Applied Information Technology And Computer Science Vol. 5 No. 1 (2024) 1360-1382

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

Blockchain untuk Keselamatan dan Privasi: Sorotan Literatur Bersistematik

Blockchain for Security and Privacy: A Systematic Literature Review

Noraini Mohd Banua[1]*, Quah Wei Boon[2,3]

[1]**College of Arts and Science, School of Computing,**
Universiti Utara Malaysia, Sintok, 06010 Bukit Kayu Hitam, Kedah, MALAYSIA

[2]**Faculty od Educational Studies,**
Universiti Putra Malaysia, Jalan Universiti 1, 43400 Serdang, Selangor, MALAYSIA

[3]**Human Resource Management Division,**
Kementerian Pendidikan Tinggi, Aras 14 & 15, No. 2, Menara 2, Jalan P5/6, Presint 5, 62200 W.P. Putrajaya, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2024.05.01.078
Received 01 July 2024; Accepted 15 August 2024; Available online 30 August 2024

Abstrak: *Blockchain* adalah teknologi canggih yang telah mendapat perhatian disebabkan kemampuannya untuk mencapai keselamatan dan privasi melalui desentralisasi. Walaupun ia menyediakan keselamatan untuk persekitaran rangkaian yang tidak dipercayai, ia juga menghadapi cabaran dalam keselamatan dan privasi. Oleh itu, objektif kajian literatur sistematik ini adalah untuk menilai secara kritis literatur sedia ada mengenai teknologi blockchain untuk keselamatan dan privasi. Kajian ini menggunakan protokol kajian PRISMA. Dua pangkalan data utama, Scopus dan IEEE, telah digunakan. Dapatan menunjukkan bahawa terdapat 20 kertas penyelidikan mengenai keselamatan dan privasi dalam teknologi blockchain yang diterbitkan antara tahun 2020 dan 2023 dan melibatkan 13 jurnal berbeza. Terdapat 13 bidang aplikasi yang berbeza yang berkaitan dengan aspek keselamatan dan privasi teknologi *blockchain*, di mana *Internet of Things* menuntut bahagian terbesar daripada perwakilan. Analisis tematik mengenal pasti tujuh tema utama berkaitan dengan cabaran dalam keselamatan dan privasi teknologi *blockchain*. Dapatan juga menekankan bahawa keselamatan dan privasi adalah di antara bidang kerja masa depan yang perlu diberi tumpuan dalam teknologi *blockchain*. Kesimpulannya, artikel ini mencadangkan bahawa integrasi teknologi *blockchain dengan Internet of Things* boleh meningkatkan keselamatan dan mencadangkan pembangunan rangka kerja yang menguatkuasakan privasi dalam teknologi *blockchain.*

Kata kunci: *Blockchain*, Keselamatan, Privasi, *Internet of Things*

**Corresponding author: norainimb29@gmail.com*

Abstract*: Blockchain is a cutting-edge technology that has gained attention due to its ability to achieve security and privacy through decentralization. While it provides security for an untrusted network environment, it also faces challenges in security and privacy. Therefore, the objective of this systematic literature review is to critically evaluate the existing literature on blockchain technology for security and privacy. This study utilized the PRISMA review protocol. Two main databases, Scopus and IEEE, were used. Findings show that 20 research papers on security and privacy in blockchain were published between 2020 and 2023 and involved 13 different journals. There are 13 various application areas that are relevant to the security and privacy aspects of blockchain, where the Internet of Things claims the largest portion of representation. The thematic analysis identified seven main themes related to challenges in blockchain security and privacy. The findings also highlight that security and privacy are among the future works that should be focused on in blockchain technology. In conclusion, the article suggests that the integration of blockchain with IoT can improve security and proposes the development of a framework that enforces privacy on the blockchain.*

Keywords*: Blockchain, Security, Privacy, Internet of Things*

1. Introduction

Blockchain technology is a decentralized and shared ledger that combines blocks of data into linked lists in chronological order [1]. It has the potential to establish reliable trust among parties that lack mutual trust, and it can share credible data and achieve value transmission via Peer-to-Peer (P2P) without trusted third-party participants [2]. Blockchain integrates the P2P network, distributed data storage, encryption algorithm, a consensus mechanism for agreement, and smart contract functionality [1]. Therefore, blockchain has the characteristics of decentralization, tamper-proof, and traceability, and can effectively solve the trust problem among many participating parties.

Blockchain is an interdisciplinary technology that has gained attention from both academic communities and the industry [3]. In addition to being used in cryptocurrency, blockchain has also been applied to various fields such as the Internet of Things (IoT), finance, e-commerce, education, smart cities and smart homes, and healthcare. The security and privacy of blockchain are some of the reasons why it has become a research hot topic. However, with the development of blockchain technology, the issues of security and privacy are becoming more prominent and require attention. Researchers have identified various challenges faced by blockchain security and privacy, such as scalability, interoperability, and privacy protection [4]. At the same time, they have also explored potential solutions, including advanced cryptography, permissioned blockchains, and privacy-preserving mechanisms [5].

Recent literature has emphasized the significance of blockchain security and privacy across diverse applications, including supply chain management, digital identity verification, and energy systems [6]. Overall, blockchain technology offers significant advantages in terms of security and privacy, but also presents new challenges. The research community is actively exploring solutions to these challenges, and there is still much to be done to ensure the secure and private use of blockchain in a variety of applications.

1.1 Research Questions

Blockchain technology has been recognized for its potential to provide a secure and trustworthy platform for various applications. Distributed ledger technology can enhance security and privacy by providing an immutable and transparent record of transactions. However, the adoption of blockchain

technology has also raised concerns about the security and privacy of data, as well as the scalability and interoperability of blockchain systems.

The following research questions are addressed in this study:

i. How many research papers have been produced focusing on security and privacy in blockchain between 2020 and 2023, and in which journals where they published?
ii. What areas of blockchain are the focus of research in terms of security and privacy?
iii. What are the differences between each research study?
iv. What are the challenges of security and privacy in blockchain?
v. What are the future works concerning security and privacy in blockchain?

2. LITERATURE REVIEW

2.1 Blockchain Overview

Blockchain is a decentralized and distributed digital ledger technology that allows transactions to be recorded and verified securely and transparently, without the need for intermediaries or central authorities. A blockchain consists of a series of blocks linked together in a chronological and immutable manner using cryptographic algorithms. Each block contains a list of transactions that have been validated and confirmed by a network of nodes or validators.

The main features of blockchain include transparency, immutability, security, and decentralization. Transactions on a blockchain are transparent and traceable back to their origin, providing a high degree of accountability and auditability. Once a transaction has been recorded on the blockchain, it cannot be altered or deleted, ensuring the integrity and immutability of the ledger. The security of the blockchain is ensured by the use of cryptographic algorithms that make it virtually impossible to hack or tamper with the ledger. Finally, the decentralization of the blockchain means that it is not controlled by any single entity or authority, making it resistant to censorship and corruption.

Blockchains can be used for a wide range of applications, including cryptocurrencies, supply chain management, digital identity, voting systems, and more. The most well-known blockchain is the Bitcoin blockchain, which was created in 2009 as a decentralized, peer-to-peer electronic cash system. Since then, many other blockchains have been developed, each with its own unique features and use cases [8].

2.2 Security and Privacy

In light of its foundational principles, let's delve deeper into the critical aspects of security and privacy that blockchain technology addresses. Security and privacy are critical concerns in the digital age, where personal and sensitive data are constantly being transmitted and stored online. Security entails safeguarding digital assets against unauthorized access, theft, and potential damage. Privacy, on the other hand, refers to the protection of personal information and the right to control how it is collected, used, and shared.

To ensure security and privacy, various technologies and methods have been developed. Encryption is one such technology used to protect data from unauthorized access by converting it into a code that can only be deciphered by authorized parties. Two-factor authentication (2FA) is another method commonly used to enhance security in digital systems. For instance, when a user attempts to log into their online banking account, they are prompted to enter their password as the first factor. However, to add an extra layer of security, the system also requires the user to provide a second factor, which could

be a unique code sent to their mobile device or a fingerprint scan. This ensures that even if someone gains access to the user's password, they still cannot access the account without the second authentication factor. The combination of these two factors significantly reduces the risk of unauthorized access and helps protect sensitive information from potential breaches.

Blockchain technology has also been proposed as a means of enhancing security and privacy. Employing cryptographic algorithms and distributed networks, blockchains offer robust security and immutability, rendering them well-suited for diverse applications, including financial transactions, supply chain management, and identity verification. Additionally, blockchains can be designed to allow for anonymity and pseudonymity, thereby enhancing privacy [9]. In the context of blockchains, "anonymity" refers to the state of concealing the true identity of participants involved in transactions. "Pseudonymity," on the other hand, involves the use of pseudonyms or aliases instead of actual names to represent participants in blockchain transactions.

3. Methodology

3.1 Identification

This study followed the PRISMA technique and adhered to a structured process of identification, screening, eligibility, data abstraction, and analysis. Systematic literature reviews involve reviewing documents based on well-defined questions and using explicit methods to select and critically evaluate relevant studies. The review focused on two (2) principal publication sources, namely Scopus and IEEE, to ensure high-quality standards. To ensure the selection of only articles in the field of blockchain for security and privacy, each database utilized a specific search string, as indicated in Table 1 below.

Table 1: Database of research and keywords used

DATABASES	KEYWORDS USED
Scopus	TITLE-ABS-KEY ("security and privacy" AND "blockchain") AND (LIMIT- TO (OA , "all")) AND (LIMIT-TO (PUBYEAR , 2023) OR LIMIT-TO (PUBYEAR , 2022) OR LIMIT-TO (PUBYEAR , 2021) OR LIMIT-TO (PUBYEAR , 2020)) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (EXACTKEYWORD , "Security and Privacy") OR LIMIT-TO (EXACTKEYWORD , "Security and Privacy."))
IEEE	**Filters Applied:** Journals data privacy blockchains security of data 2020 – 2023

3.2 Screening

During the screening phase, articles were evaluated and classified as either eligible or ineligible based on a predefined set of criteria. For this review, the screening process was confined to articles published between 2020 and 2023, as a sufficient number of studies were available within this

timeframe to conduct a comprehensive review. Consequently, the time frame covering the period between 2020 and 2023 was included as one of the criteria for article selection. To avoid any confusion, only articles written in English were considered. In alignment with the review's objective, which centered on blockchain security and privacy areas and challenges, research studies were also included as selection criteria to enhance the relevance of the findings.

Table 2: Criterion, inclusion and exclusion criteria

CRITERION	INCLUSION CRITERIA	EXCLUSION CRITERIA
Publication Timeline	Papers published between 2020 to 2023	Papers that were published before 2020 or after 2023
Language	Papers published in English	Papers that are not published in English
Document Type	Papers that are published in journals	Review articles, chapters of book, proceedings
Nature of the study	Papers that focus on security and privacy in blockchain technology	Papers that do not address security and privacy in blockchain technology

Out of 4693 articles identified, a total of 4504 articles were excluded from the review during the screening process for not meeting the pre-established inclusion criteria, and 15 duplicate articles were also removed. Following this, the remaining 189 articles were deemed eligible and included in the third step of the review process.

3.3 Eligibility

After completing the screening process, the next step involved assessing the eligibility of articles related to blockchain security and privacy. In this step, the authors manually reviewed the articles that had successfully passed the screening process to ensure their alignment with the established criteria. This involved scrutinizing of the title, abstract, and content of each article. During this phase, 174 articles focused on blockchain security and privacy were selected. Eventually, these articles were subjected to further analysis and synthesis as part of the systematic literature review.

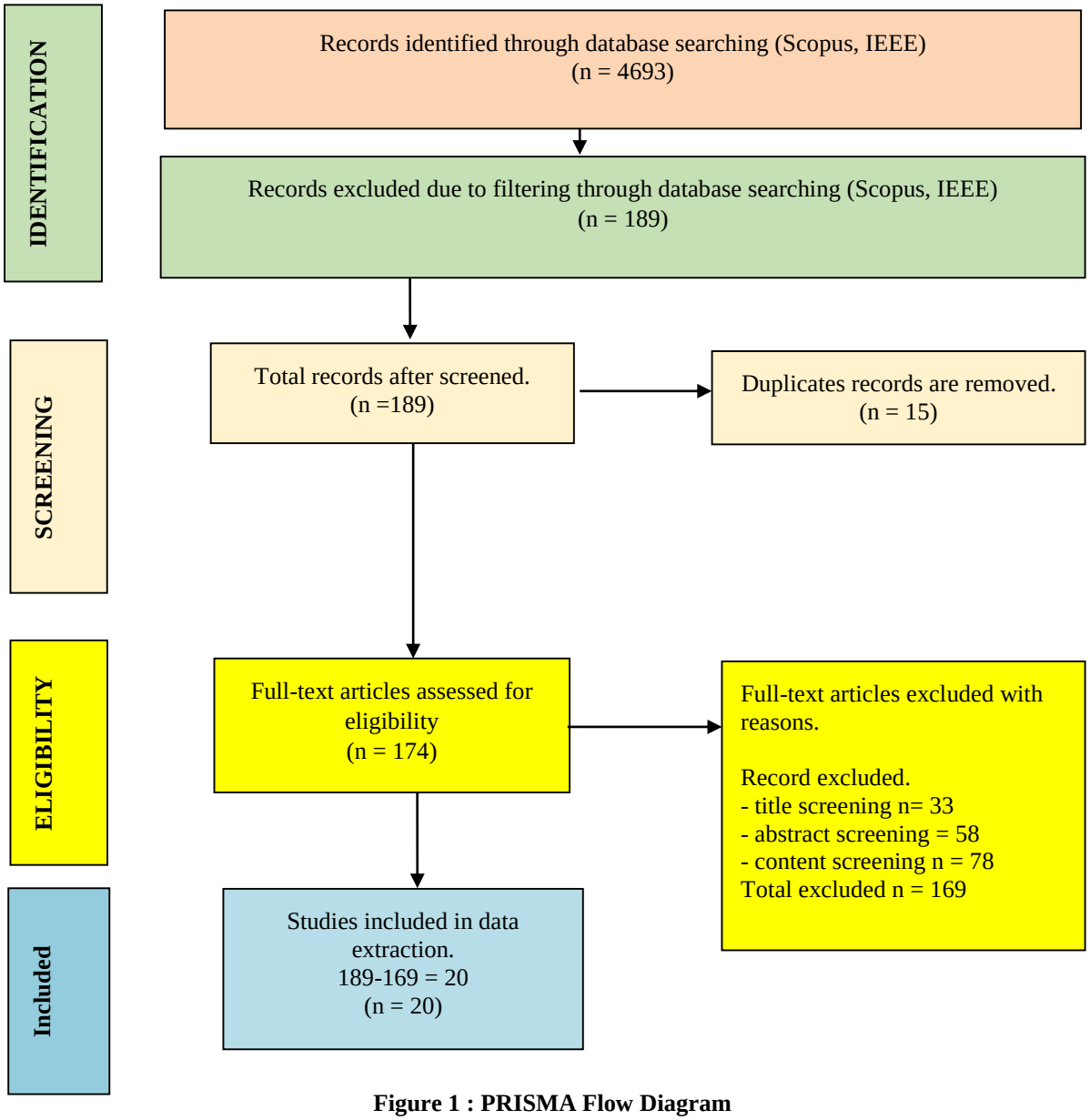

Figure 1 : PRISMA Flow Diagram

3.4 The quality appraisal

The quality assessment stage was conducted to ensure that the methodology and analysis of the chosen studies were executed to a satisfactory level. The next stage involves subjecting the papers to a quality assessment process. To ascertain the relevance of a paper to the research topic, three quality criteria were established for its evaluation. These quality criteria encompass:

QC1: Does the paper discuss the areas in which blockchain security and privacy are applied?

QC2: Does the study address the challenges/limitations of blockchain security and privacy?

QC3: Does the paper explore the future developments in blockchain security and privacy?

3.4 Data Abstraction and Analysis

After identifying the relevant papers, they were assessed and analyzed, with a focus on specific articles pertaining to the study's issues. The data were initially collected by reviewing the abstracts, followed by an in-depth analysis of the entire article to discern relevant themes and sub-themes. Furthermore, each article's abstract was examined and evaluated for its contribution to the ongoing discourse.

4. Results and Discussion

4.1 Search and Selection Results

Out of the 20 articles selected, Table 1 below displays the titles of each article, the year of publication, and the corresponding journal.

Table 3: Primary study selected

PAPERS	TITLE	YEAR	CITE	JOURNAL
P1	Customized blockchain-based architecture for secure smart home for lightweight IoT	2021	[1]	Science Direct
P2	PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities	2020	[2]	Science Direct
P3	A framework of blockchain-based secure and privacy-preserving E-government system	2020	[3]	Wireless Networks (SpringerLink)
P3	A framework of blockchain-based secure and privacy-preserving E-government system	2021	[10]	IEEE Transactions on Network and Service Management
P5	Blockchain Technology to Handle Security and Privacy for IoT Systems	2022	[11]	International Journal of Electrical and Electronics Research (IJEER)
P6	Blockchain-Based Privacy Enforcement in the IoT Domain	2022	[5]	IEEE Transactions on Dependable and Secure Computing
P7	Design of a Cloud-Blockchain-based Secure Internet of Things Architecture	2022	[6]	International Journal of Advanced Computer Science and Applications

P8	Presenting a method to detect intrusion in IoT through private blockchain	2022	[12]	Turkish Journal of Electrical Engineering and Computer Sciences
P9	Rampant Smoothing (RTS) Algorithm: an optimized consensus mechanism for private Blockchain enabled technologies	2022	[13]	EURASIP Journal on Wireless Communications and Networking
P10	Securing the access control policies to the Internet of Things resources through permissioned blockchain	2022	[14]	Concurrency and Computation: Practice and Experience (Wiley)
P11	Security and privacy for mobile IoT applications using blockchain	2021	[15]	Sensors (MDPI)
P12	Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hash Function	2022	[16]	Future Internet (MDPI)
P13	New Blockchain Based Special Keys Security Model With Path Compression Algorithm for Big Data	2022	[17]	IEEE Access
P14	Privacy-Preserving Mechanism in Smart Home Using Blockchain	2021	[18]	IEEE Access
P15	Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges	2020	[19]	IEEE Access
P16	Towards Using Blockchain Technology to Prevent Diploma Fraud	2021	[20]	IEEE Access
P17	MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address	2021	[21]	IEEE Access
P18	A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges and Future Research Directions	2022	[22]	IEEE Access
P19	A Two-Stage Privacy Preservation and Secure Peer-to-Peer Energy Trading	2021	[23]	IEEE Access

	Model Using Blockchain and Cloud-Based Aggregator			
P20	The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses	2021	[24]	IEEE Communications Surveys and Tutorials

A narrative summary has been crafted to guide the reader through the studies focusing on the implementation of blockchain for security and privacy A narrative summary has been crafted to guide the reader through the studies, elucidating features, designs, and key findings of the investigation. Given the diversity of research designs employed in this review, a thematic analysis was undertaken to effectively synthesize and integrate these variations. Thematic analysis, a method employed in this review, seeks to unveil patterns among existing studies by uncovering similarities or relationships present within the available data [25]. The approach for thematic synthesis in this review was structured in accordance with the steps proposed by [26].

The content analysis was executed using ATLAS.ti 22 to pinpoint themes concerning the implementation of blockchain for security and privacy. To commence, the researchers immersed themselves in the entire dataset, engaging in active and repeated readings. This foundational step provided the researchers with crucial insights into the raw data, laying the groundwork for subsequent steps. These stages were conducted utilizing the ATLAS.ti software as an aid in the thematic analysis. Researchers can use ATLAS.ti to code, categorize, and analyze their data, as well as to identify patterns, themes, and relationships within the information they've collected. Following this, the process of generating initial codes took place. During this phase, the researchers meticulously organized data at a granular and specific level. A comprehensive reading of all selected articles was performed, with a focus on extracting data relevant to the principal research question.

The subsequent phase encompassed the generation of themes. The researchers employed an inductive coding framework, aiming to recognize interests, commonalities, and connections inherent in the extracted data. The synthesis process adhered to this inductive coding framework, wherein the themes emerged from the coded data. These developed themes were intrinsically linked to the original data, reflecting the entirety of the dataset [25].

4.2 RQ1: How many research papers are produced focused on security and privacy in blockchain between 2020 to 2023 and which journals were published?

From the findings, a total of 20 research papers were identified. The distribution of these research contributions across a spectrum of reputable journals reflects the interdisciplinary nature of blockchain research. The IEEE journal, a prominent platform in the realm of technology, emerged as a prominent contributor, publishing a total of seven papers across the three-year span. Particularly noteworthy is its substantial presence in 2021, where it published four papers, further emphasizing the burgeoning relevance of blockchain research.

Other notable contributions come from a diverse array of journals, each with a unique focus on distinct aspects of blockchain security and privacy. For instance, the IEEE Communications Surveys and Tutorials, IEEE Transactions on Dependable and Secure Computing, and IEEE Transactions on Network and Service Management each offered valuable insights in the years 2021 and 2022. The Science Direct journal featured two papers, with one in 2020 and another in 2021, contributing to the broader discourse.

Furthermore, the dispersion of research papers across a variety of other journals such as the International Journal of Advanced Computer Science and Applications, International Journal of Electrical and Electronics Research (IJEER), Sensors (MDPI), Turkish Journal of Electrical Engineering and Computer Sciences, Wireless Networks (SpringerLink), Concurrency and Computation: Practice and Experience (Wiley), EURASIP Journal on Wireless Communications and Networking, and Future Internet (MDPI) signifies the wide-reaching impact of blockchain technology on various domains.

Table 4: The Journal name and the year of publish

Journal Name	**Number of Papers / Years**			
	2020	**2021**	**2022**	**Grand Total**
IEEE	1	4	2	7
IEEE Communications Surveys and Tutorials		1		1
IEEE Transactions on Dependable and Secure Computing			1	1
IEEE Transactions on Network and Service Management		1		1
Science Direct	1	1		2
International Journal of Advanced Computer Science and Applications			1	1
International Journal of Electrical and Electronics Research (IJEER)			1	1
Sensors (MDPI)		1		1
Turkish Journal of Electrical Engineering and Computer Sciences			1	1
Wireless Networks (SpringerLink)	1			1
Concurrency and Computation: Practice and Experience (Wiley)			1	1
EURASIP Journal on Wireless Communications and Networking			1	1
Future Internet (MDPI)			1	1
Grand Total	**3**	**8**	**9**	**20**

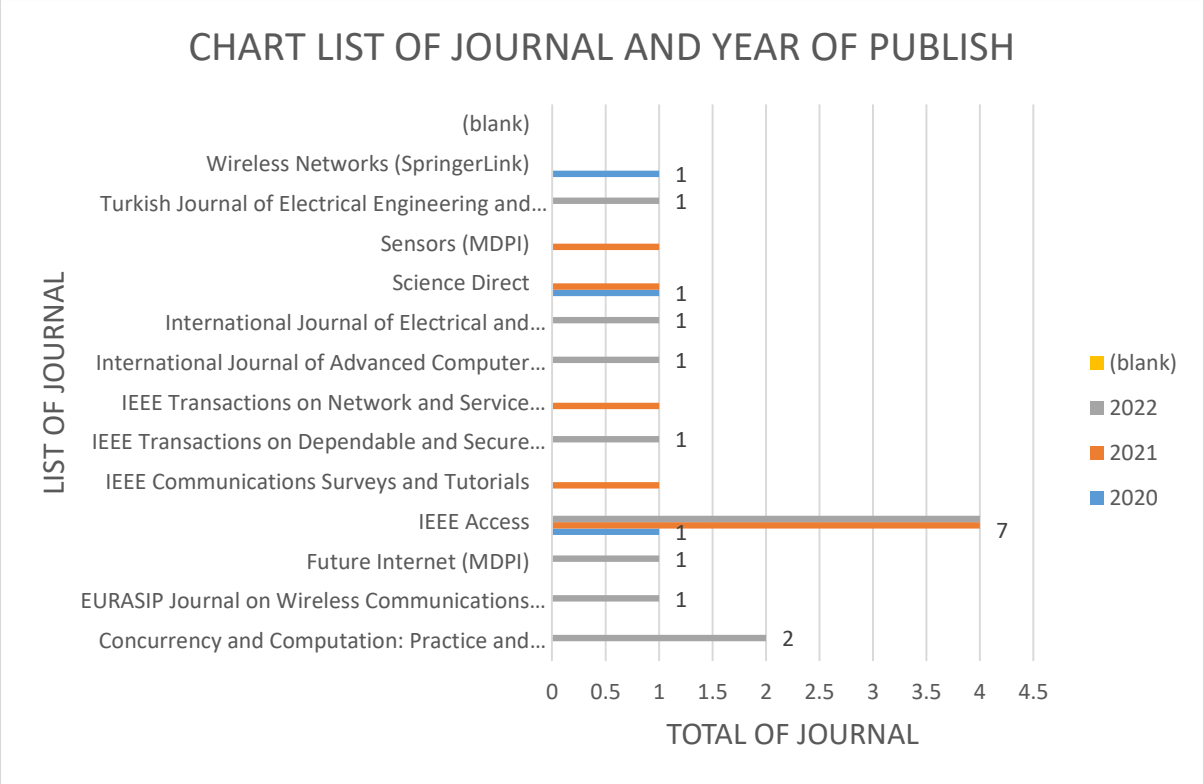

Figure 2 : Chart list of journal and year publish

4.3 RQ2: What areas of Blockchain are focusing on security and privacy?

Upon a comprehensive review of the paper's content, it is evident that multiple application areas are pertinent to the security and privacy dimensions of blockchain. These encompass a wide range of sectors, including Artificial Intelligence (AI) [27], Internet of Things (IoT) [1], [5], [6], [11], [12], [21], [22], [18], [14]–[16], Education Sector [20], Energy Trading [23], Big Data [17], Energy Sector [17], Blockchain [24], Electronic government (e-Government) [3], Smart Cities [2], Smart Contracts [19], e-Commerce [10], Clinical Data Management [13]. The visual representation in Figure 3 succinctly emphasizes the pervasive significance of security and privacy considerations across diverse fields. Notably, the Internet of Things emerges as the prominent contributor in this context.

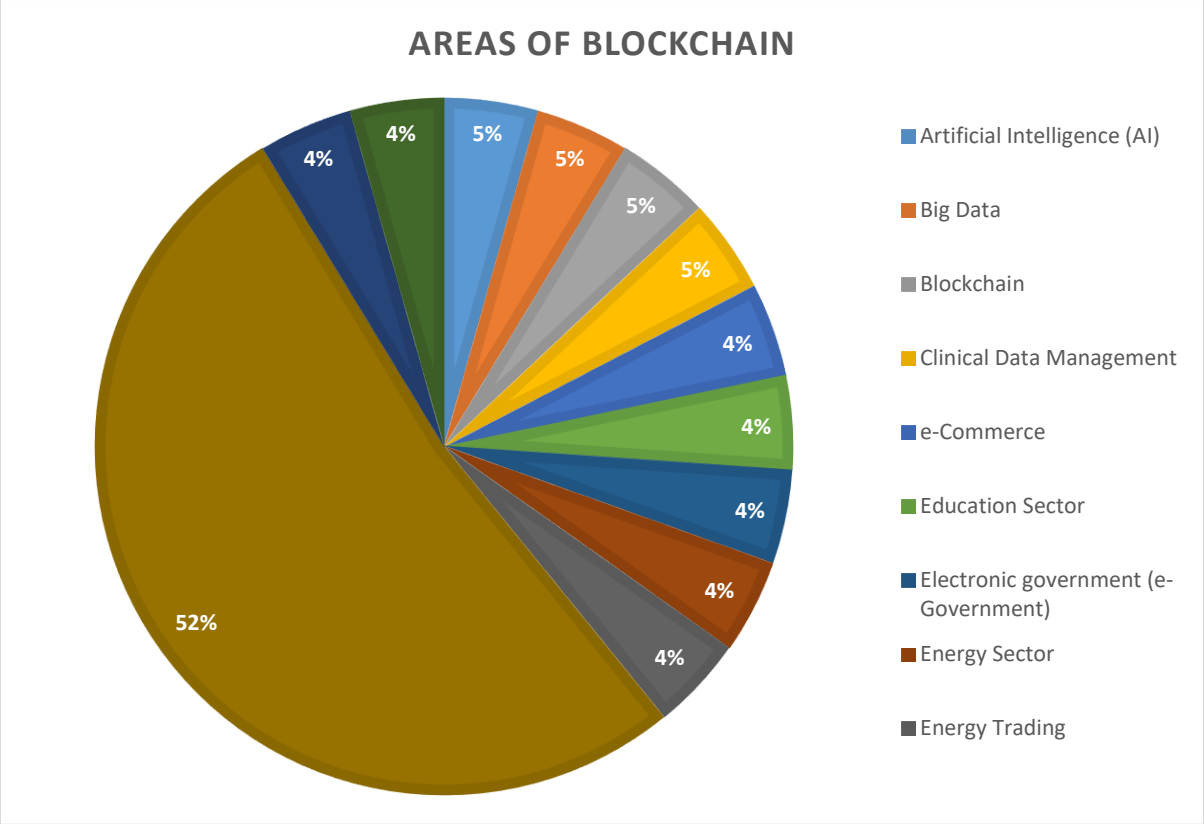

Figure 3 : The areas fields related to the blockchain for security and privacy

4.4 RQ3: What are the differences between each research study?

The differences among the referenced research studies are thoroughly scrutinized by dissecting the specific objectives pursued by each group of researchers. The subsequent table comprehensively outlines the individual articles, their respective domains, and the discernible divergences inherent in these studies. Each dissimilarity is meticulously elucidated, drawing from the accompanying explanations.

Table 5: The thematic analysis resulted in differences between each research study

ARTICLES	AREAS	DIFFERENCES
P1	IoT applications	Blockchain for secure smart homes. - Smart home devices can communicate with each other using blockchain as a secure and reliable medium. This technology can ensure data privacy, prevent unauthorized access, and offer a secure platform for communication between smart devices in a smart home ecosystem.
P2	IoT data sharing in a smart city environment.	PrivySharing: Secure IoT Data Sharing in Smart Cities using Blockchain - "PrivySharing" is a blockchain framework that enables secure and private sharing of IoT data in smart cities. It

		ensures data authenticity and confidentiality while promoting secure data sharing among authorized entities.
P3	Electronic government (e-Government)	Decentralized e-Government Peer-to-Peer System using Blockchain" - A decentralized e-government P2P system is proposed using blockchain technology. It provides a secure and transparent platform for government services by removing the need for intermediaries and central authorities.
P4	e-Commerce	RepChain: Blockchain-based Privacy-Preserving Reputation System for E-commerce - RepChain is a privacy-preserving reputation system for e-commerce platforms that is based on blockchain technology.
P5	Internet of Things (IoT)	Blockchain-based Privacy Policies for IoT Protection - This study presents an overview of blockchain-based policies for privacy protection in the Internet of Things (IoT). It highlights how blockchain technology can be utilized to enhance privacy and security in IoT applications.
P6	Internet of Things (IoT)	Blockchain-based Privacy Enforcement Framework for User Data Control - To allow consumers to control how their data is used and verify that their wishes are honoured without depending on a centralised management, we propose a blockchain-based privacy enforcement system.
P7	Internet of Things (IoT)	Cloud-Blockchain-based Secure IoT Architecture for Advanced Storage and Security - This work aims to develop an architecture for IoT systems that utilizes cloud and blockchain technologies to provide secure and efficient storage solutions. The proposed architecture can enhance the security of IoT devices and protect against data breaches.
P8	Internet of Things (IoT)	IoT-Optimized Private Blockchain Overlay Network - Suggested an overlay network in private BC to enhance its scalability, decrease network overhead, and shorten response times.

P9	Healthcare system	Real-Time Consensus with Rampant Smoothing Algorithm for Distributed Data - The Rampant Smoothing (RTS) algorithm, which ensures integrity, security, and dependability for scattered data structures in real time, was used in a revolutionary consensus process.
P10	Internet of Things (IoT)	Integration of Permission Blockchain in IoT Distributed Middleware for Secure Resource Access. - Propose integrating a permission blockchain into an honest but sceptic (not trust) IoT distributed middleware layer to ensure that interested parties have the proper management access to resources. in a nutshell
P11	Internet of Things (IoT)	User-Controlled Privacy with Blockchain Anonymisation - By implementing user-controlled privacy, blockchain's anonymization features can be used to improve user privacy and the privacy of their data.
P12	Internet of Things (IoT)	Preserving User Access Policy Privacy with Confidentiality and Authenticity" - By safeguarding the secrecy and veracity of the conveyed message and collecting the required consents for data access, this work intends to maintain the privacy of user access policy.
P13	Big Data	BSKM: Blockchain-based Security Model for Big Data Blockchain-based Special Key Security Model (BSKM). - For big data, BSKM develops, implements, and integrates three information security components: confidentiality, integrity, and availability.
P14	Internet of Things (IoT)	Secure Authentication for IoT in Smart Homes with ABAC, Smart Contracts, and Edge Computing - To establish a safe foundation for IoT devices in smart home systems, offer an authentication strategy that blends attribute-based access control with smart contracts and edge computing.
P15	Artificial Intelligence (AI)	AI Techniques for Supply Chain Privacy Protection - examines numerous artificial intelligence (AI) methods and solutions for protecting SC privacy

P16	Education And Training Sector	Blockchain-based Cryptographic Solution for Data Security - By utilising several fundamental cryptographic primitives and data structures, we provide a Blockchain-enabled solution.
P17	Health Information	MEXchange: Privacy-Preserving HIE with Blockchain - We recommend MEXchange, a cutting-edge blockchain-based HIE that protects user privacy by hiding sender and receiver addresses.
P18	Internet of Things (IoT)	Decentralized Authentication with Blockchain Technology - Decentralized architectures are enforced by blockchain-based authentication systems.
P19	Energy Trading	Two-Layered Secure P2P Energy Trading with Blockchain - In this paper, a blockchain-based, two-layered P2P energy trading paradigm is proposed
P20	Blockchains	Security Reference Architecture for Blockchain - We suggest the Security Reference Architecture (SRA) for Blockchains, which uses a layered model (like the ISO/OSI) to describe the types and hierarchies of various security and privacy features.

4.5 RQ4: What are the challenges of security and privacy in blockchain?

Blockchain functions within a peer-to-peer (P2P) network, operating through a distributed protocol that eliminates the need for a centralized and reliable third party. Despite this absence, blockchain remarkably possesses the capacity to cultivate trust among entities that may not inherently hold mutual trust. Moreover, each transaction conducted on the blockchain is characterized by transparency and visibility. These inherent benefits bestow upon blockchain a distributed, openly accessible, and tamper-resistant data architecture, thereby ensuring the security of data. The realms of IT and communications are profoundly influenced by the transformative potential of blockchain, positioning it as a cornerstone technology in these industries.

Table 6: The thematic analysis resulted in challenges of security and privacy in blockchain

ARTICLES	CHALLENGES
P1	Internet of Thing (IoT)
P2	Challenges in Integrating Blockchain and IoT for Secure Data Management
P5	- The integrate blockchain in Internet of Thing (IoT)
P7	- Security and privacy challenges for data generated in IoT environment
P8	- Concern about how data will be collected and shared with others in term of
P10	data security and privacy.

P14 P11 P12 P13	- to make restricted IoT devices and the blockchain more interoperable - lack of user access policies that ensure privacy when accessing personal data in the IoT system. - These issues—data loss, data breach, data leakage, and data theft—have developed into serious dangers to the organizations. - Secure IoT device integration
P3	e-Government Challenges in Implementing Blockchain for E-Government Systems - Trend in the creation of an e-government system is blockchain technology.
P4 P6	e-Commerce Security and Privacy Challenges in User Data Sharing - Data sharing without understanding risks leads to security and privacy issues - Security and privacy issues develop as a result of end users often sharing sensitive data with other customers without fully understanding how it will be handled and used. - Due to end users frequently sharing sensitive data with other consumers without being fully aware of how it will be handled and utilised, security and privacy issues arise.
P9 P17	Healthcare Challenges in Implementing Blockchain in Healthcare - implementation of blockchain in the healthcare sector - Health information management across healthcare organisations is connected, and sharing is secure.
P16	Education Blockchain's Role in Stopping Diploma Issuer Fraud - The record-keeping and time-stamping capabilities unique to the blockchain are essential for our solution to stop diploma issuer fraud.
P18 P15 P20	Blockchain Challenges in Analysing Security Risks in Blockchain Architecture - All the architectural frameworks that security and privacy function in now include them as essential components. - absence of established techniques for analysing security issues associated to blockchain. - there are no defined techniques for analysing security risks connected to blockchains.
P19	Energy

Challenges in Ensuring Trust, Security, and Privacy in Energy Trading Systems	- Energy systems have trust, security, and privacy issues as a result of the energy trading between numerous prosumers.

Referring to Table 6 above, the previous studies have highlighted several challenges as identified by researchers. These challenges include:

i. Challenges in Integrating Blockchain and IoT for Secure Data Management
The integration of blockchain and IoT offers secure and decentralized communication for devices. However, addressing challenges such as security and privacy concerns related to IoT-generated data, secure data collection, storage, sharing, and user access policies is crucial. Collaborative efforts among stakeholders are necessary to develop secure IoT device integration strategies and a reliable ecosystem that safeguards user privacy and data.

ii. Challenges in Implementing Blockchain for E-Government Systems
Blockchain technology has the potential to revolutionize e-government systems by providing a secure and efficient means for citizens to engage with the public sector. This technology ensures fault tolerance, maintaining operational efficiency despite errors or failures. Governments can enhance service delivery by adopting blockchain technology, offering citizens a convenient and secure mode of interaction. Leveraging blockchain can lead to more secure, efficient, and transparent e-government systems that benefit citizens and businesses alike.

iii. Security and Privacy Challenges in User Data Sharing
The challenge involves educating end users about data sharing risks and implementing strict access control policies to limit data exposure. This prevents security and privacy issues stemming from sharing sensitive data without understanding its implications.

iv. Challenges in Implementing Blockchain in Healthcare
Implementing blockchain technology in the healthcare sector comes with challenges. Ensuring interoperability among different healthcare systems and platforms is a key challenge. Healthcare organizations may use disparate systems, complicating integration into a unified blockchain network. Additionally, maintaining data privacy and confidentiality proves challenging due to the sensitivity of healthcare data and regulatory requirements. Ensuring cybersecurity and protection against threats necessitates significant technical expertise and investment.

v. Blockchain's Role in Preventing Education Issuer Fraud
Challenges in using blockchain to prevent diploma issuer fraud include ensuring accuracy and authenticity of data entered into the blockchain. Privacy and security of sensitive personal data are paramount. Promoting blockchain adoption by educational institutions and regulatory bodies poses another challenge. Addressing technical complexities and costs associated with developing and maintaining blockchain-based solutions is also a concern.

vi. Challenges in Analyzing Security Risks in Blockchain Architecture
Analyzing security risks in blockchain architecture is challenged by the absence of established techniques and tools for assessing blockchain-specific security issues. Integrating security and privacy components into architectural frameworks adds complexity. Overcoming these

challenges requires new methodologies for evaluating blockchain security risks and their implementation in existing security frameworks.

vii. Challenges in Ensuring Trust, Security, and Privacy in Energy Trading Systems
Ensuring trust, security, and privacy in energy trading systems involves creating secure and decentralized systems to handle extensive transactions among prosumers. Developing privacy-preserving techniques to safeguard sensitive information, like energy consumption and trading history, is another challenge. Maintaining reliability and transparency in energy trading systems is crucial for maintaining prosumer trust. Addressing the technical intricacies and costs of developing and maintaining secure energy trading systems is also a concern.

4.6 RQ5: Future Directions for Security and Privacy in Blockchain

Security and privacy will continue to be central in future blockchain technology research. Various recommendations are made to enhance blockchain network security, including establishing a mechanism for secure IoT device connection to the blockchain network and deploying appropriate blockchain technology in the public sector. The paper underscores the importance of privacy on blockchains and proposes a framework that upholds privacy while granting individuals control over their data usage. Further research is needed to assess diverse privacy approaches, improving privacy protection without compromising accuracy. To ensure the successful adoption of evolving blockchain technology, resolving these security and privacy issues is imperative.

Table 7: The thematic analysis resulted in future works on security and privacy in blockchain

ARTICLES	AREAS	FUTURE WORK
P1	IoT applications	Focus on security threat.
P2	IoT data sharing in a smart city environment.	Create a system that would allow IoT devices to safely connect to the blockchain network.
P3	Electronic government (e-Government)	The implementation of the right blockchain technology in public sectors to improve and meet the security and privacy of individual data.
P4	e-Commerce	Enhance RepChain to support textual comments and ratings with a privacy-preserving system.
P5	Internet of Things (IoT)	Enterprise and organizational innovation has shifted its strategic attention to developing new IoT service models, and merging blockchain technologies to create a "decentralized" IoT structure has emerged as one of the most important models.
P6	Internet of Things (IoT)	Framework for enforcing privacy on the blockchain that allows individuals to control how their data is used.

P7	Internet of Things (IoT)	For the development of various applications in IoT infrastructure with high security and efficiency, IoT architecture can be used.
P8	Internet of Things (IoT)	to integrate the BC with the IoT
P9	Healthcare system	To identify additional relevant evaluation criteria, confirm results using legitimate Blockchain-centered healthcare use cases.
P10	Internet of Things (IoT)	Express the situation in a more complicated setting
P11	Internet of Things (IoT)	To create techniques that protect privacy so that public nodes can identify the data they can access without revealing the entry's ACL or any other private information.
P12	Internet of Things (IoT)	In the IoT ecosystem, cryptographic methods offer a secure platform for users and data requesters to share their data.
P13	Big Data	To give big data-based bank and financial data improved security and privacy features.
P14	Internet of Things (IoT)	More research is needed to assess the different privacy guarantees in order to achieve enhanced privacy protection without compromising accuracy.
P15	Artificial Intelligence (AI)	Use the SC in a variety of smart applications.
P16	Education And Training Sector	For our needs, the majority of Consortium Blockchain platforms with smart contract functionalities, such as Hyperledger Fabric 3 or Corda 4 or Enterprise Ethereum, will be sufficient.
P17	Health Information	While implementing blockchain in the healthcare industry, future research to manage sensitive data might be taken into account.
P18	Internet of Things (IoT)	It is obvious that the smart city architecture may face security and privacy issues because it also depends on the traditional internet, which is backed by communication and transmission technologies for data gathering and transfer, respectively.
P19	Energy Trading	The protection of privacy based on blockchain systems is another issue that has not been fully

		addressed. Thus, it is vital that solutions be found to protect user privacy.
P20	Blockchains	Future research should focus on network protocols' security features, their applicability in a decentralised setting, and any room for improvement.

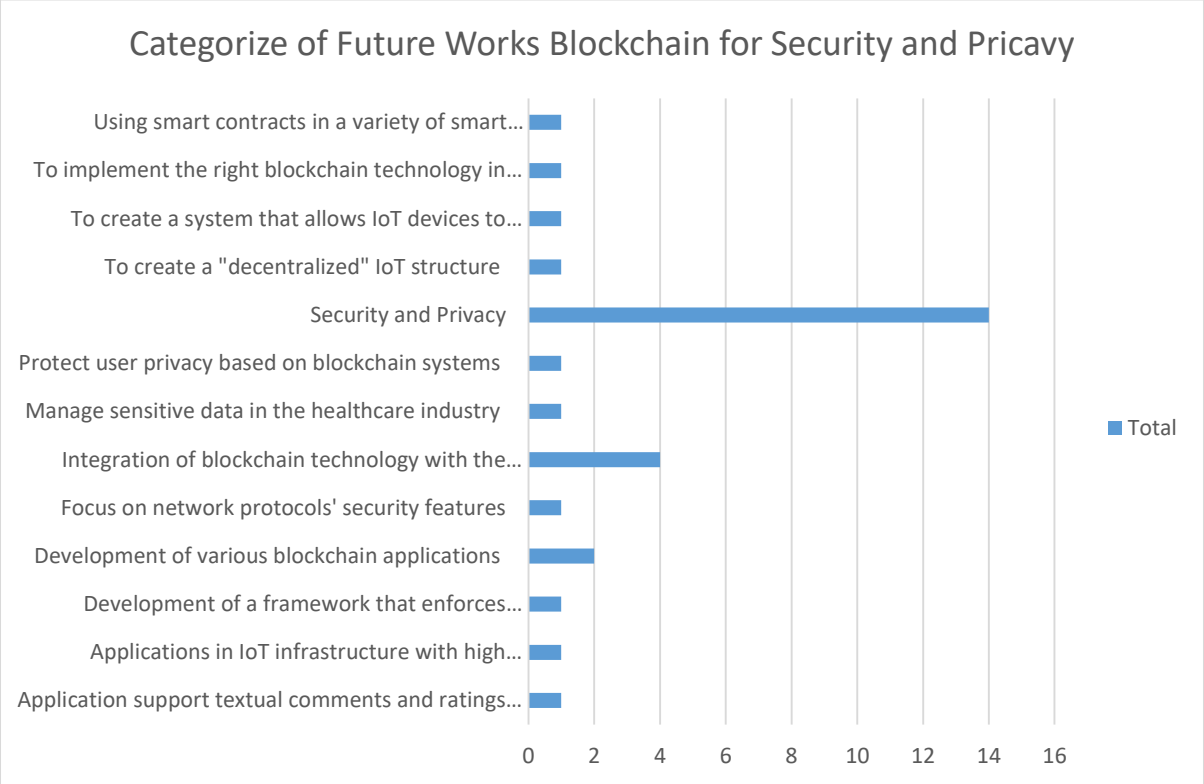

Figure 4 : Categorize of Future Works Blockchain for Security and Privacy

The article highlights several areas of future work for blockchain technology. Security and privacy is a major area of concern, as highlighted by references [1]–[3], [5], [13], [15]–[18], and [21]–[24].. The article emphasizes the need to address security threats and enhance the privacy of individual data. There is a call to create a system that allows IoT devices to safely connect to the blockchain network [2], and to implement the right blockchain technology in public sectors to improve security and privacy [3]. Additionally, there is a suggestion to enhance RepChain to support textual comments and ratings with a privacy-preserving system. The article proposes the development of a framework that enforces privacy on the blockchain, giving individuals control over how their data is used [5].

Another area of future work is exploring the integration of blockchain technology with the Internet of Things (IoT) [2], [6], [11], [12]. The article notes that there has been a strategic shift in enterprise and organizational innovation towards developing new IoT service models. The merging of blockchain technologies to create a 'decentralized' IoT structure has emerged as a prominent and impactful model [11]. The article suggests that IoT architecture can be used for the development of various applications in the IoT infrastructure with high security and efficiency [6]. There is also a recommendation to integrate blockchain with IoT for improved security [12].

Lastly, the article calls for the development of various blockchain applications [19], [20]. It proposes using smart contracts in a variety of smart applications and highlights that the majority of

Consortium Blockchain platforms with smart contract functionalities, such as Hyperledger Fabric 3 or Corda 4 or Enterprise Ethereum, will be sufficient for most needs [20]. Future research is suggested to manage sensitive data in the healthcare industry while implementing blockchain [21]. The article also emphasizes the importance of finding solutions to protect user privacy based on blockchain systems [23]. Lastly, it recommends future research to focus on network protocols' security features, their applicability in a decentralized setting, and any room for improvement [24].

5. CONCLUSION

In conclusion, the article highlights several areas of future work for blockchain technology, particularly in the areas of security and privacy, integration with the IoT, and the development of various blockchain applications. With the increasing adoption of blockchain technology in various sectors, it is essential to address security threats and enhance the privacy of individual data. The article suggests that the integration of blockchain with IoT can improve security and proposes the development of a framework that enforces privacy on the blockchain. Furthermore, it highlights the importance of exploring the potential of smart contracts in various smart applications. Continued research in this field holds promise for the emergence of innovative solutions and applications that address these challenges, ultimately leading to a more secure and decentralized future.

Following the three issues about the security and privacy of blockchain that were put forth in this work, we searched and screened 20 papers in the IEEE database and SCOPUS database using a systematic literature review. The goal of the study is to review and examine the current level of research on blockchain security and privacy. Initially, we provide a summary of the blockchain's security and privacy applications. The difficulties with blockchain security and privacy are then examined. We conclude by talking about the development trend for blockchain privacy and security.

References

[1] M. Ammi, S. Alarabi, and E. Benkhelifa, “Customized blockchain-based architecture for secure smart home for lightweight IoT,” *Inf. Process Manag.*, vol. 58, no. 3, p. 102482, May 2021, doi: 10.1016/j.ipm.2020.102482.

[2] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, “PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities,” *Comput. Secur.*, vol. 88, p. 101653, Jan. 2020, doi: 10.1016/j.cose.2019.101653.

[3] N. Elisa, L. Yang, F. Chao, and Y. Cao, “A framework of blockchain-based secure and privacy-preserving E-government system,” *Wirel. Netw.*, vol. 29, pp. 1005–1015, Dec. 2018, doi: 10.1007/s11276-018-1883-0.

[4] C. Zhonghua and S. B. Goyal, “Blockchain technology to handle security and privacy for IoT systems: Analytical review,” *Int. J. Electr. Electron. Res.*, vol. 10, no. 2, pp. 74–79, Jun. 2022, doi: 10.37391/IJEER.100204.

[5] F. Daidone, B. Carminati, and E. Ferrari, “Blockchain-based privacy enforcement in the IoT domain,” *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 6, pp. 3887–3898, Sept. 2021, doi: 10.1109/TDSC.2021.3110181.

[6] D. Rani, N. S. Gill, and P. Gulia, “Design of a cloud-blockchain-based secure Internet of Things architecture,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, pp. 443–454, Jan. 2022, doi: 10.14569/IJACSA.2022.0130851.

[7] S. Kumar and A. K. Pundir, “Integration of IoT and blockchain technology for enhancing supply chain performance: A review,” 2020 11th IEEE Annual Information Technology, Electronics

and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2020, pp. 0396-0401, doi: 10.1109/IEMCON51383.2020.9284890.

[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." 2009. [Online]. Available: www.bitcoin.org. [Accessed May 31, 2023].

[9] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Inf Process Manag*, vol. 58, no. 1, Jan. 2021, doi: 10.1016/j.ipm.2020.102397.

[10] M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, and M. Alazab, "Anonymous and verifiable reputation system for e-commerce platforms based on blockchain," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 4, pp. 4434–4449, Dec. 2021, doi: 10.1109/TNSM.2021.3098439.

[11] C. Zhonghua and S. B. Goyal, "Blockchain technology to handle security and privacy for IoT systems: Analytical review," *Int. J. Electr. Electron. Res.*, vol. 10, no. 2, pp. 74–79, Jun. 2022, doi: 10.37391/IJEER.100204.

[12] R. Mahmoudie, S. Parsa, and A. M. Rahmani, "Presenting a method to detect intrusion in IoT through private blockchain," *Turk. J. Electr. Eng. Comput. Sci.*, vol. 30, no. 6, Art. 23, Sept. 2022, doi: 10.55730/1300-0632.3943.

[13] U. Tariq, "Rampant Smoothing (RTS) Algorithm: an optimized consensus mechanism for private Blockchain enabled technologies," *EURASIP J. Wirel. Commun. Netw.*, vol. 2022, no. 1, Art. 47, Dec. 2022, doi: 10.1186/s13638-022-02123-5.

[14] A. Rizzardi, S. sicari, D. Miorandi, and A. Coen-Porisini, "Securing the access control policies to the Internet of Things resources through permissioned blockchain," *Concurrency Computat. Pract. Exper.*, vol. 34, no. 15, p. e6934, Mar. 2022, doi: 10.1002/cpe.6934.

[15] K. Carvalho and J. Granjal, "Security and privacy for mobile iot applications using blockchain," *Sens.*, vol. 21, no. 17, p. 5931, Sep. 2021, doi: 10.3390/s21175931.

[16] Y. P. Khanal *et al.*, "Utilizing blockchain for IoT privacy through enhanced ECIES with secure hash function," *Future Internet*, vol. 14, no. 3, Mar. 2022, doi: 10.3390/fi14030077.

[17] C. Bakir, "New blockchain based special keys security model with path compression algorithm for big data," *IEEE Access*, vol. 10, pp. 94738-94753, Sept. 2022, doi: 10.1109/ACCESS.2022.3204289.

[18] A. Qashlan, P. Nanda, X. He, and M. Mohanty, "Privacy-Preserving Mechanism in Smart Home Using Blockchain," *IEEE Access*, vol. 9, pp. 103651–103669, 2021, doi: 10.1109/ACCESS.2021.3098795.

[19] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24746–24772, Jan. 2020, doi: 10.1109/ACCESS.2020.2970576.

[20] Q. Tang, "Towards Using Blockchain Technology to Prevent Diploma Fraud," *IEEE Access*, vol. 9, pp. 168678–168688, 2021, doi: 10.1109/ACCESS.2021.3137901.

[21] D. Lee and M. Song, "MEXchange: A privacy-preserving blockchain-based framework for health information exchange using ring signature and stealth address," *IEEE Access*, vol. 9, pp. 158122–158139, Nov. 2021, doi: 10.1109/ACCESS.2021.3130552.

[22] U. Khalil, Mueen-Uddin, O. A. Malik, and S. Hussain, "A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements,

challenges and future research directions," *IEEE Access*, vol. 10, pp. 76805–76823, Jul. 2022, doi: 10.1109/ACCESS.2022.3189998.

[23] A. S. Yahaya, N. Javaid, A. Almogren, A. Ahmed, S. M. Gulfam, and A. Radwan, "A two-stage privacy preservation and secure peer-to-peer energy trading model using blockchain and cloud-based aggregator," *IEEE Access*, vol. 9, pp. 143121–143137, Oct. 2021, doi: 10.1109/ACCESS.2021.3120737.

[24] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, pp. 341–390, Jan. 2021, doi: 10.1109/COMST.2020.3033665.

[25] V. Braun and V. Clarke, "Reflecting on reflexive thematic analysis," *Qualitative Research in Sport, Exercise and Health*, vol. 11, no. 4, pp. 589–597, Jun. 2019, doi: 10.1080/2159676X.2019.1628806.

[26] J. Thompson, "A guide to abductive thematic analysis," *Qual. Rep.*, vol. 27, no. 5, pp. 1410–1421, May 2022, doi: 10.46743/2160-3715/2022.5340.

[27] O. Fadi, Z. Karim, E. G. Abdellatif and B. Mohammed, "A survey on blockchain and Artificial intelligence technologies for enhancing security and privacy in smart environments," *IEEE Access*, vol. 10, pp. 93168-93186, Sept. 2022, doi: 10.1109/ACCESS.2022.3203568.