S.-T., Zhao, Y., and Zhao, J. Reviewing blockchain scalability challenge with a discussion of off-chain approaches.

Chelladurai, U. and Pandian, S. (2021). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–11.

De Florio, V. (2014). Antifragility= elasticity+ resilience+ machine learning models and algorithms for open system fidelity. *Procedia Computer Science*, 32:834–841.

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., and Tan, K.-L. (2017). Blockbench: A framework for analyzing private blockchains. In *Proceedings of the 2017 ACM International Conference on Management of Data*, pages 1085–1100. ACM.

Directive, C. (2008). 114/ec on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*, 23:2008.

Eberhardt, J. and Tai, S. (2017). On or off the blockchain? insights on off-chaining computation and data. In *European Conference on Service-Oriented and Cloud Computing*, pages 3–15. Springer.

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*.

Ge, C., Ma, X., and Liu, Z. (2020). A semi-autonomous distributed blockchain-based framework for uavs system. *Journal of Systems Architecture*, 107:101728.

Georgescu, A. and Cîrnu, C. E. (2019). Blockchain and critical infrastructures–challenges and opportunities. *Romanian Cyber Security Journal*, pages 2668–1730.

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.

Greenspan, G. (2015). Avoiding the pointless blockchain project. *MultiChain, blog*.

Gulati, S., Sousa, S., and Lamas, D. (2019). Design, development and evaluation of a human-computer trust scale. *Behaviour & Information Technology*, 38(10):1004–1015.

Gupta, R., Nair, A., Tanwar, S., and Kumar, N. (2021). Blockchain-assisted secure uav communication in 6g environment: Architecture, opportunities, and challenges. *IET Communications*.

Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., and Guizani, N. (2020). Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Network*, 34(1):8–14.

Iqbal, M. and Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. *IEEE Access*, 9:76153–76177.

Jaffrey, H. (2015). Crypto 2.0 'lenses'. *LinkedIn Pulse blog, April*, 17.

Jang, S.-g. and Gim, T.-H. T. (2021). Considerations for encouraging citizen participation by information-disadvantaged groups in smart cities. *Sustainable Cities and Society*, page 103437.

Jessup, S. A., Schneider, T. R., Alarcon, G. M., Ryan, T. J., and Capiola, A. (2019). The measurement of the propensity to trust automation. In *International Conference on Human-Computer Interaction*, pages 476–489. Springer.

Ladleif, J., Weber, I., and Weske, M. (2020). External data monitoring using oracles in blockchain-based process execution. In *International Conference on Business Process Management*, pages 67–81. Springer.

Liu, Y., Lu, Q., Paik, H.-Y., and Xu, X. (2020). Design patterns for blockchain-based self-sovereign identity. In *Proceedings of the European Conference on Pattern Languages of Programs 2020*, pages 1–14.

Liu, Y., Lu, Q., Xu, X., Zhu, L., and Yao, H. (2018). Applying design patterns in smart contracts. In *International Conference on Blockchain*, pages 92–106. Springer.

Lu, Q., Xu, X., Bandara, H., Chen, S., and Zhu, L. (2021). Design patterns for blockchain-based payment applications. *arXiv preprint arXiv:2102.09810*.

Marchesi, L., Marchesi, M., Pompianu, L., and Tonelli, R. (2020). Security checklists for ethereum smart contract development: patterns and best practices. *arXiv preprint arXiv:2008.04761*.

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.

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*.

Pedersen, A. B., Risius, M., and Beck, R. (2019). A ten-step decision path to determine when to use blockchain technologies. *MIS Quarterly Executive*, 18(2):99–115.

Rajput, A. R., Li, Q., and Ahvanooey, M. T. (2021). A blockchain-based secret-data sharing framework for personal health records in emergency condition. In *Healthcare*, volume 9, page 206. Multidisciplinary Digital Publishing Institute.

Sartorio, F. S., Aelbrecht, P., Kamalipour, H., and Frank, A. (2021). Towards an antifragile urban form: a research agenda for advancing resilience in the built environment. *Urban Design International*, pages 1–24.

Seibold, S. and Samman, G. (2016). Consensus: Immutable agreement for the internet of value. *KPMG¡ https://assets. kpmg. com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism. pdf*.

Silva, B. N., Khan, M., and Han, K. (2018). Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable Cities and Society*, 38:697–713.

Singh, S., Hosen, A. S., and Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access*, 9:13938–13959.

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.

Singhal, S. and Uthappa, M. C. (2019). Role of a checklist to improve patient safety in interventional radiology. *Journal of Clinical Interventional Radiology ISVIR*.

Soni, M. and Singh, D. K. (2021). Blockchain-based security & privacy for biomedical and healthcare information exchange systems. *Materials Today: Proceedings*.

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

Treiblmaier, H. (2020). Toward more rigorous blockchain research: Recommendations for writing blockchain case studies. In *Blockchain and Distributed Ledger Technology Use Cases*, pages 1–31. Springer.

Vance, T. R. and Vance, A. (2019). Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, pages 107–112. IEEE.

Venkatesh, V., Kang, K., Wang, B., Zhong, R. Y., and Zhang, A. (2020). System architecture for blockchain based transparency of supply chain social sustainability. *Robotics and Computer-Integrated Manufacturing*, 63:101896.

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.

Weber, I., Lu, Q., Tran, A. B., Deshmukh, A., Gorski, M., and Strazds, M. (2019). A platform architecture for multi-tenant blockchain-based systems. In *2019 IEEE International Conference on Software Architecture (ICSA)*, pages 101–110. IEEE.

Weigold, M., Barzen, J., Breitenbücher, U., Falkenthal, M., Leymann, F., and Wild, K. (2020). Pattern views: Concept and tooling for interconnected pattern languages. In *Symposium and Summer School on Service-Oriented Computing*, pages 86–103. Springer.

Wöhrer, M. and Zdun, U. (2018). Design patterns for smart contracts in the ethereum ecosystem. In *2018 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 1513–1520. IEEE.

Wohrer, M. and Zdun, U. (2018). Smart contracts: security patterns in the ethereum ecosystem and solidity. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pages 2–8. IEEE.

Xu, X., Bandara, H., Lu, Q., Weber, I., Bass, L., and Zhu, L. (2021). A decision model for choosing patterns in blockchain-based applications. In *18th IEEE Int. Conf. on Software Architecture (ICSA 2021)*.

Xu, X., Pautasso, C., Zhu, L., Lu, Q., and Weber, I. (2018). A pattern collection for blockchain-based applications. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs*, pages 1–20.

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.

Zhang, P., White, J., Schmidt, D. C., and Lenz, G. (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. *arXiv preprint arXiv:1706.03700*.

Zhu, L., Zheng, B., Shen, M., Yu, S., Gao, F., Li, H., Shi, K., and Gai, K. (2018). Research on the security of blockchain data: A survey. *arXiv preprint arXiv:1812.02009*.