Journal of Namibian Studies, 35 S1 (2023): 3937-3959 ISSN: 2197-5523 (online)

The Intersection Of Blockchain And The Web Of Things: A Systematic Mapping Study

Amjad Aldweesh

College of Computer Science and IT, Shaqra University, Shaqra, Saudi Arabia.

Abstract

The integration of blockchain technology with the Web of Things (WoT) has the potential to enhance security, privacy, and interoperability, opening new opportunities for various industries. This systematic mapping study provides a detailed overview of the current state of research in the field of WoT based on blockchain technology. We analyzed 20 papers published until early 2023, classifying them based on their research objectives, methods, and contributions. Most of these papers targeted security and privacy concerns, emphasizing areas such as digital twins, access control, and data sharing. Additionally, topics such as interoperability, scalability, and governance were addressed. A significant number of papers propose the use of blockchain for structural health monitoring and food quality assurance, while others examine the integration of blockchain with wireless sensor networks and e-commerce. Although blockchain-based WoT has garnered increasing attention, further research is required to overcome challenges in scalability and interoperability, and to realize the full potential of this technology.

Keywords Blockchain, Web of Things (WoT), Ethereum, Hyperledger, Internet of Things (Iot)

1. Introduction

Blockchain technology has emerged as a promising solution for securely managing the vast amount of data generated by Internet of Things (IoT) devices. A blockchain-based Web of Things (WoT) system utilizes the distributed ledger technology of blockchain to ensure the integrity and security of IoT data, while also providing a mechanism for decentralized decision making.

In recent years, there has been a growing interest in the use of blockchain technology for IoT applications. This has led to the development of various blockchain-based WoT systems, each with their own unique features and capabilities. However, despite the growing body of research in this area, there is a lack of a comprehensive overview of the current state of the field.

To address this gap, we conduct a systematic mapping study of the literature on blockchain-based WoT systems. Our study aims to provide a comprehensive overview of the current state of the field, including the key challenges and opportunities facing the development of these systems.

We begin by conducting a literature search using a set of predefined keywords and inclusion criteria. The resulting set of papers is then analyzed and classified according to a set of predefined categories, including the type of blockchain used, the application area, and the key challenges and opportunities facing the development of the system.

Our study shows that the majority of the existing research on blockchain-based WoT systems has focused on the use of permissioned blockchain platforms, such as Hyperledger and Ethereum. The most common application areas for these systems include supply chain management, industrial IoT, and smart cities.

However, the study also highlights a number of key challenges facing the development of blockchain-based WoT systems, including scalability, interoperability, and the lack of standardization. In addition, the study highlights a number of opportunities for future research, including the use of new consensus algorithms, the development of new use cases, and the integration of blockchain with other technologies, such as edge computing and artificial intelligence.

Overall, our study provides a comprehensive overview of the current state of the field of blockchain-based WoT systems and highlights the key challenges and opportunities facing the development of these systems. As the field continues to evolve, further research is needed to address these challenges and capitalize on the opportunities presented by blockchain technology in the context of the IoT.

2. BACKGROUND

2.1. Blockchain

Blockchain technology is a decentralized, digital ledger that records transactions across a network of computers. It was first introduced in 2008 as the underlying technology for the digital currency, Bitcoin [1]. Since then, it has been applied to a wide range of industries and use cases, from cloud solutions [2] to Museum systems [3, 4].

One of the key features of blockchain technology is its ability to create a secure and transparent record of transactions. This is achieved through the use of cryptography and a consensus mechanism, which allows multiple parties to agree on the contents of the ledger. This eliminates the need for a central authority or intermediary to validate transactions, which can increase the efficiency and reduce the cost of many types of transactions [5].

Another important aspect of blockchain technology is its ability to create smart contracts, which are self-executing contracts with the terms of the agreement written directly into the code. This allows for the automation of complex processes, such as the transfer of assets or the execution of certain actions based on certain conditions.

One of the most well-known applications of blockchain technology is in the financial industry. Blockchain-based platforms such as Ripple and Ethereum have been used to create decentralized payment systems and digital currencies. These systems can facilitate cross-border transactions at a fraction of the cost of traditional payment methods, and can also provide increased security and transparency for financial transactions.

Another industry that has seen significant interest in blockchain technology is supply chain management. Blockchain based systems can be used to track the movement of goods and materials through the supply chain, providing increased transparency and traceability. This can help to improve efficiency, reduce fraud, and increase consumer trust in the authenticity of products.

In recent years, blockchain technology has also been applied to various use cases in the public sector. For example, blockchain-based voting systems have been proposed as a way to increase the transparency and security of the voting process. Some countries, such as West Virginia in the United States, have even tested blockchain-based voting systems in real elections [6].

Overall, blockchain technology has the potential to revolutionize many industries and use cases by increasing transparency, security, and efficiency. However, it is still a relatively new technology and there are many challenges that need to be addressed, such as scalability and regulatory compliance. Despite these challenges, many experts believe that blockchain technology will continue to grow and mature in the coming years, and will play an increasingly important role in many areas of our lives.

2.2. Smart Contract

Smart contracts are self-executing contracts with the terms of the agreement written directly into the code. They are one of the key features of blockchain technology and have the potential to revolutionize many industries by automating complex processes, reducing the need for intermediaries, and increasing transparency.

The concept of smart contracts was first proposed by computer scientist Nick Szabo in 1994 [7]. He defined them as ”a set of promises, specified in digital form, including protocols within which the parties perform on these promises”. Szabo recognized that smart contracts could be used to enforce, verify, and execute the negotiation or performance of a contract, and that they could be stored and replicated on a decentralized network.

Smart contracts are implemented on a blockchain network and are executed automatically when certain conditions are met. They can be used to transfer assets, execute actions based on certain conditions, and enforce the terms of an agreement. One of the most well-known applications of smart contracts is in the creation of decentralized autonomous organizations (DAOs). A DAO is a decentralized organization that is run by a set of rules encoded in a smart contract [8].

One of the main benefits of smart contracts is their ability to automate complex processes and reduce the need for intermediaries. For example, in the insurance industry, smart contracts can be used to automate the claims process, reducing the need for manual verification and speeding up the process. In the real estate industry, smart contracts can be used to automate the process of buying and selling property, reducing the need for intermediaries such as lawyers and real estate agents.

Smart contracts also have the potential to increase transparency and reduce fraud. For example, in supply chain management, smart contracts can be used to track the movement of goods and materials through the supply chain, providing increased transparency and traceability. This can help to improve efficiency, reduce fraud, and increase consumer trust in the authenticity of products.

However, there are also some challenges that need to be addressed before smart contracts can be widely adopted. One of the main challenges is scalability, as the current blockchain infrastructure is not able to handle the high volume of transactions required for many use cases. Additionally, there are also legal and regulatory challenges that need to be addressed, as smart contracts may not be recognized as legally binding in all jurisdictions.

In conclusion, smart contracts are a powerful tool that has the potential to revolutionize many industries. By automating complex processes and reducing the need for intermediaries, they have the potential to increase efficiency, transparency, and reduce fraud. However, there are still challenges that need to be addressed before they can be widely adopted, such as scalability and regulatory compliance.

2.3. Blockchain platforms

Blockchain platforms are the infrastructure on which blockchain applications can be built and run. There are several different types of blockchain platforms, each with their own unique features and capabilities. Some of the most well-known blockchain platforms include:

Bitcoin [1]: The first blockchain platform, created in 2008 by an unknown individual or group of individuals using the pseudonym Satoshi Nakamoto. It is a decentralized digital currency that uses a proof-of-work consensus mechanism to validate transactions.

Ethereum [8]: Launched in 2015, Ethereum is a decentralized platform that enables the creation of smart contracts and decentralized applications (dApps). It uses a proof-of-stake consensus mechanism and has its own native cryptocurrency, Ether (ETH).

Ripple [9]: Ripple is a decentralized platform that enables fast and low-cost cross-border transactions. It uses a consensus mechanism called the Ripple Protocol Consensus Algorithm (RPCA) to validate transactions.

Hyperledger [10]: An open-source collaborative effort created to advance cross-industry blockchain technologies.

It provides a range of modular blockchain frameworks and tools for building enterprise-grade blockchain applications.

EOS [11]: EOS is a blockchain platform that aims to provide a decentralized, high-performance, and low-latency platform for building dApps. It uses a Delegated Proof of Stake (DPoS) consensus mechanism and has its own native cryptocurrency, EOS.

Each platform has its own unique features and capabilities, and the choice of platform will depend on the specific use case and requirements of the application. For example, Bitcoin is primarily used as a digital currency, while Ethereum is used for creating smart contracts and dApps

2.4. Blockchain Consensus Protocols

Blockchain consensus protocols are mechanisms that are used to validate transactions and ensure the integrity of the blockchain. They are crucial to the functioning of blockchain networks, as they enable nodes in the network to reach a consensus on the state of the blockchain. There are several different types of consensus protocols, each with their own advantages and disadvantages. Some of the most well-known consensus protocols include:

Proof of Work (PoW): This is the first and most widely used consensus protocol. It was first introduced in the Bitcoin blockchain and is used to validate transactions by solving complex mathematical puzzles. The first node to solve the puzzle is rewarded with a block reward and is responsible for adding the next block to the blockchain.

Proof of Stake (PoS): PoS is a consensus protocol that aims to address the energy consumption issues associated with PoW. It validates transactions by selecting nodes to add the next block to the blockchain based on their stake, or the amount of cryptocurrency they hold [8, 1].

Delegated Proof of Stake (DPoS): DPoS is a variation of PoS in which token holders vote for a limited number of nodes to validate transactions and add blocks to the blockchain. This helps to increase the scalability of the network and reduce the risk of centralization [12].

Practical Byzantine Fault Tolerance (PBFT): PBFT is a consensus protocol that is designed to be resilient to Byzantine failures, where some nodes in the network may act maliciously. It is mainly used in private blockchain networks where the number of nodes is known and trust is established among them [13].

Raft: Raft is a consensus protocol that ensures that a network of nodes stays consistent. It is mainly used in distributed systems and it's simpler than PBFT, also it's more flexible [14].

Each consensus protocol has its own unique features and trade-offs, and the choice of protocol will depend on the specific requirements of the blockchain application. PoW is the most widely used protocol but it has a high energy consumption, PoS and DPoS are more energy efficient but have a risk of centralization, PBFT is mainly used in private blockchain networks, and Raft is mainly used in distributed systems.

2.5. Web of Things (WoT)

The Web of Things (WoT) is an emerging technology that enables the connection of physical objects to the Internet. It is a concept that has been around since the early 2000s, but has recently gained traction due to advances in communication technologies and the proliferation of connected devices. The WoT is based on a combination of existing technologies such as the Internet of Things (IoT), Semantic Web, and Web Services. It provides a platform for connecting physical objects to the Internet, allowing them to interact with each other and with users in a more meaningful way.

The WoT is an important development in the field of connected devices, as it allows for more efficient communication between devices and users. This can be used to create new applications and services that are not possible with traditional IoT solutions. For example, it can be used to create smart homes, where appliances can be controlled remotely from anywhere in the world. Additionally, it can be used for predictive maintenance, where sensors can detect potential problems before they occur and alert users or take corrective action automatically [15].

The WoT also has implications for security and privacy, as it allows for more secure communication between devices and users. By using encryption techniques such as TLS/SSL or DTLS, data sent over the WoT can be kept secure from unauthorized access or tampering. Additionally, by using authentication protocols such as OAuth or OpenID Connect, users can ensure that only authorized individuals have access to their data.

In order to realize these benefits, however, there are several challenges that must be addressed first. These include developing standards for interoperability between different systems; ensuring scalability; providing secure authentication; and protecting user privacy. Additionally, there are still many open questions about how best to implement these technologies in practice [16].

2.6. Comparing IoT and WoT: Key Differences and Similarities

IoT and WoT are both related to the concept of connecting devices to the internet, but they have some key differences.

IoT refers to the network of physical objects, such as devices and appliances, that are embedded with sensors, software, and connectivity, allowing them to collect and exchange data. IoT devices can range from smartphones and smart home devices to industrial machinery and medical equipment. The goal of IoT is to create a seamless and integrated network of connected devices that can communicate with each other and with central systems, such as cloud-based servers, to provide new levels of automation, efficiency, and intelligence [17].

WoT, on the other hand, is a specific application of IoT that focuses on connecting devices to the World Wide Web. WoT devices are designed to be easily accessible and controllable through web technologies, such as HTML, CSS, and JavaScript. WoT devices can be controlled through web browsers, and they can also be integrated with web services, such as social media and cloud storage. The goal of WoT is to make it easy for people to interact with and control the devices around them, using the same technologies and interfaces that they are already familiar with from the web [18].

Both IoT and WoT are driving the development of new technologies and standards, such as 5G networks, lowpower wide-area networks (LPWANs), and edge computing. These technologies are helping to make it possible to connect more devices to the internet, at lower cost, and with higher reliability, enabling new use cases and applications.

In summary, IoT is a broader concept that refers to the network of connected devices, while WoT is a specific application of IoT that focuses on connecting devices to the web. IoT devices can be controlled through web browsers, and they can also be integrated with web services, such as social media and cloud storage.

2.7. The need for Blockchain in WoTs

Blockchain technology has the potential to revolutionize the way data is stored and shared in the Web of Things (WoT). The WoT is a network of physical objects, such as sensors, that are connected to the internet and can communicate with each other. These objects can be used to collect data about their environment and share it with other connected devices. However, this data must be secure and reliable in order for it to be useful.

Blockchain technology provides a secure way to store and share data in the WoT. It uses a distributed ledger system which records all transactions on a public ledger that is shared among all participants in the network. This ensures that all transactions are secure and immutable, meaning they cannot be changed or deleted once they have been recorded. Additionally, blockchain technology provides an efficient way to verify transactions without relying on a central authority or third-party intermediary. This makes it ideal for use in the WoT, where trust between devices is essential for successful communication.

In addition to providing security and reliability, blockchain technology can also help reduce costs associated with managing data in the WoT. By using blockchain-based smart contracts, companies can automate processes such as payments and record keeping without having to rely on costly third-party intermediaries. This could lead to significant cost savings for companies operating within the WoT.

Finally, blockchain technology can help improve transparency within the WoT by providing an immutable record of all transactions that have taken place within the network. This could help ensure that data is not manipulated or tampered with by malicious actors, thus improving trust between devices within the network.

In conclusion, blockchain technology has great potential for use in the Web of Things due to its ability to provide secure storage and sharing of data, reduce costs associated with managing data, and improve transparency within the network.

2.8. Systematic Mapping Study

Systematic mapping is an example of evidence-based software engineering (EBSE) [19]. A systematic mapping's goal is to summarize a field of study by developing taxonomy and organizing evidences in that study. Peterson et al. [20, 21] have presented a general method for developing comprehensive maps. The procedure consists of three distinct phases: preparation, execution, and analysis and reporting. Justifying the need and scope of the mapping is the first step in planning, followed by developing and validating a protocol outlining all of the decisions that need to be made in order to carry out the mapping. The protocol identifies search terms, a search strategy, and literature sources to be used to retrieve relevant papers, as well as how and in which base found papers are selected and included in the mapping, what data must be extracted from selected papers, and how extracted data are synthesized and classified. The conducting phase involves putting into action the validated protocol developed in the planning phase. This includes retrieving papers from the identified sources, reviewing those papers to determine their relevance, extracting relevant data from the papers that were accepted, and finally synthesizing and classifying the extracted data. Visualization of data collected from main publications Interpretation of results answering of research questions Validation and documentation of mapping.

3. METHODOLOGY

In this section, we will describe the methodology used to create this map. In this study, we conduct a systematic mapping study to provide a comprehensive overview of the current state of the field of blockchain-based Web of Things (WoT) systems. The methodology used in this study is based on the guidelines provided by [21] and Felderer and Craver [20] and followed by several studies in the field of blockchain and IoT. The methodology consists of several steps. In the next subsections, we will cover each step in more detail.

As shown in Figure 1, the methodology for the systematic mapping study can be broken down into five distinct parts.

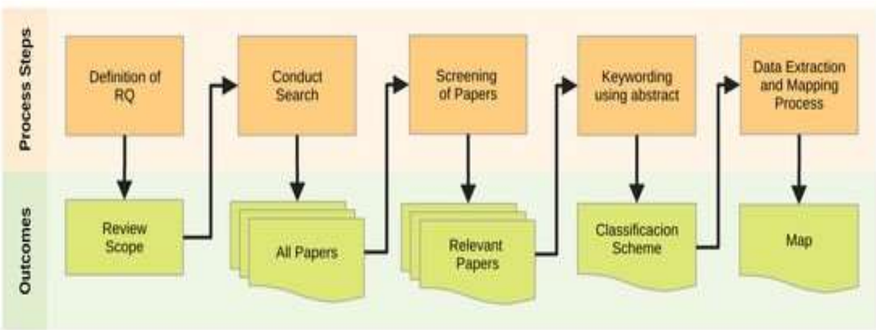

Figure 1. The process of Systematic Mapping Study [21]

3.1. Defining the research question

This research aims to establish what constitutes the current state of the art in the blockchain-based Web of Things field. We follow the recommendations of Kuhrmann et al. [21, 20] and design our research questions based on the aims of our study. There are three primary inquiries driving this research. The reasoning behind these inquiries as well as their respective aims will be outlined in the following sections.

3.1.1. Q1: What research topics have been addressed in WoT-based Blockchain techniques?”

This research question is formulated to guide the study in identifying and understanding the current state of the field of blockchain-based WoT systems. It is important to define a clear and specific research question at the beginning of the study as it helps to focus the literature search and data analysis, and ensures that the study is relevant and addresses an important area of research.

The research question is designed to provide a comprehensive overview of the current state. This includes identifying the most common research directions, the types of blockchain platforms used, and the key challenges and opportunities facing the development of these systems. By answering this research question, the study will provide a valuable resource for researchers and practitioners working in the field of blockchain and WoT, as well as for those interested in understanding the potential of blockchain technology for IoT applications.

3.1.2. Q2: How effective is the use of Blockchain in WoT?

The purpose of this question is to understand how well blockchain technology can address the key challenges faced by WoT systems, such as security and scalability, and to identify any limitations or obstacles that may need to be overcome in order to make blockchain technology suitable for use in WoT systems.

The effectiveness of blockchain technology in WoT can be evaluated by looking at its ability to provide secure and tamper-proof communication channels between devices, establish decentralized marketplaces for data and resources, and enable automation of device interactions and business processes. It can also be evaluated by looking at its scalability, energy consumption and cost, interoperability, and compliance with regulations. The question also aims to evaluate the privacy and data protection, complexity and the limited use cases of blockchain technology in WoT.

Overall, the question is trying to evaluate the suitability of blockchain technology for use in WoT systems and to identify any challenges or limitations that need to be addressed before it can be widely adopted.

3.1.3. Q3: What are the challenges of adopting blockchain in WoT?

The purpose of this question is to identify and understand the various issues that must be addressed in order to effectively implement blockchain in WoT systems.

By understanding these challenges, researchers and practitioners can work to develop solutions that can overcome these obstacles and create an efficient, secure, and effective blockchain-based WoT system. Additionally, this question helps to identify potential issues that organizations may face when they consider adopting blockchain technology in their WoT systems and also help them to take better decisions.

3.2. Identifying relevant literature

We conduct a literature search using a set of predefined keywords and inclusion criteria. The keywords used in the search include (”blockchain” AND ”Web of Things” OR ”WoT”). The inclusion criteria for the papers included in the study are: (1) peer-reviewed articles published in English, (2) articles published until 1st Feb 2023 and (3) articles that specifically address the topic of blockchain-based WoT systems.

We follow the methods outlined by Kuhrmann et al [20] to retrieve the studies that were of interest to our mapping study. Therefore, we started using the following academic databases; Scopus, IEEE Xplore, ACM Digital Library, Web of Science and Science Direct.

In addition to our automated search, we employ a recursive backward and forward snowballing technique, as proposed by Wohllin [22], on a subset of studies to ensure we don’t overlook any important ones. By using a process called”backward snowballing,” we ensure that all references in accepted papers are useful. Forward snowballing allows us to verify the significance of publications quoting accepted ones. Each accepted manuscript undergoes this snowballing process in reverse. For forward snowballing, Google Scholar is the only source used.

3.3. Classifying the literature

There were two rounds of selection applied to the collection of papers found by automated search. First, we looked at the titles and abstracts to see if anything seemed relevant. Our second step involved reading whole papers to see if they fulfilled our criteria for inclusion. Each person reviews the full list of papers independently before discussing and resolving any issues that arise. Both individuals perform their own independent reviews of any papers uncovered by snowballing that may be of interest.

The resulting set of papers is then analyzed and classified according to a set of predefined categories, including the type of blockchain used, the researching area, and the key challenges and opportunities facing the development of the system.

3.4. Analyzing the data

Using the use of the key-word method laid out in [21]. We begin by reading the abstracts of each publication to determine which ones contain the most relevant keywords and provide the most substantive research. The papers were organized by subject using the keywords that were found within them. Each document was first classified, and then we read them to see if any adjustments needed to be made to the categorization.

The data collected from the literature is then analyzed to identify the current state and trends in the field of blockchain-based WoT systems. This includes identifying the most common application areas, the types of blockchain platforms used, and the key challenges and opportunities facing the development of these systems.

3.5. Reporting the results

The results of the study are reported in a systematic and structured manner, including a summary of the main findings and a discussion of the implications of the results.

It is important to note that this systematic mapping study is focused on providing an overview of the current state of the field and is not intended to be a comprehensive review of all the literature on blockchain-based WoT systems.

4. RESULTS

Our systematic mapping study encompassed an analysis of 20 pertinent papers that explored Blockchain-based WoT. This section discusses the results of our comprehensive search and screening of relevant papers, and the subsequent classification of these papers.

4.1. Search and Screening Process

Our search and screening process, which was delineated in the previous section, unearthed a total of 70 papers that mentioned both ”Blockchain” and ”WoT”. However, a significant number of these papers (50) were deemed irrelevant based on their titles and abstracts, and hence were excluded. The primary reason for exclusion was that many of these papers did not focus on the technical aspects of Blockchain-based WoT solutions and use cases, which was the primary focus of our research. Instead, they explored the subject from a monetary or legal perspective. Additionally, papers focusing on topics like cryptocurrency, blockchain, and the Internet of Things, which did not directly relate to our research, were also excluded. After eliminating duplicates (14), we were left with 20 unique papers. Of these, 16 were disqualified because they did not make any significant contributions beyond providing background information on Blockchain, IoT, and their general operation. Consequently, our systematic mapping study was confined to the remaining 4 papers.

4.2. Classification

The 20 papers that were included in our systematic mapping study were further classified into three main categories based on their core focus: Security and Privacy, Interoperability and Scalability, and Applications.

Category	Number of Papers
Security and Privacy	7
Interoperability and Scalability	5
Applications	8

Table1. Classification of papers based on research focus

The results of our investigation are summarized in Table 1. We found that security and privacy were the most common topics, followed by applications and interoperability.

4.2.1. Security and Privacy

Security and privacy are paramount in the WoT due to the interconnectedness of various devices and networks. A significant portion of the analyzed papers proposed solutions to bolster the security and privacy of the WoT, leveraging on the distributed and immutable nature of blockchain technology and the programmability of smart contracts.

The papers highlighted the use of smart contracts-based digital twins [23, 24, 25] as a valuable approach for enhancing security. Digital twins, virtual replicas of physical devices, when encoded in smart contracts on the blockchain, can ensure the privacy and security of the data they generate and process.

Moreover, permissioned blockchains were proposed as a solution for secure and efficient digital twins in the WoT [26]. Unlike public blockchains, permissioned blockchains restrict participants in the network and validators of transactions, thereby providing enhanced privacy and security.

Another proposed solution was for secure and auditable distributed ledger technology (DLT)-based digital twins [24]. DLT, a type of decentralized database of which blockchain is an example, provides verifiable privacy and security protections due to its inherent auditability.

Furthermore, a decentralized web of trust and authentication for the IoT was proposed [27], which leverages the decentralized nature of blockchain to establish trustworthy relationships among devices. This approach addresses the challenge of ensuring the authenticity of devices and the integrity of their data.

In addition, blockchain-empowered access control frameworks for smart devices in green IoT were introduced [28]. By utilizing blockchain, these frameworks ensure that only authorized devices or users can access certain data or services, enhancing the overall security of the WoT ecosystem.

Lastly, a decentralized self-balancing architecture for the WoT using blockchain technology was presented [29]. This architecture uses blockchain to enable secure and decentralized communication among WoT devices, allowing for self-organization and self-management of the network, thus enhancing the robustness and security of the system.

4.2.2. Interoperability and Scalability

As the WoT involves a wide range of devices, systems, and protocols, interoperability and scalability are crucial for the efficient and effective operation of the network. Many research papers have focused on addressing these challenges using blockchain technology.

A number of papers proposed a decentralized self-balancing architecture for the WoT [30]. This architecture aims to enable devices in the WoT to communicate and interact with each other in a seamless and secure manner, regardless of the underlying hardware, software, or protocol used by the devices. By decentralizing the management and control of the network, this architecture can also enhance the scalability and resilience of the WoT.

In addition, a description model for heterogeneous smart devices and GUI generation was proposed [31]. This model provides a standardized way for describing the functionality and characteristics of different devices, enabling them to interact and communicate with each other more effectively. This can greatly enhance the interoperability of the WoT.

Furthermore, a blockchain infrastructure for the semantic WoT was proposed [32]. By integrating semantic technologies with blockchain, this infrastructure aims to provide a unified and standardized framework for data representation and exchange in the WoT. This can enable devices to understand and interpret the data generated by other devices, enhancing the interoperability of the WoT.

Several papers also proposed solutions for secure IoT access at scale using blockchains and smart contracts [33, 34]. By automating the management and control of access rights with smart contracts, these solutions can enhance the scalability of the WoT, allowing it to accommodate a large number of devices and users.

An implementation of a proposed food quality ensuring architecture using blockchain technologies was also proposed [35]. This architecture leverages the transparency and traceability of blockchain to enhance the reliability and trustworthiness of food quality data, while also enabling the data to be shared and accessed by various stakeholders in a secure and controlled manner.

Moreover, [36] discusses the use of the W3C Web of Things (WoT) standard to achieve interoperability between IoT devices. The authors propose a solution that enables seamless integration of different IoT devices and platforms, allowing for more efficient and effective communication and data exchange.

In addition, authors in [37] present a decentralized software framework called Devify that aims to achieve interoperability between IoT devices. The authors propose a peer-to-peer architecture that allows for easy integration and communication between different devices, while also ensuring security and privacy.

In summary, the analyzed papers showcase the potential of blockchain technology in addressing the challenges of interoperability and scalability in the WoT. However, more research is needed to further develop and refine these solutions.

4.2.3. Applications

The application of blockchain technology in the WoT spans across various real-world use cases and sectors. The analyzed papers showcased a range of innovative applications of blockchain technology in WoT, demonstrating its potential to revolutionize various industries.

One important application domain is structural health monitoring, as detailed in the study by [38]. The authors proposed a blockchain-based solution for monitoring the structural health of buildings and infrastructure. By storing the monitoring data on a blockchain, they ensure the data's integrity and verifiability, allowing for more accurate and reliable structural health assessments.

Another significant application area is resource sharing in a blockchain environment [39]. The authors proposed a context-based WoT resource sharing approach, leveraging the decentralization and transparency of blockchain to enable fair and efficient sharing of resources among devices in the WoT.

The integration of blockchain with e-commerce was also explored in [40]. The authors proposed a smart bot and e-commerce approach based on IoT and blockchain technology. This approach leverages the automation capabilities of smart bots and the security and transparency of blockchain to enhance the efficiency and trustworthiness of ecommerce transactions.

The application of blockchain in healthcare was highlighted in [41], where the authors proposed a blockchain secured health wearables solution in smart homes utilizing Raspberry Pi WoT gateways. This solution leverages the security and privacy protections of blockchain to ensure the confidentiality and integrity of health data collected by wearable devices.

Finally, [42] presents a futuristic application of blockchain in the industry sector. The authors propose a blockchain based Internet of Things (IoT) system, called BIOt, that is integrated into futuristic networking for industry. The system leverages blockchain to enhance the security and privacy of IoT devices and enable the development of new applications such as smart contracts and decentralized applications.

In conclusion, the analyzed papers demonstrate the vast application potential of blockchain technology in the WoT. However, further research is required to refine these applications and fully realize the benefits of blockchain in these contexts.

Overall, the systematic mapping study identified various solutions proposed in the literature to address the challenges of WoT based on blockchain technology. The papers proposed various solutions for security and privacy, interoperability and scalability, and different applications. However, further research is needed to evaluate the effectiveness and practicality of these solutions in real-world scenarios.

In this systematic mapping study, a wide array of solutions and applications of blockchain technology in the WoT were discovered across the categories of Security and Privacy, Interoperability and Scalability, and Applications. See Table 2. For Security and Privacy, solutions ranged from using smart contract-based digital twins to decentralized web of trust and authentication for the IoT. In the category of Interoperability and Scalability, solutions included the use of a decentralized self-balancing architecture for the WoT, the creation of a description model for heterogeneous.

Category	Proposed Solution/Application	Reference(s)
Security and Privacy	Smart contracts-based digital twins for enhanced security.	[23, 24, 25]
	Permissioned blockchains for secure and efficient digital twins.	[26]
	Secure and auditable DLT-based digital twins.	[24]
	Decentralized web of trust and authentication for the IoT.	[27]
	Blockchain-empowered access control frameworks for smart devices in green IoT.	[28]
	Decentralized self-balancing architecture for the WoT.	[29]
Interoperability and Scalability	Decentralized self-balancing architecture for the WoT.	[30]
	Description model for heterogeneous smart devices and GUI generation.	[31]
	Blockchain infrastructure for the semantic WoT.	[32]

	Secure IoT access at scale using blockchains and smart contracts.	[33, 34]
	Implementation of a proposed food quality ensuring architecture using blockchain technologies	[35]
	Use of the W3C Web of Things (WoT) standard to achieve interoperability..	[36]
	Decentralized software framework called Devify for IoT device interoperability.	[37]
Applications	Structural health monitoring.	[38]
	Resource sharing in a blockchain environment.	[39]
	Integration of blockchain with ecommerce.	[40]
	Blockchain-secured health wearables solution in smart homes.	[41]
	Futuristic application of blockchain in the industry sector (BIOt).	[42]

Table 2. Summary of proposed solutions and applications of blockchain technology in WoT

smart devices, and the use of the WoT standard to achieve interoperability. The Applications category highlighted the versatility of blockchain technology in the WoT, with applications in diverse areas such as structural health monitoring, resource sharing in a blockchain environment, and integration of blockchain with ecommerce. This review underscores the vast potential of blockchain technology in enhancing the WoT across various dimensions.

5. DISCUSSION

In this section, we delve deeper into the central research topics that have been addressed in the domain of WoT based on Blockchain, scrutinize the effectiveness of Blockchain in WoT, and discuss the challenges that hinder the adoption of blockchain in WoT.

5.1. Research Topics in Blockchain-based WoT

The integration of blockchain technology with the Web of Things (WoT) has been a subject of considerable interest in recent years. This interest hinges on the understanding that blockchain can provide a secure, transparent, and decentralized platform for managing data and resources among interconnected devices.

A major research theme in this domain is the use of blockchain for secure device communication and identity management. Given the critical role of communication in the WoT, the ability of blockchain to establish secure, tamper-proof communication channels between devices is of paramount importance. Additionally, blockchain can validate the authenticity of devices and data they produce, thereby minimizing the risk of fraudulent activities and enhancing the overall security of a WoT ecosystem.

Another key area of research revolves around the management and sharing of data and resources in a WoT setting using blockchain. Blockchain's intrinsic decentralization feature facilitates secure sharing and trading of data and resources among devices. This has the potential to create new business models and revenue streams for device manufacturers and service providers, and to promote efficient and sustainable use of resources.

The use of blockchain-based smart contracts for automating device interactions and business processes in a WoT environment is also a significant research topic. Smart contracts allow for the encoding of rules and logic of device interactions and business processes and their automatic execution. This can lead to unprecedented levels of automation and efficiency in the WoT, opening up new possibilities for application developers and service providers.

Lastly, some researchers have explored the use of blockchain for secure and decentralized device updates and management. This approach, by eliminating the need for a centralized authority, can lead to more efficient, reliable, and secure management of devices in a WoT environment.

5.2. Effectiveness of Blockchain in WoT

The deployment of blockchain technology in the Web of Things (WoT) demonstrates promising potential effectiveness in addressing some of the key challenges plaguing WoT systems, particularly those related to security and scalability.

The capability of blockchain to provide secure and tamper-proof communication channels between devices and to authenticate the devices and their generated data can significantly bolster the security of WoT systems. This enhanced security can make the systems more resilient against cyber threats, making them more reliable for users and more attractive for service providers.

Furthermore, blockchain can be used to create decentralized marketplaces for data and resources, facilitating secure sharing and trading of data and resources among devices. This can lead to the emergence of new business models and revenue streams for device manufacturers and service providers, potentially transforming the entire IoT industry.

The automation of device interactions and business processes, enabled by blockchain and smart contracts, can also significantly enhance the efficiency and effectiveness of WoT systems. This could lead to the development of new applications and use cases that were previously not feasible.

However, it is important to note that the application of blockchain technology in WoT is still in its early stages. There are significant challenges that need to be addressed, including scalability issues due to the current limitations of blockchain technology, and the cost and energy consumption associated with maintaining a blockchain-based system.

5.3. Challenges in Adopting Blockchain in WoT

While the potential of blockchain technology in the WoT is vast, its adoption is not without challenges. These challenges pertain to several aspects, including scalability, cost and energy consumption, integration with existing WoT systems, lack of standardization and interoperability, and regulatory issues.

Scalability is a significant challenge, as the current blockchain technology is not capable of handling a large number of transactions per second, a requirement for WoT systems that involve a high volume of interconnected devices. This limitation can lead to network congestion and delays, which can negatively impact the performance and usability of the WoT system.

The cost and energy consumption associated with maintaining a blockchain-based system can also pose a significant challenge. Blockchain-based systems require substantial computational power, leading to high energy consumption. This can be of particular concern for devices with limited resources, such as battery-powered devices, and also has implications for the environmental sustainability of these systems.

Integration with existing WoT systems can also present challenges, especially as many current systems were not designed with blockchain technology in mind. This can make it difficult to retrofit these systems with blockchain technology and can lead to compatibility issues, potentially requiring substantial redesign and redevelopment efforts.

The lack of standardization and interoperability among different blockchain platforms and protocols is another challenge. This lack of standardization can make it difficult to develop a seamless and integrated WoT ecosystem and can pose difficulties for communication between devices from different manufacturers.

Finally, the regulatory landscape for blockchain-based systems is still evolving. The decentralized and autonomous nature of these systems can make governance and regulation challenging, creating potential legal and compliance concerns.

6. CONCLUSION

In conclusion, this systematic mapping study has provided a comprehensive overview of the current state of research on blockchain-based WoT. The results of this study indicate that there is a significant interest in using blockchain technology to enhance the security and privacy, Interoperability of IoT devices and applications.

The most common application areas for blockchain-based WoT are supply chain management, smart cities, and industrial IoT. In the supply chain management area, blockchain technology is used to improve transparency, traceability and security of the supply chain information. In the smart cities and industrial IoT area, blockchain is used to improve the management of data, devices and their interconnection.

The most commonly studied blockchain platforms for WoT are Ethereum and Hyperledger, which are both opensource platforms that provide a wide range of tools for building blockchain-based applications. Other platforms such as IOTA, EOS, and Ripple have also been studied but to a lesser extent.

One of the key findings of this study is that there is a lack of mature and practical solutions that have been deployed in real-world scenarios. This highlights the need for further research and development in the area of blockchain-based WoT. Additionally, the integration of blockchain technology with other emerging technologies such as edge computing and 5G networks, could open up new opportunities for the development of innovative WoT solutions.

In summary, this study provides a valuable overview of the current state of research on blockchain-based WoT. It highlights the potential of blockchain technology to enhance the security, scalability, and privacy of IoT devices and applications. However, it also indicates the need for further research and development in the area, in order to bring mature and practical solutions to real-world scenarios.

Acknowledgement

The authors extend their appreciation to the Deanship of Scientific Research at Shaqra University for funding this research work through project number (ANN-SU-2023013)

References

S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Decentralized business review (2008) 21260.

C. Dong, Y. Wang, A. Aldweesh, P. McCorry, A. van Moorsel, Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing, in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 211–227.

M. B. F. B. M. AL, A. Aldweesh, et al., Blockchain-based museum asset management system, Innovative Technologica: Methodical Research Journal 3 (09) (2022) 116–127.

M. Al Osimi, A. Aldweesh, Towards designing and development of an artifact storage and trading framework utilizing the ethereum blockchain, in: 2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS), IEEE, 2022, pp. 101–104.

A. Aldweesh, M. Alharby, M. Mehrnezhad, A. van Moorsel, The opbench ethereum opcode benchmark framework: Design, implementation, validation and experiments, Performance Evaluation 146 (2021) 102168.

A. Aldweesh, A. VanMoorsel, A survey about blockchain software architectures, in: 32nd Annual UK Performance Engineering Workshop & Cyber Security Workshop-2016,

Newcastle University, 2016. 13
N. Szabo, Smart contracts: Building blocks for digital markets. 1996, URL: http://www. fon. hum. uva. nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo. best. vwh. net/smart contracts 2. html (: 30 2018 .).
V. Buterin, A next-generation smart contract and decentralized application platform, Ethereum White Paper, 2014.
D. Schwartz, N. Youngs, A. Britto, et al., The ripple protocol consensus algorithm, Ripple Labs Inc White Paper 5 (8) (2014) 151.
C. Cachin, et al., Architecture of the hyperledger blockchain fabric, in: Workshop on distributed cryptocurrencies and consensus ledgers, Vol. 310, Chicago, IL, 2016, pp. 1–4.
B. Xu, D. Luthra, Z. Cole, N. Blakely, Eos: An architectural, performance, and economic analysis, Retrieved June 11 (2018) 2019.
F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, M. Zhou, Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism, IEEE Access 7 (2019) 118541–118555.
D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm, in: 2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14), 2014, pp. 305–319.
M. Castro, B. Liskov, et al., Practical byzantine fault tolerance, in: OsDI, Vol. 99, 1999, pp. 173–186.
R. Sardar, T. Anees, Web of things: Security challenges and mechanisms, IEEE Access 9 (2021) 31695–31711. doi:10.1109/access.2021.3057655.
URL https://doi.org/10.1109/access.2021.3057655
L. Sciullo, L. Gigli, F. Montori, A. Trotta, M. D. Felice, A survey on the web of things, IEEE Access 10 (2022) 47570–47596. doi:10.1109/access.2022.3171575.
URL https://doi.org/10.1109/access.2022.3171575
L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54 (15) (2010) 2787–2805.
D. Guinard, V. Trifa, F. Mattern, E. Wilde, From the internet of things to the web of things: Resource-oriented architecture and best practices, in: Architecting the Internet of Things, Springer Berlin Heidelberg, 2011, pp. 97–129. doi:10.1007/978-3-642-19157-25.
B. A. Kitchenham, D. Budgen, P. Brereton, Evidence-based software engineering and systematic reviews, Vol. 4, CRC press, 2015.
M. Felderer, J. C. Carver, Guidelines for systematic mapping studies in security engineering, in: Empirical Research for Software Security, CRC Press, 2017, pp. 47–68.
K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, Systematic mapping studies in software engineering, in: 12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12, 2008, pp. 1–10.
C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: Proceedings of the 18th international conference on evaluation and assessment in software engineering, 2014, pp. 1–10.
I. Pittaras, N. Fotiou, C. Karapapas, V. A. Siris, G. C. Polyzos, Secure,

mass web of things actuation using smart contracts-based digital twins, in: 2022 IEEE Symposium on Computers and Communications (ISCC), IEEE, 2022.

I. Pittaras, G. C. Polyzos, (POSTER) SmartTwins: Secure and auditable DLT-based digital twins for the WoT, in: 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), IEEE, 2022.

I. Lopez-Arevalo, J. L. Gonzalez-Compean, M. Hinojosa-Tijerina, C. Martinez-Rendon, R. Montella, J. L. Martinez-Rodriguez, A WoT-based method for creating digital sentinel twins of IoT devices, Sensors (Basel) 21 (16) (2021) 5531.

I. Pittaras, G. C. Polyzos, Secure and efficient web of things digital twins using permissioned blockchains, in: 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), IEEE, 2022.

A. Durand, P. Gremaud, J. Pasquier, Decentralized web of trust and authentication for the internet of things, in: Proceedings of the Seventh International Conference on the Internet of Things, ACM, New York, NY, USA, 2017.

L. Tan, N. Shi, K. Yu, M. Aloqaily, Y. Jararweh, A blockchain-empowered access control framework for smart devices in green internet of things, ACM Transactions on Internet Technology (TOIT) 21 (3) (2021) 1–20.

I. Thomas, S. Kikuchi, E. Baccelli, K. Schleiser, J. Doerr, A. Morgenstern, Design and implementation of a platform for hyperconnected cyber physical systems, Internet of Things 3-4 (2018) 69–81.

A. Tosiˇ c, J. Vi´ ciˇ c, M. Mrissa, A blockchain-based decentralized self-balancing architecture for the web of things, in: Communications in Computerˇ and Information Science, Communications in computer and information science, Springer International Publishing, Cham, 2019, pp. 325–336.

L. Baresi, M. Sadeghi, M. Valla, TDeX: A description model for heterogeneous smart devices and GUI generation, in: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018.

M. Ruta, F. Scioscia, S. Ieva, G. Capurso, A. Pinto, E. Di Sciascio, A blockchain infrastructure for the semantic web of things., in: SEBD, 2018.

N. Fotiou, I. Pittaras, V. A. Siris, S. Voulgaris, G. C. Polyzos, Secure IoT access at scale using blockchains and smart contracts, in: 2019 IEEE 20th International Symposium on “A World of Wireless, Mobile and Multimedia Networks” (WoWMoM), IEEE, 2019.

S.-Y. Wang, Y.-J. Hsu, S.-J. Hsiao, Integrating blockchain technology for data collection and analysis in wireless sensor networks with an innovative implementation, in: 2018 International Symposium on Computer, Consumer and Control (IS3C), IEEE, 2018.

P. S. Sujan, R. Ashok, S. C. Mana, B. K. Samhitha, J. Jose, An efficient implementation of a proposed food quality ensuring architecture using blockchain technologies, in: Lecture Notes in Electrical Engineering, Lecture notes in electrical engineering, Springer Nature Singapore, Singapore, 2021, pp. 715–723.

M. Lagally, M. McCool, IoT interoperability with W3C web of things, in: 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2022.

J. Chen, Devify: Decentralized internet of things software framework for a peer-to-peer and interoperable iot device, ACM SIGBED Review 15 (2) (2018) 31–36.

L. Gigli, L. Sciullo, F. Montori, A. Marzani, M. Di Felice, Blockchain and web of things for structural health monitoring applications: A proof of concept, in: 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2022.

Y. Li, J. Qi, L. Min, H. Yang, C. Zhou, B. Jin, CWoT-share: Context-based web of things resource sharing in blockchain environment, Comput. Mater. Contin. 72 (3) (2022) 5079–5098.

A. Madhu, K. Archana, D. H. Kulal, R. Sunitha, P. B. Honnavalli, Smart bot and e-commerce approach based on internet of things and block-chain 14

technology, in: 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, 2020.

S. H. Kembo, P. Mpofu, B. T. Mukorera, S. Jacques, Blockchain-secured health wearables in smart homes utilising raspberry pi web of things gateways, in: 2nd African International Conference on Industrial Engineering and Operations Management, IEOM 2020, 2020, pp. 2269–2280.

I. Pittaras, G. C. Polyzos, (POSTER) SmartTwins: Secure and auditable DLT-based digital twins for the WoT, in: 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), IEEE, 2022.