Blockchain Security in the Internet of Things: Literature Review

Joyce Quintino, Carina T. de Oliveira, Rossana M. C. Andrade

Blockchain Security in the Internet of Things: Literature Review

Joyce Quintino[1], Carina T. de Oliveira[2], and Rossana M. C. Andrade[1]*

[1] Federal University of Ceara - UFC - Fortaleza, Ceara, Brazil
joycequintinoalves@alu.ufc.br, rossana@ufc.br
[2] Federal Institute of Ceara - IFCE - Fortaleza, Ceara, Brazil
carina@lar.ifce.edu.br

Abstract

The Internet of Things (IoT) allows different devices in our daily routines, such as refrigerators, light bulbs and autonomous cars, to be part of the Internet. Accordingly, the amount of data circulating in the network increases. Thus, a secure and reliable IoT environment becomes essential to avoid security vulnerabilities. In IoT, resources are limited and existing security solutions used in the traditional Internet can be ineffective, making data security still a challenge. In this scenario, Blockchain emerges as a promising technology to improve security in IoT, as it enables the recording of data in a decentralized, encrypted and immutable way with the consensus of the network participants in a packet data structure called a block. In Blockchain, the consensus is a protocol responsible for maintaining the state of the network and allowing the addition of new blocks with data. However, many consensus protocols require high computational power and power consumption to solve the mathematical problems that make possible data records in the blocks. Since many devices have low processing power in the IoT environment, developing new consensus approaches is needed to use Blockchain in IoT effectively. Therefore, this paper presents the results of a literature review about the use of Blockchain technology, specifically consensus protocol approaches, in IoT security.

Keywords: Internet of Things; Security; Blockchain; Consensus Protocols.

1 Introduction

The Internet of Things (IoT) is a network of objects and embedded devices connected to the Internet [6]. IoT connects devices of our everyday life, such as refrigerators, light bulbs, wearables devices and autonomous cars, through the Internet. According to [3], the number of these devices will reach about 25 billion by 2025. Data that comes from IoT devices can be useful, for example, to connect patients to doctors, enable more efficient farming, aid decision-making in smart environments, optimize the industrial sector, and contribute to economic growth. So, the IoT has significant benefits that contribute to society.

On the other hand, as the amount of connected devices increases, so does the amount of data traversing the network and, thus, a secure and reliable IoT environment becomes essential to avoid security vulnerabilities [1]. However, the limitations of IoT devices in computing power, storage, and power consumption hinder the development of a secure IoT. Existing security solutions used in the traditional Internet can be ineffective [5]. In this way, IoT devices are subject to several security threats, considering generic vulnerabilities for Internet-connected devices and specific threats inherent to the technology of these devices [9].

In this scenario, Blockchain emerges as a promising technology to improve security in IoT, as it enables the recording of data in a decentralized, encrypted and immutable way with the consensus of network participants in a packet data structure called block [2]. Considering that many devices have low processing power in the IoT environment, there is a need to develop new approaches to consensus protocols, as the current versions are not suitable for IoT due to the high processing power required [7].

This paper presents the results of a literature review for using Blockchain technology, specifically consensus protocol approaches, to improve the Internet of Things security. We hope to bring to the community the state of the art about consensus protocols, the low-cost consensus approaches, applications and mechanisms, which have been developed to improve security in IoT environment, as well as the most frequent attacks related to Blockchain consensus, where consensus solutions are applied, and what tools are used for Blockchain simulations, development, and testing.

*CNPq's Productivity Scholarship in Technological Development and Innovative Extension - DT - Level 1D

2 Literature Review

Our literature review follows the precepts of a systematic mapping [4] and the PICOC (Population, Intervention, Comparison, Outcome, and Context) structure, which is a conceptual model to support the research questions [10]. Furthermore, the Parsif.al[1] tool was used to document the review process.

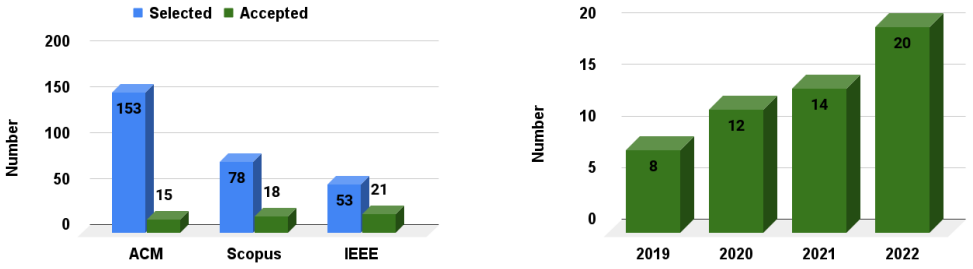
We selected three well-known digital libraries to find the relevant papers for this research: ACM Digital Library[2], Scopus[3] and IEEE Xplore[4]. In the research for the most relevant papers published in recent years, this review considered papers published from 2019 to October 2022. To find the papers that are part of this review, a search string was formulated and can be viewed on the github repository[5]. We defined five research questions (RQ) to address in the literature review that are presented in Section 3.

The selection process of the papers was initiated considering the defined inclusion and exclusion criteria. The inclusion criterias are papers about low-cost consensus used to improve security in blockchain-based IoT and english papers. The exclusion criterias are extended abstracts, unrelated papers about low-cost consensus used to improve security in blockchain-based IoT, secondary studies (surveys and systematic mappings) and papers published before 2019. Also, others two filters were considered to improve the selection of the papers. The first filter involves reading the papers' titles, abstracts, and keywords. The second filter is the complete reading of the papers to fill in the form with the research questions.

3 Results

Figure 1(a) shows the total number of papers selected from each base and the number of papers accepted at the end of the selection process. It is noticeable that most of the accepted papers are from IEEE Xplore. With the support of the Parsif.al tool, 35 duplicates papers were identified. As a way to validate the 35 duplicates, the titles of each paper were checked. After the duplicates were removed, 249 papers remained, which went through the remaining stages of the review. After the selection phases, 195 papers were rejected, and 54 were accepted.

Figure 1(b) presents the distribution of the accepted papers per year. Among the 54 accepted papers, 8 papers were published in 2019, 12 papers in 2020, 14 papers in 2021, and 20 papers in 2022. This result shows a growth in the number of publications in recent years on low-cost consensus protocols for improving the security of the Blockchain-based Internet of Things.



(a) By base

(b) By year

Figure 1: Number of accepted papers.

RQ1 - What are the approaches/applications or low-cost consensus algorithm/protocol mechanisms for improving security in the Blockchain-based Internet of Things? We categorized the research according to the focus of the paper's proposal. The categories defined are application, mechanism, or approach. The application category in this work means using a consensus protocol already known in the literature to test its performance or compare it with others in the IoT context. Mechanism represents new proposed consensus

[1] https://parsif.al/
[2] https://dl.acm.org/
[3] https://www.scopus.com/
[4] https://ieeexplore.ieee.org/Xplore/home.jsp
[5] https://github.com/JoyceQuintino/masterResearch/blob/literaturereview/searchstring

protocols. Finally, the approach represents a solution based on some consensus protocol modified for IoT. Among the 54 selected, 33 papers were classified as mechanisms, 16 were classified as approaches, and 5 were classified as applications. Figure 2(a) shows the number of approaches, applications, and mechanisms.

RQ2 - What is the main focus of the low-cost consensus approach/mechanism/application? Some consensus solutions found are aimed at integrity, authenticity, and access control. According to [8], integrity is defined as the property in which information has not been altered unauthorizedly. Authenticity is defined as the property of being genuine and capable of being verified and trusted. Access control is limiting and controlling access to systems and applications through links. According to our research, it was observed that 6 of the papers focus on Authenticity, 4 papers on Access Control, and 1 on Integrity. Also, 43 papers have this diversified response and were classified as Others. Figure 2(b) represents the division of the categories by solution focus. This part of the study shows a trend in research toward authenticity focused solutions.

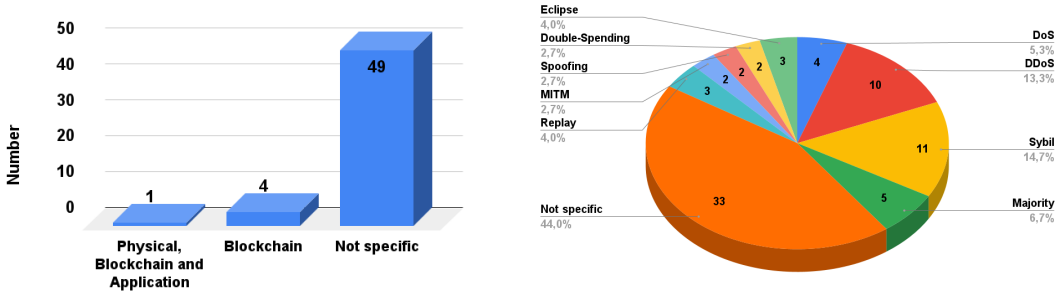
(a) Applications, approaches, and mechanisms

(b) Main focus of the solutions

Figure 2: Research Questions RQ1 and RQ2.

RQ3 - What level/layer is the low-cost consensus solution applied? This question identifies at which level/layer the consensus solution is applied. The results show that only 4 specified the layer. More specifically, 1 of the solutions applied at 3 different layers (Physical, Blockchain, and Application), and 4 papers focused on the Blockchain layer. The remaining 49 papers did not specify which layer they suit. Figure 3(a) shows how many papers have specified the layer.

RQ4 - What are the attacks associated with blockchain consensus? The results show that 21 papers cited one or more types of attacks, while 33 cited no types of attacks at all. The most frequent attacks are Denial of Service (DoS), Distributed Denial of Service (DDoS), Sybil, Majority Attack (*Majority*, also known as 51% Attack), Eclipse, Double-spending, Spoofing, Replay, and Man in the Middle (MITM). Twenty-one papers have mostly cited DDoS and *Sybil* attacks. In the future, a study based on these two types of attacks can be conducted to determine how they affect Blockchain-based IoT security. Figure 3(b) shows the frequency of the mentioned attacks.



(a) Level/layer of the low-cost consensus solution

(b) Frequency and types of attacks

Figure 3: Research Questions RQ3 and RQ4.

RQ5 - What are the tools used? It was observed that some of the papers used tools to test, implement, and validate the solution. Among the 54 accepted papers, 25 papers used one or more tools. To facilitate the presentation of the tools, we have grouped them according to their context of use. The tools are grouped into the following categories: blockchain platforms, simulators, Integrated Development Environment (IDE), software testing, network testing, and browser extension. Table 1 shows the classification of the tools according to these categories.

Category	**Tools**
Blockchain Platforms	Ethereum, Hyperledger Fabri, Hyperledger Sawtooth and Ganache
Simulators	NS-3, NS-2 and TeraSim
IDE	Remix IDE online
Software Testing	HPE LoadRunner and Caliper
Network Testing	Fabric test blockchain
Browser extension	Metamask

Table 1: Tools categories.

4 Final Remarks

The results of this literature review suggest that new consensus solutions should be developed to run on low-processing IoT devices. Another recommendation is to study how new consensus solutions can prevent Sybil and DDoS attacks to avoid future vulnerabilities. For future work, we intend to study how the consensus solutions proposed by the selected papers improve the IoT security, and to identify which methodologies are used for developing consensus protocols.

References

[1] Muhammad Ahmad, Qaiser Riaz, Muhammad Zeeshan, Hasan Tahir, Syed Ali Haider, and Muhammad Safeer Khan. Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using unsw-nb15 data-set. *EURASIP Journal on Wireless Communications and Networking*, 2021.

[2] Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari, and Yue Cao. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access*, 9, 2021.

[3] Yulin Fan, Yang Li, Mengqi Zhan, Huajun Cui, and Yan Zhang. Iotdefender: A federated transfer learning intrusion detection framework for 5g iot. In *IEEE International Conference on Big Data Science and Engineering (BigDataSE)*, 2020.

[4] Barbara Kitchenham and Pearl Brereton. A systematic review of systematic review process research in software engineering. *Information and Software Technology*, 55(12), 2013.

[5] Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, and Wei Ni. Anatomy of threats to the internet of things. *IEEE Communications Surveys & Tutorials*, 21(2), 2019.

[6] Roberto Minerva, Abyi Biru, and Domenico Rotondi. Towards a definition of the internet of things (iot). *IEEE Internet Initiative*, 1(1), 2015.

[7] Arshdeep Singh, Gulshan Kumar, Rahul Saha, Mauro Conti, Mamoun Alazab, and Reji Thomas. A survey and taxonomy of consensus protocols for blockchains. *Journal of Systems Architecture*, 127, 2022.

[8] William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson, 2015.

[9] Nazar Waheed, Xiangjian He, Muhammad Ikram, Muhammad Usman, Saad Sajid Hashmi, and Muhammad Usman. Security and privacy in iot using machine learning and blockchain: Threats and countermeasures. *ACM Computing Surveys*, 53(6), 2020.

[10] Claes Wohlin, Per Runeson, Martin Höst, Magnus C. Ohlsson, Björn Regnell, and Anders Wesslén. *Experimentation in Software Engineering*. Springer, 2012.