JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 39, 197-222 (2023)
DOI: 10.6688/JISE.202301_39(1).0012

A Systematic Analysis of Security in Blockchain

MARIA I. ORTEGA[1,3], JULIO MORENO[1,4], MANUEL A. SERRANO[2]
AND EDUARDO FERNÁNDEZ-MEDINA[1]
[1]*GSyA Research Group*
[2]*Alarcos Research Group*
University of Castilla-La Mancha
Ciudad Real, 13071 Spain
[3]*Telefónica, Madrid, 28050 Spain*
[4]*IBM, Madrid, 28002 Spain*
E-mail: mariaisabel.ortegacanalejo@telefonica.com; Julio.Moreno@alu.uclm.es;
{Eduardo.FdezMedina; Manuel.Serrano}@uclm.es

Blockchain has consolidated its status as one the most disruptive technologies of the last few years. Recent attacks on blockchain, are constantly being identified, highlighting the need to strengthen their security. For that reason, security of blockchain technology is now more than ever in the spotlight. The high economic impact on cryptocurrencies and the sensitive information proposed to be handled by their networks (*i.e.*, implementation of notaries, electronic voting, …) make security an essential aspect. This paper aims to determine the main security problems which have been identified in blockchain by following a well-known methodology called "Systematic Mapping Studies". Systematic Mapping Studies are designed to convey an outline of our analysis space through classification and investigating contributions regarding classes of that classification. This work aims to address the main security problems in blockchain technologies and analyze their solutions. Finally, a proposal was made to define a model of improvement in the security of blockchain. The purpose of this model is to allow a better understanding of the security concepts and the typical structure of this kind of environment.

Keywords: blockchain, security, systematic mapping study, security model, threats

1. INTRODUCTION

Over the last few years, blockchain has been consolidated as a technology that allows data and transactions to be to be securely stored and verified without the need for any centralized authority [1]. Blockchain is a decentralized ledger that keeps record transaction that takes place across a peer-to-peer network. This allows for data exchange to be made directly with third-parties involvement. Its main features, which have contributed to attracting such interest, are the guaranteed integrity of its data and fault tolerance. This fault tolerance is achieved through the use of cryptographic puzzle technology to achieve consensus and agreement on the transactions that are conducted [2].

Blockchain has brought new concepts for the resolution issues in cloud information storage as the Internet of Things (IoT), and other areas, making blockchain a popular topic not only in the industry but also in the scientific community. Several reports also point to increased awareness of the use of blockchains in many applications and significant investment in the development of blockchain by various industries. The blockchain is expected to lead to considerable change in a wide range of systems and enterprises [3]. Distributed reliability and consequently, security and privacy are at the heart of the block-

Received December 28, 2020; revised October 13 & December 20, 2021; accepted May 6, 2022.
Communicated by Rolando Nuñez Edward Valdez.

chain technologies and can make them successful or make them fail [4].

Although blockchain technology is presented as a tamper-proof transaction ledger technology, the reality is that blockchain networks are not immune to cyber-attacks and fraud. Some attacks and security vulnerabilities were recently made public, and it is necessary to keep in mind that smart contracts with security vulnerabilities can cause financial losses. As an example, thieves and scammers stole more than $356 million from exchanges and users in the first quarter of 2019 [5]. The popular Bitcoin wallet "Electrum" reported an attack on its servers in April 2019; the economic consequences of this attack are calculated in millions of dollars [6]. Moreover, blockchain threat intelligence firm Ciphertrace [7] shows that $100 million has been subtracted from distributed networks in 2020 alone, reinforcing the importance of security features in any blockchain solution.

Understanding the state-of-the-art of blockchain security is crucial to identify the main trends and gaps in this field and how it has been addressed in academia and industry. This study aims to gather the main vulnerabilities and threats in blockchain, making a proposal for improvement based on these to advance the field of security in this area.

The remainder of his paper is organized as follows. Section 2 introduces the concept of blockchain. Section 3 presents related work with this paper. Section 4 outlines the Systematic Mapping Study (SMS) carried out and describes the activities of the SMS process. Section 5 presents the main results obtained through this paper and a proposal. Additionally, an example of the application of the proposed security model is included in this section. The paper concludes with a discussion of the results and a security model proposal to increase the security of the blockchain as well as outlines future work.

2. BLOCKCHAIN OVERVIEW

Blockchain technology was introduced by Satoshi Nakamoto under the term Bitcoin [1]. Bitcoin is outlined as one of the applications of blockchain technology within the monetary field. The blockchain technology is nothing over a distributed ledger. It will method transactions between people and organizations while not the necessity for third-party involvement [8]. Fig. 1 shows a blockchain Technology architecture. The main blockchain elements are [8]:

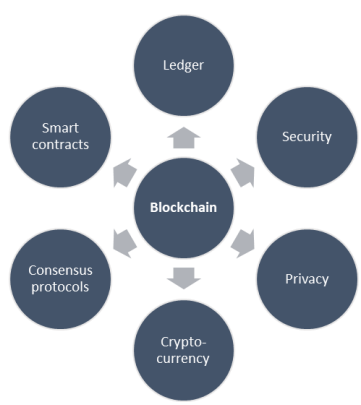

Fig. 1. Main components of blockchain technology.

1. Ledger: As a distributed and consensually shared database, the copied record is the same because the collaboration with the network.
2. Consensus Protocols: Every part of the network ought to verify each transaction. All the nodes within the network ought to agree on the transactions listed on the fresh deep-mined block [3].
3. Security: Digital signature and public-key cryptography techniques are used to validate network transactions.
4. Privacy: all sorts of information are often kept within the blockchain. The privacy rules are applicable if sensitive data is processed.
5. Smart contract: Agreements with a self-executing and self-performing facility. It can obtain data from external sources, to assess that data is not manipulated a cryptogramphical proof will be included.

Blockchains are supposed to have inherited numerous security characteristics. The main characteristics associated with blockchains are [4]: Immutability, auditability, integrity, authorization, fault tolerance, transparency, availability, consistency, and privacy. The holistic blockchain approach includes the entities validation and agreement, transactions transparency, confidence in the proof and communication protocol, the protection of unauthorized persons, the compromised nodes, or the failure of the server. blockchain systems are mainly used to consider security in the following aspects [8]:

- Ledger level security: Members only participate in blocks. Member-initiated operation need to be signed, and members must produce network transactions.
- Network level security: Node relations among other nodes must be secure from network perspective. It should be tolerant to external and internal network attacks.
- Transaction-level security: All transactions have to be encrypted with Public Key Infrastructure (PKI). No one is allowed to change the transaction details and a multi-signature function will be available for sensitive transactions in the blocking chain.
- Associated surround system security: The related components of the surround system, such as fictitious databases, must be accessible to valid users. To accomplish this, authentication and authorization mechanisms must be implemented.
- Smart contract security: It can be pre-programmed with auto-execution capability. Smart contracts must follow the basic rules given by the network. It may need data from external sources that can be altered. For this reason, cryptographic proof is needed.

Nodes usually compete to publish the next block at the same time with the aim of win cryptocurrencies and/or transaction fees. The consensus model should work even within the presence of probably malicious users since permissionless users would possibly arrange to disrupt or take over the blockchain to achieve fees. Note that legal actions can be applied to authorized blockchain networks if a user acts maliciously. Consensus methods are aimed to propose a solution to the Byzantine Generals Problem. The Byzantine Generals Problem, first described in Lamport *et al.* [9], is associated with a communication failure.

3. RELATED WORK

Despite different researches that have been done in blockchain security since the emergence of the first real blockchain application in 2009, the issue has not been sys-

tematically addressed in a widespread sense. A systematic mapping study (SMS) is a research methodology developed to identify, evaluate, and interpret all relevant information on a topic in order to answer specific research questions. This paper addresses a SMS following a widely used and validated methodology proposed by Brereton *et al.* [10]. It allows us to obtain an auditable procedure and a strict selection of primary studies that support stronger conclusions to address security in blockchain systems by identifying existing vulnerabilities and attacks in these systems and possible security solutions that can be implemented.

Security issues and vulnerabilities of blockchain have been addressed in studies as K. Jonathan points out [11]. This study highlights the problem of security in blockchain if a blockchain with crucial data is to be implemented and highlights that much emphasis would need to be placed on this area at present. A. Averin *et al.* [12] analyzed the security vulnerabilities of blockchain to identify future possible vulnerabilities. These vulnerabilities are also tackled by Shrivas *et al.* [13] who identified different types of blockchain threats and categorized them based on blockchain Platform Components.

X. Li *et al.* [14] realized a survey focusing on the security risks to popular blockchain systems, real attacks on popular blockchain systems, and present the practical academic achievements for enhancing security of blockchain.

Huynh *et al.* [15] also outlined some security attacks from blockchain overlapping mostly with those identified by Anita *et al.* [16]. Both studies highlight a challenge that needs to be addressed as soon as possible by stressing that the security framework faces current research in the field of security systems that needs a dynamic and adaptable security framework.

A classification of the consensus algorithms and a comprehensive comparison of studied consensus algorithms were discussed in Alsunaidi *et al.* [17]. This study highlights that blockchain technology today is in its infancy; the future of the platform looks promising and requires but close attention from developers and the scientific community.

X. Zheng *et al.* [18] investigated the state-of-the-art progress of blockchain and also make experiments on Ethereum and survey other popular blockchain platforms on the scalability feature of blockchain. Moreover, [19] focuses on Ethereum smart contracts rather than popular blockchain systems. Viewed from a security programming perspective, his work discussed the security vulnerabilities of Ethereum's intelligent contracts and delivers a taxonomy of common programming pitfalls that can potentially lead to exploits. The smart contract issue has been the subject of interest, with recent studies [20] linking the applications of blockchain and smart contracts, their main problems, and the corresponding solutions

H. Chen *et al.* [21] provide a systematic study on the security of Ethereum systems, analyzing vulnerabilities, attacks and defenses, as well as relationships in the Ethereum platform and the environment in which Ethereum operates. As a result, they list 40 types of Ethereum vulnerabilities in Ethereum architecture layers and systematize their root causes.

J. Cheng *et al.* [22] summarizes basic security properties of blockchain and from the view of the blockchain's architecture. They describe security threats and attacks of blockchain, including weak anonymity, vulnerability of P2P network, consensus mechanism, incentive mechanism and smart contract. Although a detailed description is provided, this is not a systematic review of the literature. No proposals or solutions are offered in response to the attacks and threats presented.

This study aims not only to systematically address existing solutions to improve security in blockchain but also to make a proposal for improvement in this area from the knowledge obtained through this review.

4. SYSTEMATIC MAPPING STUDY OUTLINE

Systematic mapping studies (SMS) outlines a research area through classification and enumeration of entries in relation to the categories in that classification [23]. Conducting a SMS allows to increase the reliability and the confidence in the obtained results. SMS consist of three activities: planning, execution, and reporting [24]. Every one of them is divided into different steps.

The aim of this SMS is to obtain evidence (empirical and non-empirical) on existing proposals to increase security in blockchain technology for this purpose, the subsequent research question was proposed:

"What are the main security problems on blockchain?"

Since this question is too wide, we divided it into four research questions in Table 1.

Table 1. Research questions.

Research questions	Main motivation
RQ1. Which are the main kinds of attacks performed on blockchain?	Identify those attacks to which blockchain are vulnerable, resulting in a loss of confidentiality, integrity, and data availability.
RQ2. What security vulnerabilities have been identified by researchers on blockchain?	Identify weaknesses in the blockchain environment that have been identified by researchers, as well as the methods used to mitigate these vulnerabilities.
RQ3. What mechanisms of blockchain design or building exist to enhance its security?	Identify the methods of designing or building blockchains that exist to enhance their security.
RQ4. At what point of maturity is the security research blockchain and how has the interest evolved over time?	Determine the interest in blockchains by academia and industry as well as whether or no research has been empirically validated.

4.1 Search Strategy

The search strategy was defined using Kitchenham *et al.* guidelines [24]. It includes the creation of search string, the definition of search sources and search period. The search string was formed applying Brereton steps [10]: (i) Obtain key terms from the questions; (ii) Identify different spellings, synonyms and connected terms for main term; (iii) Utilize the Boolean OR to include different spellings, synonyms and associated terms; and (iv) Use the Boolean AND to relate the main terms.

Consequently, we broke down the research question into separate elements regarding technology, type of study, and answer measures to obtain the key search terms. In second place, the obtained keywords from the primary studies were assessed with respect to other main terms. Following this, we identified the synonyms of the main terms. Lastly, we con-

structed the search string utilizing the Boolean "AND" in order to connect the main terms and "OR" in order to incorporate all synonyms. Through this process, both the main search terms and the alternative terms (spelling, synonyms and terms related to the main terms) have been defined as presented in Table 2.

Table 2. Terms in the search string.

Main Terms	Additional Terms
Security	("Secur*" OR "privac*" OR "integri*" OR "availab*")
blockchain	("blockchain" OR "DTL*" OR "bitcoin" OR "Ethereum")

The resulted search string is the following:

("Secur*" OR "privac*" OR "integri*" OR "confidential*" OR "availabl*") AND ("blockchain" OR "DTL*" OR "Bitcoin" OR "Ethereum")

Research was conducted in digital libraries with a wide variety of computer journals. In particular, the search was performed on Scopus database, IEEE Digital Library and ACM Digital Library. To guarantee the accuracy of the articles to be studied, only journal articles, workshop documents and conference documents were examined. A summary of the defined search strategy is shown in Table 3.

Table 3. Search strategy.

Databases	Scopus, IEEE Digital Library and ACM Digital Library
Target items	Journal papers, Conference and Workshop papers
Search applied to	Title, Abstract and Keywords
Language	Papers written in English.
Publication period	From 2009 as the milestone of bitcoin appearance until October 2021

4.2 Selection Criteria and Procedure

The purpose of this SMS was to bring to light all the works that introduce any research regarding the security of blockchain, which have been written in English and published until October 2021. The arrival of bitcoin has been established as a relevant event owing to the relevance of this milestone in the use of blockchain technology. Therefore, publications since 2009 have been included as part of our scope. Papers were omitted based on the criteria shown in Table 4.

Table 4. Inclusion/exclusion criteria.

Inclusion criteria	Journals, conferences, and workshop papers. English language documents. Published papers up to October 2021 (incl.).
Exclusion criteria	Papers not aiming at blockchain/DTLs security. Papers aiming at blockchain/DTLs applications. Duplicate papers. Papers in which blockchain/DTLs security is referred to only as a introductory term.
Search applied to	Title, Abstract and Keywords
Language	English
Publication period	From 2009 as the milestone of bitcoin appearance until October 2021

Two stages of the study selection process were carried out from the final string. In the first step, the selection of studies was made by reviewing the title, abstract, and keywords of the studies; only papers addressing the security of blockchains were accepted. In the second stage, from the set of studies selected in the first stage, we examine the full texts of these studies and then applied the inclusion and exclusion criteria.

4.3 Data Extraction and Synthesis Procedure

Data extraction implies reviewing primarily studies looking for useful information According to Kitchenham *et al.* [24] the data extraction implies that results must be contrasted and conflicts must be resolved.

Furthermore, the synthesis of data implies checking and synthesizing the results of the primary studies [10]. Synthesis is often descriptive but it's generally potential to enhance a descriptive synthesis with a quantitative outline.

In the first half, overall "demographic" data like title, authors, and establishment were included. The second half included the dimensional classification related to the research questions outlined above.

4.4 Extraction and Data Synthesis Procedure

Five dimensions were used to classify the investigation, based on the research questions. This classification scheme was established earlier for data extraction. The potential categories were selected considering the results found during the review. Table 5 shows the resultant classification.

Table 5. Summary of the classification scheme.

Dimensions	Categories
Attacks	51% attack, balanced attack, block discarding attack, cache attacks, collapse of the decentralized, DAO attack, DDoS attack, death spiral, double spending attack, eclipse attack, fork-after-withholding (FAW) , hijacking attack, liveness attack, long-range attack, malicious contracts, malleability attack, mining malware, p+ epsilon attack, partitioning attack, phishing, private key threats, pseudonymity, ransomware, reentrancy attack, selfish mining attack, spam attack, sybil attack, tampering, the balance attack, time jacking attacks and wallets injection.
Weaknesses	Poor architecture design, poor network design, poor cryptography, poor access management, smart contracts and consensus.
Security reinforcement methods	Architecture proposed solution, consensus proposed solution, cryptography proposed solution and network proposed solution.
Research method	Proposal, evaluation, validation, philosophical, opinion or personal experience [25].
Time evolution	Year of the publication.
Dimensions	Categories

5. RESULTS AND DATA SYNTHESIS

In this section, the answers to each of the questions formulated in Section 2 are presented and discussed.

5.1 RQ1: Which are the main kinds of attacks performed on blockchain?

Although blockchain were initially presented as a secure and reliable method, recurrent attacks in both industries and cryptocurrencies reveal security breaches. This question exposes multiple attacks scenarios that have been performance on blockchains and are therefore of concern to both academia and industry. The SMS reveals that the most usual attacks are Double Spending Attack (12.38%) and 51% attacks (12.38%) nearly followed by DDoS attacks (9.52%).

The results are explained taking into account that most of the blockchains' security is based on the principle that no entity should have more than 50% of the processing power since such entity can efficiently control the system while sustaining the longest chain [26]. private blockchain is created by this attack, which is totally independent from the real version of the chain. Later, the separated chain is presented to the network to be established as a real chain. As a result, a double-spending attack is possible [27].

Distributed denial-of-service (DDoS) is used to stop resources being available to network members by inundating them with distributed end traffic. DDoS represents one of the commonest attacks in the blockchain network employed by attackers to prevent authentic transactions from being executed. [28].

The problem of double spending allows the same single digital system can be spent more than once, and this is possible because a digital token consists of a digital file that can be duplicated or forged [29]. The creator of Bitcoin was in tune with the problem of double spending, and included it in the seminal white paper that outlined the deployment of Bitcoin (2008) [1].

Other common attacks not only associated with blockchain technology are also exploited. Attacks mentioned previously and the appearances of these attacks in each of the selected primary studies is shown in the table below.

Table 6. Distribution of papers per attack referred.

RQ1	Reference
51% Attack	[30] [31] [32] [14] [33] [27] [34] [35] [36] [37] [38] [39] [40] [41]
Balance attack	[14] [36]
Block Discarding Attack	[42] [43]
Cache Attacks	[44]
Collapse of the decentralized	[30]
DAO attack	[30] [14]
DDoS attack	[4] [45] [46] [28] [47] [27] [36] [38] [35] [48] [49] [41]
Death Spiral	[33]
Double spending attack	[50] [4] [32] [42] [26] [27] [34] [35] [38] [51] [39] [52] [41]
Eclipse Attack	[42] [14] [34] [38] [41]
Fork-After-Withholding	[53] [35]
Hijacking attack	[14] [27]
Liveness attack	[14] [36]
Long-Range Attack	[27]
Malicious contracts	[4] [54] [45] [55] [26] [56] [36]
Malleability attack	[34] [35]
Mining malware	[4] [31]

RQ1	Reference
P+ Epsilon Attack	[27]
Partitioning attack	[34]
Phishing	[30] [40] [40]
Private Key Threats	[14] [34]
Pseudonymity	[14]
Ransomware	[30]
Re-entrancy Attack	[36] [40] [40]
Selfish Mining Attack	[42] [14] [33] [26] [57] [53] [36] [38] [41] [58]
Spam attack	[50] [45] [59] [60]
Sybil Attack	[27] [34] [38]
Tampering	[34]
The Balance Attack	[27]
Time jacking attacks	[4] [45] [36]
Wallets injection	[31] [35] [38]

5.2 RQ2: What security vulnerabilities have been identified by researchers on blockchain?

The different attacks performed over on blockchains, reveals the high number of vulnerabilities related to this kind of technology. The objective of this question is to identify which vulnerabilities are of most concern to researchers, either because of the criticality of this vulnerability or because of the impact it can have if exploited by attackers.

The different weaknesses identified have been classified according to the element of the blockchain that is vulnerable: Poor architecture design, poor network design, poor cryptography, poor access management, smart contracts, or consensus. The results obtained stood out a serious concern about poor network design on blockchains. More than half of the primary studies that address the vulnerabilities of blockchains, are mainly concerned about the attacks related with network issues lack and the security gap that this fact represents. Fig. 2 shows the most relevant blockchain vulnerabilities identified through this SMS the number of primary studies that deal with this issue.

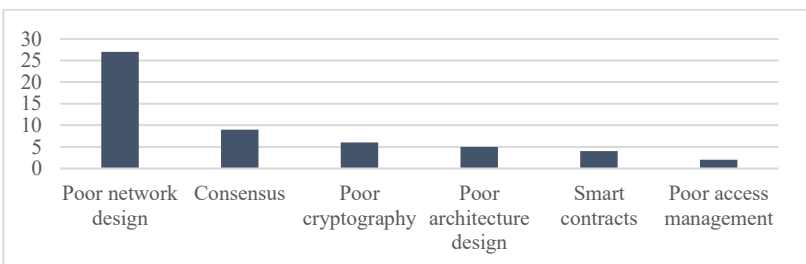

Fig. 2. Most relevant blockchain vulnerabilities.

The blockchain network security issues is the hottest research topics in the area of network security [35]. Among the different attacks, most relevant attacks are related with network security in blockchain.

Most concerns are not only present in blockchain instead they are generic problems that we can find in other distributed systems. One example is distributed denial of service (DDoS) attacks, which constitute one of the most common bandwidth consumption attacks [35]. An eclipse attack is the second most common attack on a Bitcoin system (peer-to-peer network), occurring in a scenario called network division [61]. On a P2P system, a shared application environment that splits workloads or tasks between peers, with no stable hosts and no peers, communicates through gossip protocols [62]. In an eclipse attack, a single node appears to be inaccessible to other nodes on the network, meaning that it could be exploited by an attacker. The distribution of each of the vulnerabilities mentioned previously and the appearances of each of it in the selected primary studies is shown in Table 7.

Table 7. Distribution of papers per attack and weaknesses.

RQ2	Reference
Poor network design	[28] [63] [35] [14] [59] [64] [65] [60] [66] [45] [4] [46] [26] [50] [33] [47] [42] [53] [54] [39] [40] [17] [48] [67] [52] [68] [69]
Poor cryptography	[35] [65] [45] [32] [42] [70]
Consensus	[71] [14] [55] [26] [54] [72] [73] [43] [58]
Poor architecture design	[35] [14] [27] [74] [75]
Smart contracts	[35] [14] [56] [76]
Poor access management	[35] [77]

Moreover, the different attacks have been classified according to the element of the blockchain that is vulnerable. As a result, Table 8 has been obtained. This table allows us to observe at which point in the architecture of a blockchain system solutions must be offered to prevent a given attack on a blockchain system. For each attack, vulnerable elements have been marked with a check (✔) mark.

Table 8. Distribution of papers per attack referred.

	Poor network design	Poor cryptography	Consensus	Poor architecture design	Smart contracts	Poor access management
51% Attack	✔			✔		
Balance attack			✔			
Block Discarding Attack	✔		✔			
Cache Attacks				✔		
Collapse of the decentralized			✔		✔	
DAO attack			✔		✔	
DDoS attack	✔					
Death Spiral	✔					
Double spending attack	✔					
Eclipse Attack	✔			✔		
Fork-After-Withholding	✔		✔			✔
Hijacking attack	✔			✔		
Liveness attack			✔			
Long-Range Attack				✔		
Malicious contracts					✔	
Malleability attack	✔		✔			✔
Mining malware	✔	✔				
P + Epsilon Attack			✔	✔		

	Poor network design	Poor cryptography	Consensus	Poor architecture design	Smart contracts	Poor access management
Partitioning attack	✔					
Phishing						✔
Private Key Threats		✔				
Pseudonymity	✔					
Ransomware				✔		
Re-entrance Attack					✔	
Selfish Mining Attack	✔		✔			
Spam attack	✔			✔		
Sybil Attack	✔			✔		
Tampering			✔	✔		✔
The Balance Attack	✔		✔			
Time jacking attacks	✔			✔		
Wallets injection					✔	✔

5.3 RQ3: What mechanisms of blockchain design or building exist to enhance its security?

Since the moment, the security breaches in the blockchains are revealed, there is a growing concern to provide solutions for these vulnerabilities. Through the primary studies included in this SMS there are a great multitude of proposals that seek to mitigate the vulnerabilities of the blockchain. The amount of different proposals reveal that it is an aspect still in an immature state since different proposals and solutions are offered but these proposals are not coincident between the various studies. In addition, none of the proposed solutions have been validated with real cases of use.

Solutions have been classified following the general risk classification on private blockchain implementation proposed by Hasanova *et al.* [35]. We also include solutions to public blockchain implementations in our classification as Fig. 3 shows. The criteria considered to classify each of the proposals identified in this SMS are the following:

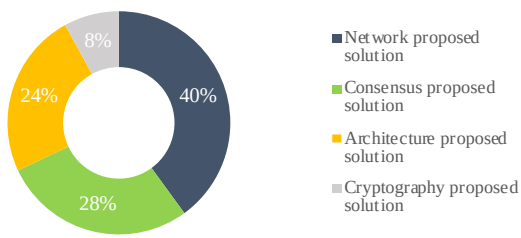

Fig. 3. Methods proposed to enhance blockchain security.

- Network proposed solution: It includes those solutions that imply a change at network level. As an example, solutions as broadcasting of messages by group or SDN controller have been included in this category.
- Architecture proposed solution: This category includes those solutions that imply a change in the design of the current architecture. As an example, solutions as implementing security switches have been included in this category.
- Consensus proposed solution: It includes all the solutions that involve changes in order to reach a consensus on a new block. As an example, a extends of the Markow Decision

Process (MDP) have been included in this category.

- Cryptography proposed solution: It includes all those solutions that propose improvements at the cryptographic level to implement the security of the blockchains. As an example, a proposal of composite signatures has been included in this category.

The distribution of each of the proposed methods to improve the security on blockchains and the appearances of each of it in the selected primary studies is shown in the table below.

Table 9. Distribution of papers per methods to enhance security.

RQ3	Reference
Architecture proposed solution	[28] [59] [64] [46] [40]
Consensus proposed solution	[55] [26] [54] [78] [48] [43] [78] [43]
Cryptography proposed solution	[70] [32]
Network proposed solution	[71] [38] [35] [14] [30] [37] [27] [65] [36] [44] [45] [56] [4] [34] [33] [31] [42] [54] [39] [49]

5.4 RQ4. At what point of maturity is the security research blockchain and how has the interest evolved over time?

This question was answered by using the classification of research approaches proposed by Wieringa *et al.* [25] as recommended in Petersen *et al.* [23]. The scheme presents the classification of non-empirical research, which contains the categories of proposal papers, evaluation papers, validation papers, philosophical papers, opinion papers and personal experience papers.

The results, shown in Fig. 4, showed that proposal (48.84%) stood out as the dominant research method. The second most common research method used was opinion (18.6%); and finally, in last place was evaluation and philosophical (14%). These data reveal a state of immaturity in the topic addressed and strengthen the importance of an in-depth study of the subject, as they have mainly been addressed theoretically but have not yet established a reliable model to test in the industry.

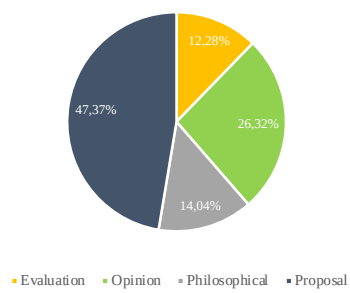

Fig. 4. Classification scheme results.

Moreover, it can be observed an exponential increase in the number of publications addressing this subject. Note that during 2020 due to the pandemic situation, the rate of publications has slowed down. This fact fits with the growing boom of applications that

have emerged based on the blockchain as well as the growing interest of society in cryptocurrencies as it is shown in Fig. 5.

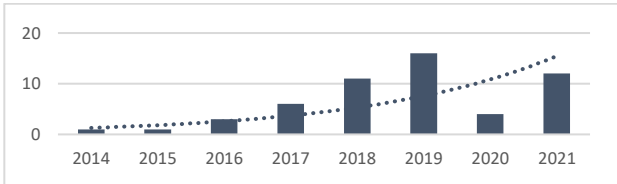

Fig. 5. Number of publications per year.

5.5 Discussion

In this paper, data collected for a systematic mapping study has allowed us to depict the current situation as regard security in blockchain technology. The increase of publication over the las five years can be explained by the increase of applications of this technology but also because numerous attacks and security vulnerabilities were recently made public.

Fig. 6 shows the combination of the most relevant attacks, the weaknesses that exploit these attacks and areas of the solutions proposed in the 56 final empirical studies. The objective of this section is to thoroughly analyze the empirical evidence on blockchain's security found in this SMS, combining some research questions with additional information extracted from the empirical studies. This figure shows that, of the 56 empirical studies analyzed:

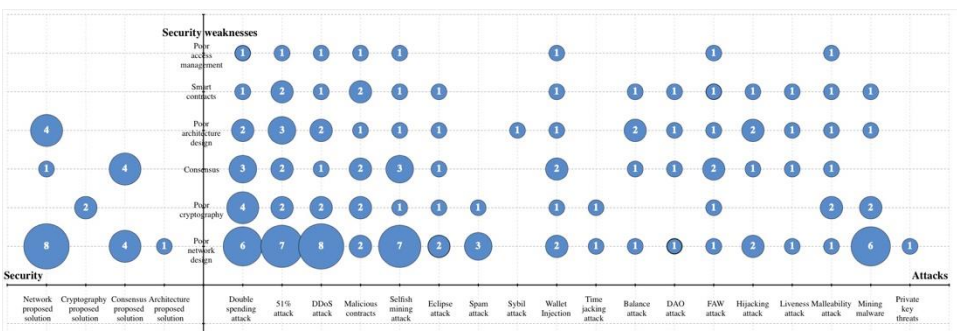

Fig. 6. Relation between investigation questions.

- On 52 instances, poor network design was identified as an issue to be addressed by identifying attacks that were exploiting this vulnerability.
- The studies that evade the weakness in the network design also identify other weaknesses closely related to the blockchain such as gaps in cryptography, the defects of the current consensus and smart contract algorithms, the inherent flaws of the actual blockchain architecture and the problems of access and identity management when editing the blockchain.
- At least 18 attacks have been identified as potential attacks by a blockchain in various studies. These attacks have already materialized and are of concern to the scientific community.

- More than 50% of the proposed solutions focus on network solutions to address attacks that exploit vulnerabilities in both network infrastructure and consensus and architecture.
- The most frequently referenced attacks throughout this SMS are the blockchain attacks, except for those involving denial of service (DDoS). Therefore, the attacks that have created more awareness are those of the blockchain such as the 51% attacks, the double spending attacks or the selfish mining attacks.

The results of this paper highlight blockchain's lack of maturity. This lack of maturity is evidenced by the lack of validations or proposals in the industry. A high percentage of the studies reviewed make proposals (47.37%) or discuss the problems identified (14.04%) and the security gaps to be addressed. However, they do not present solutions that have been validated in a real environment.

5.6 Security Model for Blockchain

Once analyzed the main security problems of blockchain, as well as the solutions proposed by the scientific community to control them, in this subsection we present a security model for blockchain. This model has the objective of relating the security concepts used and instantiating them according to the results of our SMS, improving its understanding. For the definition of this model, we have carried out an analysis of the functionalities and fundamental components of blockchain proposed by NIST [79]. In addition, we considered the main blockchain implementations spotlighting on Bitcoin [1], Ethereum [80], Hyperledger [81], as are the most consolidated technologies. We have abstracted their main components to create our architecture. A layered structure, which is common in modeling and designing blockchain systems, was employed along with security implementations, to represent the main functions and components of blockchain systems. The security model allows the implementation of a security solution through security patterns which provides implement a solution to recurring problems against a threat, or a set of threats, in a concise and reusable way [82]. Fig. 7 shows the proposed security model for blockchain.

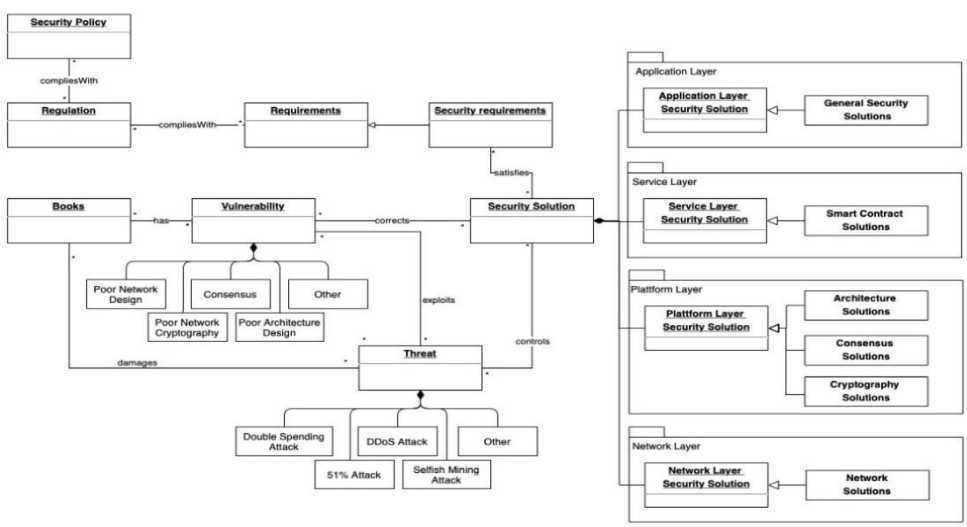

Fig. 7. Security model for blockchain.

As it can be seen, our proposal has two main parts: on one hand, the security concepts instantiated with the results of the SMS process and, on the other hand, a blockchain layer structure. In order to define our model, we have used security ontologies as basis. A security ontology is a well-known mechanism used to provide connection between security concepts. They provide useful knowledge that allows organization, communication and reusability of the represented concepts [83, 84] . Our proposal highlights the concepts of threat and vulnerability that damage and have each asset of the blockchain. Thus, the main types of threats and vulnerabilities that we have identified in our SMS process can be observed. These elements must be controlled and corrected through different security solutions, which must be implemented in the different components of the blockchain system. In addition, these security solutions must be defined by means of security requirements which must be aligned with the security policies and regulations of the context where the blockchain is implemented.

To represent the blockchain system, we have used a layer-based structure, typical of this type of system. Our proposed layer structure is based on blockchain 2.0 most popular implementations such as Ethereum [80] and Hyperledger [85, 86], as well as blockchain 1.0 implementation as Bitcoin since it can be considered as the booster of this technology [1]. In addition, during our SMS, we discovered that those are the most approached blockchain implementations by the scientific community. Hence, all these proposals have in common the use of layers to represent and group the different elements and components typical of a blockchain system. Thus, our proposal defines a structure in layers and relates them to the main security mechanisms identified previously:

- Application layer: The application layer contains functionalities for the end-user and applications built on blockchains; therefore, security threats are specific to certain types of applications. In addition, this layer includes the applications used to manage and control the blockchain. For that reason, the security mechanisms used to correct the vulnerabilities and control the threats are general purpose security solutions, such as access control or authentication methods.
- Service layer: The service layer defines blockchain's own services, such as the management of smart contracts and transactions or the interfaces to communicate with other external systems. Thus, when securing this layer, security solutions related to the secure use of smart contracts or the encryption of data, both in transit and at rest, must be considered.
- Platform layer: The entire infrastructure of the blockchain platform can be understood as a blockchain-as-a-Service (BaaS) that allows the creation and management by third parties of cloud-based networks for companies dedicated to building blockchain applications. This is beginning to be a growing trend and is one of the main reasons for separating the platform layer from the service layer. Hence, this layer represents the typical components of a blockchain system, such as the blocks or the consensus algorithms. For that reason, the security mechanisms that can be applied in this layer are related to the definition of the blockchain architecture, the decision and configuration of consensus algorithms, and the protection of the data stored in the blocks by means of cryptography solutions.
- Network layer: The network layer is the base on which the blockchain is supported. Basically, blockchains are networks that are superimposed on other networks; therefore, blockchains inherit security and privacy issues from the underlying networks. Obviously, the security mechanisms to ensure this layer must be focused on secure the communication infrastructure of the blockchain.

Finally, this security model for blockchain allows a better understanding not only of the security concepts but also the typical structure of this kind of systems. This structure can be defined in greater depth by including the main elements of each layer. However, the main objective of this model is to serve as a guide when applying the knowledge obtained after the realization of the SMS.

5.7 Security Model Application

In order to facilitate the understanding of our Security Model for Blockchain, we have developed an illustrative example which aims to show how our model can be applied to consider security in the blockchain design and implementation. In this section, we depict a Blockchain application that has the main objective of managing the books of a library. In addition, this illustrative example has a set of security aspects that must be considered. Table 10 shows a list of the different requirements that the application has to address.

To conduct our example, a library DApp has been developed. We deployed an Ethereum [80] network using Ganache [87]. Moreover, to deploy smart contracts Truffle Suite [88] has been used. Finally, smart contracts have been built in Solidity [89].

Table 10. Requirements of security model application.

ID	Type of requirement	Description
BR-1	Business requirements	Borrowed books must be traceable.
BR-2	Business requirements	A borrowed book should not be allowed to be lent.
SR-1	Security requirements	Adding new assets must be restricted to a set of accounts with explicit permission.
SR-2	Security requirements	A consensus between a minimum number of blocks must be required to authorize a transaction before it is added to the blockchain.
SR-3	Security requirements	High availability is required for the service

To meet the defined business requirements, a smart contract has been set up to manage the books. Fig. 8 depicts the code that defines the smart contract. This smart contract interacts with the blockchain, generating a new block that reflects the transaction once it has been requested and loaned to the user. As a result, we obtain the DApp shown in Fig. 9.

```
pragma solidity ^0.5.0;
contract Loan {
    address[16] public users;
    // lending book
    function lend(uint userId) public
    returns (uint) {
    require(userId >= 0 && userId <= 15);
           users[userId] = msg.sender;
           return userId;}
    // Retrieving the users
    function getusers() public view returns  (address[16]
memory) {
    return users;}
}
```

Fig. 8. Smart contract library.

Based on the security requirements, a set of threats was identified. As described in the model, these threats should be controlled or corrected by means of some security solutions. These security solutions are intended to correct possible existing vulnerabilities that could damage blockchain integrity. Table 11 shows a summary of the identified threats and the security solutions that are meant to control them. In addition, it is important to highlight that our model can be used not only to help in the definition of the security solutions, but also to identify the layer of the Blockchain application in which each security solution should be implemented.

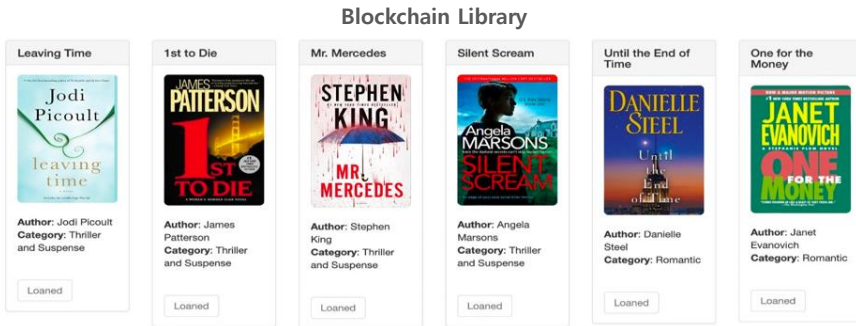

Fig. 9. Library DApp.

Based on the security requirements, a set of threats was identified. As described in the model, these threats should be controlled by means of some security solutions, which are also intended to correct the corresponding existing vulnerabilities that could damage the blockchain integrity. Table 11 shows a summary of the vulnerabilities and threats that the proposed security solutions are intended to control. Information on which layer the security solution should be applied has also been added.

Table 11. Security solutions of security model application.

ID	Threat	Security solution	Implementation
SR-1	Books or assets are added by unauthorized users	Embedded Permission Pattern [90]	Service layer
SR-2	An immutable transaction is added to the chain without enough acknowledgements performing a FAW attack	X-Confirmation Pattern [91]	Platform layer
SR-3	DDoS attack causing high availability to be not possible	Dynamic Transaction Limit Volume [49]	Network layer

The first threat to be covered describes the possibility of books or other assets being added by unauthorized users. This threat can be addressed by implementing the Embedded Permission Pattern [90] and access control techniques such as mandatory, role-based and attribute-based. To allow updating the list of authorized accounts after deploying the smart contract, additional functionality is added to enable this modification. In addition, a list of authorized addresses is added to make these modifications.

The second risk to be covered describes the possibility of a transaction being altered

due to a longer malicious fork being created taking advantage of transactions being stored without sufficient acknowledgements by performing a FAW attack. This threat can be addressed by implementing the X-Confirmation Pattern. This solution is implicit in the selected technology as Ethereum assumes the confirmation of 10-12 blocks, which is between 2.5 and 3 minutes with an inter-block time of 15-17 seconds. This solution guarantees the immutability of the transaction. It should be noted that in case it is decided to increase the number of confirmation blocks, the latency between the submission and confirmation of a transaction, once it is included in a blockchain, increases.

Finally, the third threat to be covered describes the possibility of receiving a DDoS attack, preventing the high availability requirement. to limit the attackers' chances of success, we use an age-based Mempool design, as proposed by Saad *et al.* [51]. Thus, the confirmation factor or "age" of a transaction to distinguish between benign and malicious transactions.

Fig. 10 shows the implementation of the security model in the example of the creation of the library using blockchain technology. Those components of the model that have been implemented in this example have been highlighted.

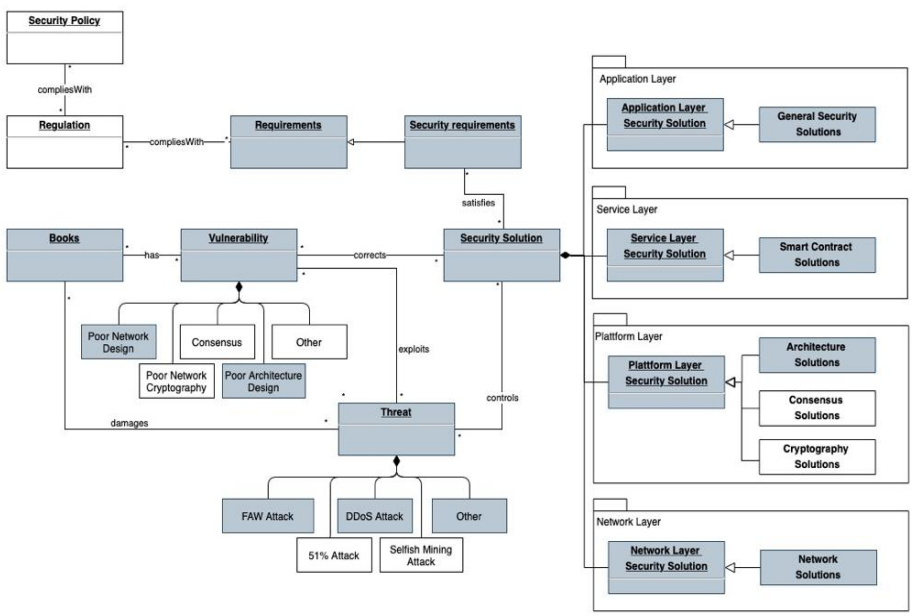

Fig. 10. Security model application.

Different security solutions have been defined in order to address the security requirements identified in the example. These solutions have been implemented at the service, platform, and network layers. The implementation of these solutions allows mitigating the existing threats in the system, specifically the FAW attack, DDoS attack and transaction immutability. The mitigation of these threats also allows us to correct known vulnerabilities in our blockchain system.

The security model allows us to easily identify the security requirements that need to be addressed and incorporate them into the blockchain system from the design phase,

considering known threats and vulnerabilities in the blockchain system, such as, specific to the blockchain system to be developed. Likewise, the implementation of security solutions using security patterns allows us to implement a solution in a simple, effective, and reusable way.

6. CONCLUSIONS AND FUTURE WORK

We focus on the security issues on blockchain technologies through this study. We conduct a systematic mapping review on the relevant attacks on blockchains and the vulnerabilities that made those attacks possible. Existing proposals to mitigate the risk of such attacks have also been investigated in a rigorous and systematic way.

Data gathered have allowed us to describe the present situation regarding published studies, thus revealing that the number of publications in this field increase every year. Considering that we cannot find recent publications – the increase comes from the last 8 years – as well as the lack of validations in the industry, we can affirm that although blockchain technology has been consolidating, security is still in a rather immature state and there are some gaps to deal with.

This SMS reveals that as blockchain have unique security features, they also have unique vulnerabilities making it particularly attractive to attackers because fraudulent transactions cannot be reversed as in the traditional financial system. It reinforces the need for this study and opens new future working lines.

Based on the results obtained, we propose a first approach for a security model for blockchain that relates the concepts of security and the main threats, vulnerabilities and possible solutions according to the results. In addition, an application scenario of the model has been presented. Furthermore, this model includes a layer structure that has been defined to represent the main functionalities and components of a blockchain system. This structure is intended to be the basis for the definition of a security reference architecture that contributes to a better understanding of the blockchain systems and, at the same time, incorporates the security aspects, following the security-by-design paradigm. As future work we intend to develop a complete reference architecture and incorporate the application of different security patterns to facilitate the implementation of security mechanisms. Furthermore, we intend to validate this proposal by means of a case study.

ACKNOWLEDGMENTS

This work has been funded by the AETHER-UCLM: A smart data holistic approach for context-aware data analytics focused on Quality and Security project (Ministerio de Ciencia e Innovación, PID2020-112540RB-C42) and the GENESIS project (SBPLY-17-180501-000202 funded by “Consejería de Educación, Cultura y Deportes de la Dirección General de Universidades, Investigación e Innovación de la JCCM”) and the Programa Operativo Regional FEDER 2014/2020.

REFERENCES

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf, 2008.
2. P. S. G. A. Sri and D. L. Bhaskari, "A study on blockchain technology," *International Journal of Engineering and Technology*, Vol. 7, 2018, pp. 418-421.
3. A. Tandulwadikar, "Blockchain in banking: A measured approach," *Cognizant Reports*, NJ, 2016.
4. J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *Proceedings of IEEE Middle East and North Africa Communications Conference*, 2018, pp. 1-6.
5. Ciphertrace, "Q1 2019 cryptocurrency anti-money laundering report," https://thenextweb.com/hardfork/2019/05/01/cryptocurrency-stolen-first-quarter-2019-hack/, 2019.
6. J. A. Lanz, "Electrum attack," https://ethereumworldnews.com/electrum-wallet-suffers-a-new-attack-losses-are-calculated-in-millions-of-dollars/, 2019.
7. Ciphertrace, "Half of 2020 crypto hacks are from DeFi protocols and exchanges," Ciphertrace, https://ciphertrace.com/half-of-2020-crypto-hacks-are-from-defi-protocols-and-exchanges/.
8. P. S. G. A. Sri and D. L. Bhaskari, "A study on blockchain technology," *International Journal of Engineering and Technology*, Vol. 7, 2018, pp. 418-421.
9. L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, Vol. 4, 1982, pp. 382-401.
10. P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, Vol. 80, 2007, pp. 571-583.
11. K. Jonathan and A. K. Sari, "Security issues and vulnerabilities on a blockchain system: A review," in *Proceedings of International Seminar on Research of Information Technology and Intelligent Systems*, 2019, pp. 228-232.
12. A. Averin and O. Averina, "Review of blockchain technology vulnerabilities and blockchain-system attacks," in *Proceedings of International Multi-Conference on Industrial Engineering and Modern Technologies*, 2019, pp. 1-6.
13. M. K. Shrivas, T. Y. Dean, and S. S. Brunda, "The disruptive blockchain security threats and threat categorization," in *Proceedings of the 1st International Conference on Power, Control and Computing Technologies*, 2020, pp. 327-338.
14. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, Vol. 107, 2017, pp. 841-853.
15. T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *Proceedings of International Conference on System Science and Engineering*, 2019, pp. 362-367.
16. N. Anita and M. Vijayalakshmi, "Blockchain security attack: A brief survey," in *Proceedings of the 10th International Conference on Computing, Communication and Networking Technologies*, 2019, pp. 1-6.
17. S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *Proceedings of International Conference on Computer and Information Sciences*, 2019, pp. 1-6.

18. X. Zheng, Y. Zhu, and X. Si, "A survey on challenges and progresses in blockchain technologies: A performance and security perspective," *Applied Sciences*, Vol. 9, 2019, p. 4731.
19. N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (sok)," in *Proceedings of International Conference on Principles of Security and Trust*, 2017, pp. 164-186.
20. E. Leka, B. Selimi, and L. Lamani, "Systematic literature review of blockchain applications: Smart contracts," in *Proceedings of International Conference on Information Technologies*, 2019, pp. 1-3.
21. H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on Ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Computing Surveys*, Vol. 53, 2020, pp. 1-43.
22. J. Cheng, L. Xie, X. Tang, N. Xiong, and B. Liu, "A survey of security threats and defense on blockchain," *Multimedia Tools and Applications*, Vol. 80, 2021, pp. 30623-30652.
23. K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Information and Software Technology*, Vol. 64, 2015, pp. 1-18.
24. B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," EBSE Technical Report, No. EBSE-2007-01, 2007.
25. R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: a proposal and a discussion," *Requirements Engineering*, Vol. 11, 2006, pp. 102-107.
26. A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 3-16.
27. S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, Vol. 9, 2019, p. 1788.
28. B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts," in *Proceedings of IFIP International Conference on Autonomous Infrastructure, Management and Security*, 2017, pp. 16-29.
29. U. W. Chohan, "The double spending problem and cryptocurrencies," *SSRN Electronic Journal*, 2017, No. ssrn.3090174.
30. T. P. Keenan, "Alice in blockchains: Surprising security pitfalls in pow and pos blockchain systems," in *Proceedings of the 15th Annual Conference on Privacy, Security and Trust*, 2018, pp. 400-402.
31. O. Boireau, "Securing the blockchain against hackers," *Network Security*, Vol. 2018, 2018, pp. 1-2.
32. K. Ikeda, "Security and privacy of blockchain and quantum computation," *Advanced Computers*, Vol. 111, 2018, pp. 199-228.
33. I. Kabashkin, "Risk modelling of blockchain ecosystem," in *Proceedings of International Conference on Network and System Security*, 2017, pp. 59-70.
34. G. Morganti, E. Schiavone, and A. Bondavalli, "Risk assessment of blockchain technology," in *Proceedings of the 8th Latin-American Symposium on Dependable Computing*, 2018, pp. 87-96.

35. H. Hasanova, U. Baek, M. Shin, K. Cho, and M.-S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *International Journal of Network Management*, Vol. 29, 2019, p. e2060.
36. S. Sayadi, S. B. Rejeb, and Z. Choukair, "Blockchain challenges and security schemes: A survey," in *Proceedings of the 7th International Conference on Communications and Networking*, 2018, pp. 1-7.
37. C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51%-attack detecting," in *Proceedings of the 5th International Conference on Dependable Systems and Their Applications*, 2018, pp. 15-24.
38. A. Soni and S. Maheshwari, "A survey of attacks on the bitcoin system," in *Proceedings of IEEE International Students' Conference on Electrical, Electronics and Computer Science*, 2018, pp. 1-5.
39. X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information," in *Proceedings of IEEE International Conference on Blockchain*, 2019, pp. 261-265.
40. O. Oksiiuk and I. Dmyrieva, "Security and privacy issues of blockchain technology," in *Proceedings of IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering*, 2020, pp. 1-5.
41. S. Muralidhara and B. Usha, "Review of blockchain security and privacy," in P*roceedings of the 5th International Conference on Computing Methodologies and Communication*, 2021, pp. 526-533.
42. D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2017, pp. 458-467.
43. S. Feng, J. He, and M. X. Cheng, "Security analysis of block withholding attacks in blockchain," in *Proceedings of IEEE International Conference on Communications*, 2021, pp. 1-6.
44. S. Roy, F. J. A. Morais, M. Salimitari, and M. Chatterjee, "Cache attacks on blockchain based information centric networks: an experimental evaluation," in *Proceedings of the 20th International Conference on Distributed Computing and Networking*, 2019, pp. 134-142.
45. I. S. Mehta, A. Chakraborty, T. Choudhury, and M. Sharma, "Efficient approach towards bitcoin security algorithm," in *Proceedings of International Conference on Infocom Technologies and Unmanned Systems: Trends and Future Directions*, 2018, Vol. 2018, pp. 807-810.
46. M. Tiloca, C. Gehrmann, and L. Seitz, "On improving resistance to Denial of Service and key provisioning scalability of the DTLS handshake," *International Journal of Information Security*, Vol. 16, 2017, pp. 173-193.
47. S. H. Shaheen and M. Yousaf, "Security analysis of dtls structure and its application to secure multicast communication," in *Proceedings of the 12th International Conference on Frontiers of Information Technology*, 2014, pp. 165-169.
48. A. Gruhler, B. Rodrigues, and B. Stiller, "A reputation scheme for a blockchain-based network cooperative defense," in *Proceedings of IFIP/IEEE Symposium on Integrated Network and Service Management*, 2019, pp. 71-79.

49. M. Saad, J. Kim, D. Nyang, and D. Mohaisen, "Contra-∗: Mechanisms for countering spam attacks on blockchain's memory pools," *Journal of Network and Computer Applications*, Vol. 179, 2021, p. 102971.
50. H. Lee, M. Shin, K. S. Kim, Y. Kang, and J. Kim, "Recipient-oriented transaction for preventing double spending attacks in private blockchain," in *Proceedings of the 15th Annual IEEE International Conference on Sensing, Communication, and Networking*, 2018, pp. 1-2.
51. N. A. Alabdali, M. A. AlZain, M. Masud, J. Al-Amri, and M. Baz, "Bitcoin and double-spending: How paving the way for betterment leads to exploitation," *Indian Journal of Computer Science and Engineering*, Vol. 11, 2020, pp. 81-88
52. Z. Xing and Z. Chen, "A protecting mechanism against double spending attack in blockchain systems," in *Proceedings of IEEE World AI IoT Congress*, 2021, pp. 0391-0396.
53. S.-Y. Chang and Y. Park, "Silent timestamping for blockchain mining pool security," in *Proceedings of International Conference on Computing, Networking and Communications*, 2019, pp. 1-5.
54. S. Jeon, I. Doh, and K. Chae, "RMBC: Randomized mesh blockchain using DBFT consensus algorithm," in *Proceedings of International Conference on Information Networking*, Vol. 2018, 2018, pp. 712-717.
55. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proceedings of IEEE International Conference on Consumer Electronics*, 2016, pp. 467-468.
56. J. Moubarak, M. Chamoun, and E. Filiol, "Hiding malware on distributed storage," in *Proceedings of IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology*, 2019, pp. 720-725.
57. B. D. C. Putri and R. F. Sari, "The effect of latency on selfish-miner attack on block receive time bitcoin network using NS3," in *Proceedings of the 12th International Conference on Telecommunication Systems, Services, and Applications*, 2018, pp. 1-5.
58. P. D'Arco and Z. E. Ansaroudi, "Security attacks on multi-stage proof-of-work," in *Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events*, 2021, pp. 698-703.
59. T. K. Kim, "Analysis of spam transaction on the blockchain," *International Journal of Engineering and Technology*, Vol. 7, 2018, pp. 551-553.
60. M. Steichen, S. Hommes, and R. State, "ChainGuard-A firewall for blockchain applications using SDN with OpenFlow," in *Proceedings of International Conference on Principles, Systems and Applications of IP Telecommunications*, Vol. 2017, 2017, pp. 1-8.
61. J. R. Douceur, "The sybil attack," in *Proceedings of International Workshop on Peer-to-Peer Systems*, 2002, pp. 251-260.
62. A.-M. Kermarrec and M. van Steen, "Gossiping in distributed systems," *ACM SIGOPS Operating Systems Review*, Vol. 41, 2007, pp. 2-7.
63. D. Modinger, H. Kopp, F. Kargl, and F. J. Hauck, "A flexible network approach to privacy of blockchain transactions," in *Proceedings of International Conference on Distributed Computing Systems*, Vol. 2018, 2018, pp. 1486-1491.
64. K. Lee and A. Miller, "Authenticated data structures for privacy-preserving Monero light clients," in *Proceedings of the 3rd IEEE European Symposium on Security and Privacy Workshops*, 2018, pp. 20-28.

65. R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security & Privacy*, Vol. 16, 2018, pp. 38-45.
66. M. Saad, L. Njilla, C. Kamhoua, and A. Mohaisen, "Countering selfish mining in blockchains," in *Proceedings of International Conference on Computing, Networking and Communications*, 2019, pp. 360-364.
67. N. Zivic, C. Ruland, and O. Ur-Rehman, "Addressing Byzantine fault tolerance in blockchain technology," in *Proceedings of the 8th International Conference on Modeling Simulation and Applied Optimization*, 2019, pp. 1-5.
68. J. O. Chervinski, D. Kreutz, and J. Yu, "Analysis of transaction flooding attacks against Monero," in *Proceedings of IEEE International Conference on Blockchain and Cryptocurrency*, 2021, pp. 1-8.
69. H. M. Varghese, D. A. Nagoree, N. Jayapandian, *et al*., "Cryptocurrency security and privacy issues: A research perspective," in *Proceedings of the 6th International Conference on Communication and Electronics Systems*, 2021, pp. 902-907.
70. A. Saxena, J. Misra, and A. Dhar, "Increasing anonymity in bitcoin," in *Proceedings of International Conference on Financial Cryptography and Data Security*, 2014, pp. 122-139.
71. Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, Vol. 126, 2019, pp. 45-58.
72. K. Otsuki, R. Nakamura, and K. Shudo, "Impact of saving attacks on blockchain consensus," *IEEE Access*, Vol. 9, 2021, pp. 133011-133022.
73. J. Zheng, H. Huang, C. Li, Z. Zheng, and S. Guo, "Revisiting double-spending attacks on the bitcoin blockchain: New findings," in *Proceedings of IEEE/ACM 29th International Symposium on Quality of Service*, 2021, pp. 1-6.
74. E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *Proceedings of International Conference on Financial Cryptography and Data Security*, 2016, pp. 43-60.
75. S. Banupriya and K. Kottilingam, "An analysis of privacy issues and solutions in public blockchain (bitcoin)," in *Proceedings of the 2nd International Conference for Emerging Technology*, 2021, pp. 1-7.
76. P. Praitheeshan, L. Pan, and R. Doss, "Security evaluation of smart contract-based on-chain Ethereum wallets," in *Proceedings of International Conference on Network and System Security*, 2020, pp. 22-41.
77. L. Su, *et al.*, "Evil under the sun: Understanding and discovering attacks on Ethereum decentralized applications," in *Proceedings of the 30th USENIX Security Symposium*, 2021, pp. 1307-1324.
78. F. A. AlShlawi, N. K. AlSa'awi, W. Y. B. Saleem, and A. Ara, "DUST-MASK: A framework for preventing bitcoin's dust attacks," in *Proceedings of the 3rd International Conference on Computer Applications and Information Security*, 2020, pp. 1-6.
79. D. Yaga, P. Mell, N. Roby, and K. Scarfone, "NISTIR 8202 blockchain technology overview," https://csrc.nist.gov/publications/detail/nistir/8202/final, 2018.
80. "Enterprise Ethereum alliance client specification v6," https://entethalliance.github.io/client-spec/spec.html, 2020.
81. "Hyperledger fabric architecture reference," https://hyperledger-fabric.readthedocs.io/en/release-1.3/architecture.html.

82. E. Fernandez-Buglioni, *Security Patterns in Practice: Designing Secure Architectures using Software Patterns*, John Wiley & Sons, UK, 2013.
83. C. Blanco, J. Lasheras, R. Valencia-García, E. Fernández-Medina, A. Toval, and M. Piattini, "A systematic review and comparison of security ontologies," in *Proceedings of the 3rd International Conference on Availability, Reliability and Security*, 2008, pp. 813-820.
84. I. Meriah and L. B. A. Rabai, "Comparative study of ontologies based ISO 27000 series security standards," *Procedia Computer Science*, Vol. 160, 2019, pp. 85-92.
85. T. Blummer, M. Sean, and C. Cachin, "An introduction to hyperledger," Technical Report, https://www. hyperledger.org/wp-content/uploads/2018, 2018.
86. H. A. W. Group, *et al*., *Hyperledger Architecture Volume 1: Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus*, Hyperledger Org, 2017.
87. Truffle Suite, "Ganache," https://www.trufflesuite.com/docs/ganache/overview.
88. Truffle, "Truffle suite," https://www.trufflesuite.com.
89. Solidity, "Solidity," https://solidity-es.readthedocs.io/.
90. CSIRO, "Blockchain patterns: embedded-permission," https://research.csiro.au/blockchainpatterns/general-patterns/contract-structural-patterns/embedded-permission/.
91. CSIRO, "Blockchain patterns: X-confirmation pattern," https://research.csiro.au/blockchainpatterns/general-patterns/security-patterns/x-confirmation/.

María I. Ortega is currently working in the security incident response team of Telefónica. She has a master's degree in Computer Science from the University of Castilla-La Mancha. Her research interests include security, vulnerability management and blockchain ecosystems.

Julio Moreno received a Ph.D. degree in Computer Science from the University of Castilla-La Mancha. His research interests include data security and privacy and security architectures for big data ecosystems.

Manuel A. Serrano received a Ph.D. degree in Computer Science from the University of Castilla-La Mancha. He is an Associate Professor at the Escuela Superior de Informatica of the University of Castilla-La Mancha in Ciudad Real. His research interests are focused on cyber-security, especially on big data and IoT, software quality and measurement and business intelligence. His scientific production is large, having published more than fifty articles in high level journals and conferences. He has participated in more than 20 research projects, has made several presentations and has worked on several transfer projects with companies.

Eduardo Fernández-Medina has a Ph.D. from the University of Castilla-La Mancha. He is a Full Professor at the School of Computer Science of the University of Castilla-La Mancha in Ciudad Real (Spain), and his research activity is in the field of security in information systems, and in particular, security in big data, cloud computing and cyberphysical systems. He is the author of more than sixty papers in international journals. He directs the GSyA research group at the Department of Computer Science of the University of Castilla-La Mancha, in Ciudad Real, Spain, and belongs to several professional and research associations (ATI, AEC, AENOR, *etc.*).