Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 09, No. 03, September 2023.

CONTAINER-BASED VIRTUALIZATION FOR BLOCKCHAIN TECHNOLOGY: A SURVEY

Nawar A. Sultan and Rawaa Putros Qasha

(Received: 29-Apr.-2023, Revised: 29-Jun.-2023, Accepted: 19-Jul.-2023)

ABSTRACT

Blockchain technology has garnered interest in several scientific and engineering fields. To improve blockchain-technology services, its execution challenges must be addressed. Container-based virtualization enables running isolated apps on a shared OS where blockchain technology can leverage this technology to run numerous nodes, smart contracts and decentralized apps in distinct containers allowing resource isolation and allocation, faster deployment and scalability and improved security through limited host OS and other container access. This article covers container-based virtualization for blockchain technology, including current methodologies, prospects and future perspectives. Initially, this study explains blockchain and containerization, as well as the reason for their integration. Then, reviews container virtualization services to address blockchain complexity, size, scalability and security. Conversely, container technology uses blockchain to protect data and enhance resource management. Next, it analyzes the latest containerization and blockchain integration studies. Finally, difficulties and future directions are considered to advance this promising research.

KEYWORDS

Container-based virtualization, Blockchain, Virtual machines, Docker, Kubernetes.

1. INTRODUCTION

In recent years, big data has gained immense significance, becoming a driving force behind the evolution of data processing, storage and management [1]. As a result, the demand for innovative technologies capable of meeting the growing challenges of big data has surged. This has led to the emergence and widespread adoption of containerization and blockchain, which have revolutionized the landscape of data management and security [2].

While blockchain technology offers decentralized and secure data management [3], container technology provides a simplified and scalable solution for system and application management [4]. The rise of cryptocurrencies like Bitcoin, Ripple and Ethereum has further propelled the need for blockchain technologies [1]. As such, the integration of containers with blockchain applications has become a critical area of research and development.

Blockchain technology can be implemented in virtual machines or containers, depending on the blockchain application's specific use case and requirements. Virtual machines can provide complete isolation between nodes in a blockchain network, making them a good choice for building private or permissioned blockchains, where security and data privacy are paramount. Each node can be deployed in a separate virtual machine with its operating system and resources, ensuring that any compromise or failure in one node does not affect the others [5].

Containers, conversely, are more lightweight and can be deployed more easily and quickly than virtual machines. They are a good choice for building decentralized applications that run on top of public blockchains, such as Ethereum. Each application can be packaged in a container and deployed to a decentralized network, where it can interact with other smart contracts and blockchain nodes [6]. In general, the choice between virtual machines and containers for blockchain applications depends on the application's specific use case and requirements. Security, scalability, portability and resource usage should be considered when choosing between these technologies [5].

Therefore, the most notable benefits of containerizing blockchain applications should be discussed to demonstrate the viability of doing so:

1) Efficiency in reducing costs through sharing resource features, where tens of containers can rapidly be virtualized to run on a single-core CPU [7].

N. A. Sultan and R. P. Qasha are with Department of Computer Science, University of Mosul, Mosul, Iraq. Emails: nawar.20csp62@student.uomosul.edu.iq and rawa_qasha@uomosul.edu.iq

2) Portability, containers are known to be genuinely built once and run software anywhere. This is achieved with the aid of platforms like Docker that facilitates the deployment process [8].
3) Improved security, as mentioned above, as containerization is an isolation technique; this allows apps to operate independently from each other and from the host system [9].
4) Agility and containerization facilitate the integration process, allowing developers to deliver the required enhancements rapidly [5].
5) Ease of management; with a container's orchestration platform like Kubernetes, it is easier to install, upgrade and manage containers [10].

Despite the growing interest and implementation of containerization in blockchain applications, there remains a need for a comprehensive study to address several shortcomings and challenges. This study aims to bridge the gap in the existing literature by exploring the benefits and limitations of containerizing blockchain applications, with a focus on improving the overall performance.

While blockchain technology and containers have many benefits, they also have restrictions and potential drawbacks when choosing these technologies for a particular use case. Careful planning and evaluation are necessary to ensure that the chosen technology meets the specific needs and requirements of the application. In the next sections, we focused on the importance of containers and blockchain technology and the role of containers in improving the performance of the blockchain. The literature review is structured as in Figure 1.

2. CONTAINER-BASED VIRTUALIZATION AND BLOCKCHAIN: AN OVERVIEW

In this section, we present a container-based virtualization overview, Docker and its orchestration mechanism, followed by an overview of blockchain technology.

2.1 Container-based Virtualization

Containers are lightweight executable packages for software codes that encapsulate these software codes with only the required operating-system libraries and dependencies in a way that abolishes the need for a specific infrastructure to run [11]. Over the last few years, containers gained maturity and popularity because of the lightweight virtualization that they provide, which enabled multiple applications to run independently and isolated from any other application and from the operating system and without the need for occupying the operating-system kernel entirely for each one of them, as it is the case with virtual machines [12]. Rather, containerization enables sharing the host operating-system kernel with multiple containers simultaneously. This sharing feature utilizes resource employment in a way that reduces the amount of the required hardware resources. Moreover, containers are easier to manage than VMs (virtual machines), thanks to their orchestration engines like Kubernetes, which influenced the emergence of many container cloud platforms [13]. Containerization, which is container virtualization, refers to creating an isolated virtual environment for each application, which is directly related to kernel functionalities. Figure 2 shows the process of shifting from VMs to containers, where each virtual environment is named a container and both namespaces and (cgroups) refer to functions provided by the operating-system kernel. The namespaces control and limit each process's number of resources used, while (cgroups) deal with a process group's resources [14].

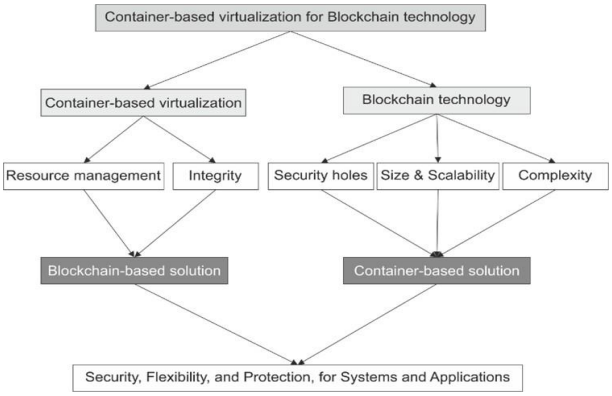

Figure 1. The structure of the literature review.

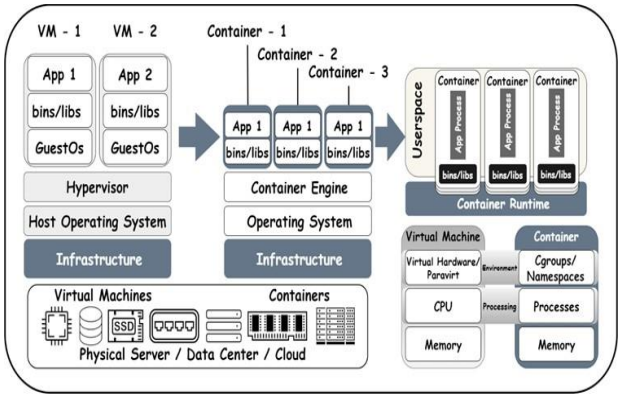

Figure 2. From virtual machines to containers.

System solutions based on hypervisor suffered many drawbacks related to resource allocation, start-up time and adaptability [15]. Currently, Docker is the most widely used virtualization tool, because it significantly increases operating system resource usage with little additional overhead. The open-source containerization engine called Docker automates the packing, shipping and deployment of software applications. These programs are delivered as thin, portable, self-contained containers that may operate almost anywhere. A Docker container is a program container that includes the constituents required for the program to run automatically [16]. A single system may contain several Docker containers and each container is totally independent of the host machine. Particularly, the software component and all of its needs are included in a Docker container, such as binaries, libraries, configuration files, scripts, jars, …and so on [17]. The following elements make up the majority of the Docker solution:

1) The Docker engine.
2) The Docker hub.

The Docker engine makes it possible to realize both general-purpose and purpose-specific Docker containers. A fast way to expand the set of Docker phases that may be gathered in different ways to make publicly-discoverable, network-accessible and exceedingly-consumable containers is *via* the Docker hub [14].

Let's say that we wish to execute the containers directly on a Linux computer. The diagram in Figure 3 shows how the Docker engine creates, oversees and manages many containers [17].

Container-based Docker ecosystem has the following characteristics [18]:

1) It supports portability by allowing for the packaged app to run anywhere, since it facilitates and improves the processes of the application's development and deployment, which makes it easy to build, ship and run any app and everywhere.
2) It strengthens the integrity of any infrastructure by enabling developers to package the application with all its necessary libraries and dependencies to build up workable software that works properly in any environment without the need for any prior setup.
3) It is easy to manage Docker by anyone in a way that meets the required additional features [19].

The Docker engine, which creates and runs containers and the Docker hub, which presents a cloud service for distributing containers, are the two distinct parts of the Docker platform [20].

Few Docker containers on a single system are easy to manage, but challenges arise when having to put these containers into production on a dispersed host network; therefore, tools for ensuring availability, scaling, networking, integration and administration are essential for managing dynamic containers as one entity on a network, where manual handling is impossible in this case [13].

Therefore, tools like Google Kubernetes, Marathon (a framework for Mesos), CoreOS's Fleet and Docker's swarm tooling are essential for managing containers on a network system. Each container needs on-host placement, monitoring and updating and at the same time, the system must be enabled to respond to failures, loading or any change in the system by taking the appropriate action by either moving, starting or aborting any container [21].

2.2 Blockchain Technology

Blockchain is a decentralized and distributed digital ledger that records transactions and stores data across a network of computers. It operates using a consensus mechanism that allows multiple parties to verify and agree on the validity of transactions without needing a trusted intermediary or central authority [22].

Each block contains a record of several transactions, as well as a unique cryptographic hash that identifies the block and links it to the previous block in the chain [23]. This creates an immutable and tamper-proof record of all the transactions on the blockchain [24].

One of the key benefits is that blockchain enables trust and transparency in a digital world without the need for intermediaries. Transactions are verified and recorded by a network of nodes, each with a copy of the blockchain. This ensures that any attempted tampering or fraud is easily detected and prevented [25].

Another key benefit of blockchain technology is that it can be used to create smart contracts; self-executing contracts with the terms of the agreement written into the code (see Figure 4). Smart contracts can automate the execution of transactions and eliminate the need for intermediaries, reducing costs and increasing efficiency [26].

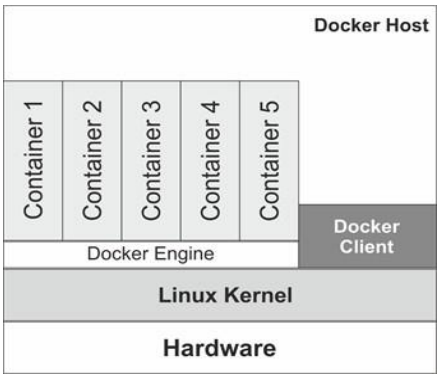

Figure 3. Docker engine.

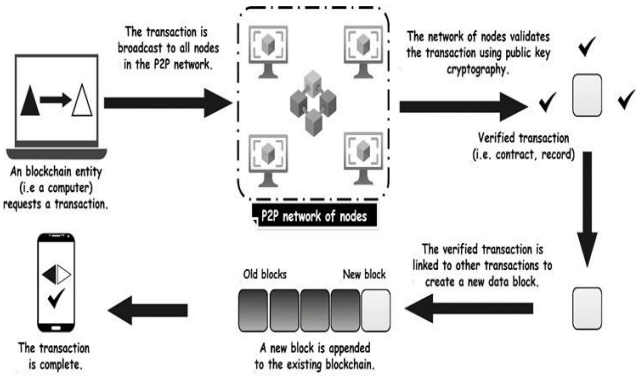

Figure 4. Contract creation by blockchain.

Blockchain technology has many potential use cases, including:

Cryptocurrencies: The underlying technology behind cryptocurrencies includes Bitcoin and Ethereum. These digital currencies use blockchain to enable secure, decentralized transactions without the need for intermediaries, like banks or financial institutions [27]. Supply-chain management: can track and verify the movement of goods and products across a supply chain. This can increase efficiency, reduce fraud and improve transparency in the supply chain [28].

Voting systems: Blockchain technology can create secure and transparent voting systems that eliminate the risk of tampering or fraud [29]. Identity verification: Blockchain technology can create decentralized and secure identity verification systems that eliminate the need for intermediaries, like government agencies or financial institutions [30]. However, blockchain technology also has some limitations and potential drawbacks. These include [31]:

Scalability: Blockchain technology can be slow and resource-intensive, especially when running on a large scale.

Energy consumption: The process of verifying transactions on a blockchain can be energy-intensive, leading to concerns about the environmental impact of blockchain technology.

Specialized infrastructure and software: Blockchain technology requires specialized infrastructure and software to run effectively, which can increase the cost and complexity of deployment.

Overall, blockchain technology represents a promising and innovative approach to sharing and verifying information in a secure and decentralized manner. While it has some limitations and potential drawbacks, careful evaluation and planning can help ensure that blockchain technology is used effectively and appropriately for a given use case [32].

3. Motivation for Integrating Container-based Virtualization and Blockchain

The challenges of adopting container-based virtualization, the technical constraints of blockchain and the promising opportunities of combining such two technologies are highlighted in this section as the driving forces behind the integration of container-based virtualization and blockchain technologies.

3.1 Challenges with Container-based Virtualization

Despite being the next revolution in cloud computing, containers are lighter than virtual machines. In comparison to conventional VMs, they may significantly reduce the start-up time for instances, as well as the processing and storage overhead [12]. However, like many other things, using and deploying containers presents particular difficulties for developers. CNCF Survey 2020, published in https://www.cncf.io/reports/cloud-native-survey-2020/, revealed that development teams encountered difficulties with several containerization-related issues (Figure 5).

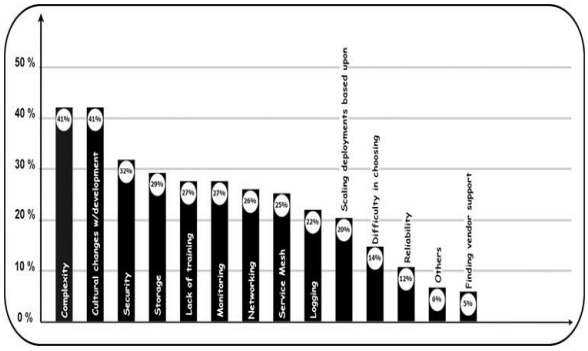

Figure 5. Challenges in using/deploying containers.

The survey showed that for (41%) of respondents, complexity was recorded to be the top challenge of containers' usage and deployment. Security came in the second place and recorded (32%) of respondents, followed by storage (29%) and lack of training and monitoring (both at 27%).

3.2 Technical Limitations of Blockchain

Despite its numerous advantages, blockchain technology has some technical limitations that need to be addressed [31]:

Scalability: As the number of transactions increases, the size of the blockchain grows, making it difficult to store and process large amounts of data. This issue becomes particularly problematic for public blockchains that require nodes to store the entire history of the chain [2].

Speed: The time it takes to validate transactions and add them to the blockchain can be slow, particularly for large networks. This is due to the fact that each transaction needs to be verified by multiple nodes in the network [33].

Cost: The cost of running a node on the network and participating in the consensus process can be high.

This is particularly true for proof-of-work blockchains, which require significant amounts of computing power and energy [25].

Interoperability: Different blockchain networks use different protocols, which can make it difficult for them to communicate with one another. This limits the potential for blockchain to be used for large-scale applications that require interoperability between different systems [34].

Security: While blockchain is considered to be a secure technology, it is not immune to hacking or other security breaches. Additionally, the use of smart contracts on blockchain networks can introduce additional security risks if they are not properly coded or audited [35].

Governance: The decentralized nature of blockchain can make it difficult to reach a consensus on changes to the network. This can lead to governance challenges and delays in implementing necessary updates or improvements [36].

3.3 The Integration of Container-based Virtualization and Blockchain Possibilities

There are several potential possibilities for integrating blockchain and container-based virtualization, some of which are outlined below:

Immutable container images: Blockchain technology can create a tamper-proof and immutable ledger of container images. This can help ensure the authenticity and integrity of container images and prevent unauthorized modifications or tampering [20].

Smart contract-based container management: Smart contracts can be used to automate the deployment and management of containerized applications. This can help simplify the container-management process and reduce the risk of errors and misconfiguration [37].

Also, to improve the scalability of blockchain technology, here are some possibilities:

Containerized blockchain nodes: Using container-based virtualization, deploying multiple blockchain nodes on a single machine or cluster of machines is possible. Distributing the workload across multiple nodes can help improve the blockchain network's performance and scalability [33].

Consensus algorithm optimization: Container-based virtualization can be used to optimize the consensus algorithm of the blockchain network by deploying multiple nodes with different consensus algorithms and testing their performance. This can help identify the optimal consensus algorithm for the blockchain network [38].

Overall, integrating container-based virtualization and blockchain technology can help improve blockchain networks' scalability and performance, enabling them to handle increased traffic and usage and support large-scale applications.

3.4 Feasibility of Integrating Container-based Virtualization and Blockchain

The integration of container-based virtualization and blockchain is a feasible and promising approach to improve the scalability, security and flexibility of blockchain networks. Container-based virtualization can help isolate different components of the blockchain network, allowing them to run in separate containers and reducing the risk of vulnerabilities or attacks affecting the entire network [7].

Furthermore, by using container-based virtualization, it is possible to deploy multiple instances of blockchain nodes with different consensus algorithms, allowing for easier testing and optimization of the blockchain network's performance. This approach can also enable more efficient resource utilization and better management of the network's computational resources [38].

While challenges must be addressed, the feasibility of integrating container-based virtualization and blockchain is high. The potential benefits make it a promising approach for the future of blockchain technology.

4. LITERATURE REVIEW

Through this survey, we touched on the strengths and weaknesses of both technologies and what the best solutions and procedures were that could be followed to achieve the best integration between them. There is a lot of research on the blockchain or its services, specifically given that the technology is open-source and has been used in bitcoins for about fourteen years. Still, there are only a few papers that discuss how to improve blockchain using containerization technology or how they can be incorporated. We have noticed through previous studies that there are major weaknesses in blockchain technology that can be addressed or improved through container technology, which can be summed up into three groups (complexity, size and scalability, and security holes).

4.1 Complexity

Zeadally and Abdo [39] [24] provided a performance-evaluation mechanism to aid in the decision-making of blockchain-based service planners. For portability and flexibility, this system is available as Docker and Kubernetes. This study's experimentation method enables service providers to assess the server performance necessary for the service's launch. Additionally, because of Docker and Kubernetes power, the experimental environment enables creators to create scenarios, like deploying several servers and replicating as many client pods as they like.

This study presents the initial review by Chen, C. et al. [6] on how decisions in blockchain design affect performance. Then, they provided their approach for employing containerization to test blockchains. In this approach, authenticity and the expensive test of P2P applications were balanced. Finally, they put their framework into action to perform a demo assessing how the characteristics of Bitcoin's network would affect system dependability. Because of this, they discovered three benefits of employing containerization for blockchain: authenticity, ease of deployment and low cost.

Minichain, a container-based emulator for testing blockchains utilizing a proof-of-work mechanism, was proposed by Wu, X. et al. [39]. Minichain offers a realistic and adaptable network environment which is absent from current blockchain experiments.

A realistic study is expensive and time-consuming, because no agreed paradigm exists for evaluating permissioned blockchain platforms' scalability and comparing consensus algorithms' performance and features. Mazzoni, M., Corradi A. and V. Di Nicola examined the Quorum blockchain's functional scalability and application [35]. They presented a framework for any permissioned blockchain technology, even though they reviewed a financial use case. They chose Hyperledger Caliper for

benchmarking and Docker for deployment for repeatable, cross-platform and cost-effective analysis.

4.2 Size and Scalability

Pongnumkulet et al. [40] conducted a study, in which two famous blockchain platforms were examined in terms of performance: Hyperledger Fabric and Ethereum. Hyperledger Fabric a private (permissioned) blockchain implementation, is designed to serve as a building block for blockchain applications in a variety of sectors. As a result, its design is modular, enabling plug-and-play compatibility for parts, like consensus and membership services. To assess the performance and constraints of these cutting-edge platforms, the study used container technology (Docker) to allow Ethereum (private deployment) and smart contracts, also known as "chaincode," which make up the application logic of the system, because one common objection to existing blockchain technology is its inability to scale. Consequently, there are two objectives for this preliminary performance review. The development of a blockchain-platform evaluation methodology comes first. The analytical results are also shared with practitioners to help them understand how to integrate blockchain technology into their IT systems. According to the testing results, which were based on different quantities of transactions, Hyperledger Fabric regularly surpasses Ethereum in terms of execution time, latency and throughput.

Current blockchain designs need to scale due to exponential message and memory complexity. Researchers presented (Hassanzadeh et al. [41]) LightChain, the first fully decentralized Distributed Hash Table (DHT)-based blockchain architecture, to address operational scalability challenges. They created a containerized model of a LightChain node system that can be run on a single computer, improving repeatability.

To address blockchain workload changes. Z. Shi et al. [42] recommended the high-performance Kubernetes scheduling technique HPKS for offline workload management. HPKS reduces worker node consumption by 13.0% in PoS blockchain applications. Compared to Kubernetes' default scheduler, Makespan's HPKS increase is less than 3%.

Volpe et al. proposed a blockchain-based smart-contract architecture for manufacturing digital processes [43]. Their key contribution is integrating blockchain with Cloud Storage and Docker, two well-known technologies.

4.3 Security Holes

Using W3C-PROV Data Model, El Ioini, N. and Pahl, C. [44] suggested a container-based blockchain architecture that tracks the sources of all orchestration choices made by a business network. This architecture offers fresh ways for many parties to communicate, enabling secure transactions and creating a new decentralized interaction paradigm for IoT-based applications.

A thorough analysis of blockchain-based trust techniques in cloud-computing systems was carried out by Li, W. et al. [18]. Using a novel method of cloud edge trust management and a cloud transaction model based on double-blockchain structures, they were able to identify the remaining challenges. They offered suggestions for additional research in this area.

Concerning container technology, we noted its reliance on blockchain technology to protect container data from tampering and maintain its integrity, in addition to making use of it to improve the efficient resource-management process.

Brinckman et al. [16] conducted a study, where many applications in research, science and industry have been stimulated by the introduction of such lightweight environments (containers), making it possible to share, reuse and instantiate pre-configured operating environments as needed. Currently, centralized repositories (such as Docker hub) have made it possible to share containers, which serves as the foundation for future growth. The researchers look at whether a distributed group of users can safely exchange container- based programs and provide an audit trail showing what has been shared and with whom. They conducted a comparison of blockchain technologies for this use case while taking into account the features of these blockchain technologies for this purpose. The majority of research was reviewing and categorizing various ledger systems.

Tosh et al. [45] stated that cloud data provenance must be secure against malicious actors. The researchers proposed a blockchain-based data provenance architecture (BlockCloud) that integrates a

proof-of-stake (PoS)-based consensus protocol to securely record data operations in a cloud environment powered by a novel PoS consensus model (CloudPoS). Validators are cloud-computing stakeholders. Rewarding involvement or securing collaboration may drive such engagement. Because participants' resources are at stake, the suggested leader-election procedure gives every cloud user an equal chance of leading the Blockchain based on the number of resources staked. Hence, blockchain activity is safer.

In a study by Marko et al. [37], resource-use optimization in a commercial setting is studied using a home- built video-conferencing (V.C.) system. All parties involved, including end users, cloud-service providers, software developers, …etc., are not provided with monetization alternatives by this type of application. Related to the technology of blockchain, Smart Contracts (SCs) may be able to help with some of these requirements. A unique architecture is provided for monetizing value generated in accordance with the desires of the stakeholders who take part in joint software service offers.

A revolutionary "permissioned Hyperledger Fabric blockchain containerized cloud ecosystem" was proposed by Awuson-David et al. [46] to protect and maintain the veracity of digital proof during both storage and transmission. Then, a "Dockerized private blockchain cloud ecosystem architecture" was designed and implemented, which would decrease the challenges faced by forensic investigators in the cloud ecosystem by ensuring evidence integrity in a multi-tenancy, private cloud environment.

J. Sun et al. [20] depending on blockchain technology, developed a container cloud security system in response to the susceptibilities and malware in container imageries in addition to specific incorrect settings that breach security-compliance standards.

Marques et al. [48] [14] described how containerization's flexibility made system monitoring harder due to the huge volume of calls and (de) allocations. This study investigated how documenting these activities in a blockchain-based data structure could simplify resource audits and procedure-order analytics. Blockchains allow container-based solution creators, end users and vendors more trust in record integrity. To meet their needs for security, flexibility and protection, numerous systems and applications have benefited from the integration of the two technologies.

Vorakulpipat, C. and Chaisawat, S. [29], in order to provide data security and flexibility in system integration, developed a system design architecture. By monitoring the use of computer resources and performing performance tests on the design, it was further examined and evaluated to confirm that it complied with the aforementioned requirements.

Aujla, G. S. et al. [47] developed a blockchain-based secure data processing system that creates a multi-objective optimization problem for an edge-envisioned vehicle-to-everything (V2X) scenario. It also features an ideal container-based data-processing scheme and a blockchain-based data integrity-management scheme to reduce latency and connection breakage.

According to Kumar, P. and Shah, M. [48], obtaining an accurate birth certificate for any individual is a significant challenge. The researchers presented and created a birth certificate storage system based on the "InterPlanetary File System" (IPFS) and "BLOCKCHAIN" technology in this paper. Due to the advancement of Docker technology and containerization as a service, this application was also deployed inside a container using Docker-compose, which creates a multi-container Docker application (CaaS).

Table 1 summarizes the issues that researchers face when fusing blockchain with containers, along with solutions for each technology.

Table 1. Literature review.

Ref.	**Research Problem**	**Challenges Faced by Blockchain/Containerization**	**Solutions Provided by Blockchain/ Containerization**
[39][24]	Portability and flexibility in the blockchain	Measuring the performance that aids in decision-making for service planners using blockchain technology	Docker and Kubernetes for portability and flexibility
[16]	Sharing container-based applications securely	Sharing container-based programs safely across a decentralized group of users while keeping track of who has shared what and with whom by using an audit trail	Blockchain technologies

[40]	Scalability of blockchain technology.	Methodology for evaluating a blockchain platform	Containerization-based
[6]	Testing blockchains	Traditional testing has issues with being unconvincing or expensive	Using containerization for Blockchain for testing, easing deployment, lowering cost and authenticity
[45]	Preserving tamper-resistant data provenance in the cloud	Making containerisation more secure	Blockchain-based data provenance architecture
[44]	Trustworthy transactions	Identifying each device/data in the network and tracking the provenance of its actions	Blockchain container-based architecture
[39]	Testing proof-of-work-based blockchains	A platform for realistic testing and evaluation of blockchain systems and applications	Container-based emulator
[37]	Providing monetization possibilities to all involved stakeholders in the video-conferencing (VC) system	Optimization of resource use for container-based video conferencing in a business context	Smart contracts
[46]	Integrity and confidentiality of data in a cloud environment	Reducing the difficulty of acquiring evidence in the cloud	Dockerized private blockchain cloud ecosystem architecture
[20]	Viruses and vulnerabilities in container images	Container cloud security enhancement	Systembased on blockchain technology
[41]	Challenges with scalability in blockchain architectures	Due to its asymptotic message and memory complexity, blockchain architectures face scalability issues	A containerized LightChain system proof-of-concept implementation
[29]	Delivering data security and agility in system integration		Using container technology along with blockchain technology
[47]	Securing data processing	The privacy of user data/activities	Using container technology along with blockchain technology
[48]	Identifying the correct birth certificate of any person		Using container technology along with blockchain technology
[18]	Building a trust-enabled transaction environment		A double- blockchain structure-based cloud transaction model
[43]	Integration of blockchain with containerization and cloud storage	Collaboration in the cloud when offering and consuming different services is a shortcoming of the blockchain	Docker and cloud storage
[48] [14]	Flow of calls and (de)allocations in massive amounts in container-based virtualization	System monitoring in container-based virtualization	Blockchain-based solution
[42]	Addressing the characteristics of PoS(Proof of Stake) blockchain applications in the cloud	Workload changes in blockchain applications	Kubernetes container orchestration
[44]	Choosing which blockchain technology and consensus algorithm best fit a specific use case is complex	Permissioned blockchain platforms need a common framework for evaluating scalability	Docker as a deployment tool

4.4 Shortcomings of Previous Studies

Previous studies' efforts in the field have provided valuable insights into the application of blockchain and container technologies. However, these studies have often lacked a detailed examination of the specific challenges associated with integrating containers into blockchain environments. Consequently, there is a need for a more focused investigation to address the following shortcomings:

1) Limited exploration of performance enhancements: Previous studies have primarily focused on the general benefits of containerization and blockchain technology without thoroughly investigating how containerization can improve the performance of

blockchain applications. The impact of containerization on scalability, resource utilization and overall efficiency requires deeper analysis.

2) Inadequate examination of security considerations: While containerization offers enhanced security through isolation, there is a need to explore the potential vulnerabilities and risks associated with deploying containerized blockchain applications. A comprehensive understanding of the security implications is crucial for ensuring the integrity and privacy of blockchain networks.
3) Insufficient evaluation of deployment and management challenges: Previous studies have often overlooked the complexities involved in deploying and managing containerized blockchain applications. The effective orchestration of containers, integration with blockchain networks and efficient resource allocation require careful consideration to maximize the benefits of containerization.

By addressing these limitations and delving into the specific challenges associated with containerizing blockchain applications, this study aims to provide a comprehensive understanding of the potential improvements that can be achieved. The following section will explore the benefits of containerization, such as cost reduction, portability, enhanced security, agility and ease of management, thereby highlighting the viability and significance of integrating containers with blockchain technology. Table 2 summarizes the aims and rationale of this survey in the context of previous works.

Table 2. Aims and rationale of the current survey.

Research Aspect	**Previous Works**	**Aim and Rationale**
Aim and Rationale	Limited exploration of containerization's impact on blockchain performance	Investigating how containerization can enhance scalability, resource utilization and overall efficiency in blockchain applications
Security Considerations	Inadequate examination of security implications of containerized blockchain applications	Analyzing the potential vulnerabilities and risks associated with deploying containerized blockchain applications to ensure data integrity and privacy
Deployment and Management	Insufficient evaluation of deployment and management challenges	Exploring the complexities involved in deploying and managing containerized blockchain applications, focusing on effective orchestration, integration with blockchain networks and efficient resource allocation

5. CONTAINER-BASED VIRTUALIZATION ROLES FOR BLOCKCHAIN ENHANCEMENT

Container-based virtualization enhances blockchain technology by addressing various research issues and providing valuable solutions. The following points provide a more detailed elaboration on the research issues related to container virtualization for blockchain technology:

Scalability: One of the key challenges in blockchain networks is scalability. As blockchain networks grow, the number of transactions being processed increases and the scalability challenge arises in ensuring that the network can handle the expanding workload efficiently. Public blockchains, in particular, face scalability concerns due to the requirement of storing the entire history of the chain on every participating node [31]. To address scalability challenges, various techniques have been explored, such as optimizing consensus algorithms, implementing sharding mechanisms or introducing layer-two scaling solutions, like state channels or sidechains [35]. These approaches aim to improve the throughput and capacity of blockchain networks, enabling them to handle a larger number of transactions or computations per unit of time. Deploying blockchain nodes within containers enables more efficient scaling of the network. By utilizing containerization, blockchain networks can dynamically adjust their capacity to meet fluctuating demands. Containers offer lightweight, portable environments that can be easily replicated and moved between hosts. This enhances the scalability of blockchain networks, allowing them to expand or contract as needed [2].

Security: It is a paramount concern in blockchain networks. Containerization contributes to enhancing the security of blockchain networks in multiple ways. By isolating blockchain nodes within separate containers, the impact of potential attacks or compromises is limited. Each container acts as an

independent unit, reducing the likelihood of an attacker gaining access to the entire network. Additionally, containerization simplifies the deployment of security patches and updates across the network, ensuring that the latest security measures are promptly applied [35].

Consistency: It is crucial for the reliable functioning of blockchain networks. Containerization aids in achieving consistency by utilizing container images. These images ensure that all nodes within the blockchain network are created with the same software stack and configurations. This reduces the risk of configuration errors and inconsistencies that can compromise the integrity of the network. Managing and maintaining the blockchain network become easier as containers offer a standardized and reproducible environment [42].

Deployment: Efficient deployment of blockchain networks is another critical research issue. Containerization, coupled with container orchestration tools like Kubernetes, simplifies and automates the deployment process. These tools enable the seamless distribution of blockchain nodes across multiple hosts, saving time and reducing the risk of human errors during deployment. Containerization streamlines the setup and configuration of blockchain networks, enhancing their manageability and overall deployment efficiency [49].

Overall, container-based virtualization provides solutions to critical research issues related to scalability, security, consistency and deployment in the context of blockchain technology. By leveraging containerization, blockchain networks can achieve enhanced performance, security and manageability. Using containerization technologies and methodologies enables more reliable and efficient utilization of blockchain networks, paving the way for their widespread adoption in various industries.

6. ISSUES AND CHALLENGES

Integrating container-based virtualization and blockchain technology can present several issues and challenges that must be addressed.

Security: While containerization can enhance the security of blockchain networks, it can also introduce new security risks. Containers can be compromised if they are not properly secured or if vulnerabilities in the container image are exploited. This could compromise the security of the entire blockchain network [9].

Performance: Containerization can affect the performance of blockchain networks. Running blockchain nodes in containers can result in overhead, which can impact the speed and throughput of the network. Careful optimization is required to minimize this overhead and ensure optimal performance [11].

Complexity: Integrating container-based virtualization and blockchain technology can add complexity to the deployment and management of blockchain networks. Container orchestration tools like Kubernetes can help simplify this process and introduce new layers of complexity that need to be managed [35].

Compatibility: Compatibility between container-based virtualization and blockchain technology can be an issue. Not all blockchain platforms may be compatible with containerization or require specific configurations to work effectively in a containerized environment [5].

Overall, integrating container-based virtualization and blockchain technology requires careful consideration and planning to address these challenges and ensure that the resulting network is secure, performant and manageable.

7. CONCLUSIONS

Previous studies have focused on the general benefits of containerization and blockchain technology, but have not extensively explored the challenges associated with integrating containers into blockchain environments. While some research has touched upon the advantages of containerization, such as resource sharing, portability, security, agility and ease of management, there is a lack of detailed analysis regarding the limitations and potential risks involved. Additionally, the performance enhancements achieved through containerization in the context of blockchain applications have not been adequately examined. Furthermore, studies have often overlooked the complexities of deploying and managing

containerized blockchain applications, neglecting the issues related to orchestration, integration and efficient resource allocation.

Based on the identified drawbacks and research gaps, the main research direction of this study is to comprehensively investigate the benefits and limitations of containerizing blockchain applications while focusing on improving overall performance. This study has explored the benefits and implications of container-based virtualization in the context of blockchain applications. The findings highlight containers' significant advantages, emphasizing their flexibility, portability and security features.

Using containers, blockchain nodes can be efficiently deployed, managed and isolated, ensuring the integrity and privacy of blockchain networks. The containerization approach enables the seamless movement of applications across different environments and infrastructures, supporting container runtimes and enhancing flexibility and scalability.

Moreover, the study emphasizes that container-based virtualization provides an efficient and lightweight method for running blockchain-based applications and services. Utilizing tools and platforms such as Docker, Kubernetes and AWS Fargate, simplifies the large-scale development, deployment and management of containerized blockchain applications.

In summary, this study contributes to understanding containerization's benefits in the realm of blockchain technology. The findings emphasize the value of container-based virtualization in enabling efficient, lightweight and secure execution of blockchain applications. Moving forward, further research and development in this area should focus on exploring advanced container orchestration techniques, enhancing security measures and addressing the challenges associated with containerization and blockchain technology integration. By doing so, the full potential of container-based virtualization in the blockchain domain can be realized, driving innovation and facilitating the adoption of blockchain technology in various industries.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus and Future Trends," Proc. of the 2017 IEEE Int. Congress on Big Data (BigData Congress), pp. 557–564, 2017.

[2] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain Challenges and Opportunities: A Survey," Int. J. of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[3] A. R. Javed, M. A. Hassan, F. Shahzad, W. Ahmed, S. Singh, T. Baker and T. R. Gadekallu, "Integration of Blockchain Technology and Federated Learning in Vehicular (IoT) Networks: A Comprehensive Survey," Sensors, vol. 22, no. 12, p. 4394, 2022.

[4] N. Naydenov and S. Ruseva, "Cloud Container Service Orchestrated with Kubernetes: A State-of-the- art Technology Review and Application Proposal," Int. J. of Advances in Computer Science and Technology, vol. 12, no. 4, 2023.

[5] A. Bhardwaj and C. R. Krishna, "Virtualization in Cloud Computing: Moving from Hypervisor to Containerization: A Survey," Arabian J. for Science and Eng., vol. 46, no. 9, pp. 8585– 8601, 2021.

[6] C. Chen, Z. Qi, Y. Liu and K. Lei, "Using Virtualization for Blockchain Testing," Proc. of the 2nd Int. Conf. on Smart Computing and Communication (SmartCom 2017), pp. 289–299, Shenzhen, China, December 10-12, 2017.

[7] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2521–2549, 2020.

[8] K. TaeYoung and K. Hyung-Jong, "Blockchain-based Service Performance Evaluation Method Using Native Cloud Environment," Proc. of the 2020 Int. Conf. on Software Security and Assurance (ICSSA), DOI: 10.1109/ICSSA51305.2020.00016, Altoona, PA, USA, 2020.

[9] G. Ramachandra, M. Iftikhar and F. A. Khan, "A Comprehensive Survey on Security in Cloud Computing," Procedia Computer Science, vol. 110, pp. 465–472, 2017.

[10] E. Casalicchio, "Container Orchestration: A Survey," Proc. of Systems Modeling: Methodologies and Tools, Part of the EAI/Springer Innovations in Comm. and Computing Book Series, pp. 221–235, 2019.

[11] N. G. Bachiega, P. S. Souza, S. M. Bruschi and S. D. R. De Souza, "Container-based Performance Evaluation: A Survey and Challenges," Proc. of the 2018 IEEE Int. Conf. on Cloud Engineering (IC2E), pp. 398–403, Orlando, USA, 2018.

[12] S. Shirinbab, L. Lundberg and E. Casalicchio, "Performance Evaluation of Container and Virtual Machine Running Cassandra Workload," Proc. of the 2017 3rd IEEE Int. Conf. of Cloud Computing Technologies and Applications (CloudTech), pp. 1–8, Rabat, Morocco, 2017.

[13] G. M. Diouf, H. Elbiaze and W. Jaafar, "On Byzantine Fault Tolerance in Multi-master Kubernetes Clusters," Future Generation Computer Systems, vol. 109, pp. 407–419, 2020.
[14] M. A. Marques, C. Miers and M. A. Simplício Jr, "Container Allocation and Deallocation Traceability Using Docker Swarm with Consortium Hyperledger Blockchain," Proc. of the 11th Int. Conf. on Cloud Computing and Services Science, vol. 1: CLOSER, pp. 288–295, 2021.
[15] J. Islam, Container-based Microservice Architecture for Local IoT Services, PhD Thesis, University of Oulu, Oulu, Finland, 2019.
[16] A. Brinckman, D. Luc, J. Nabrzyski et al., "A Comparative Evaluation of Blockchain Systems for Application Sharing Using Containers," Proc. of the 13th IEEE Int. Conf. on e-Science (e-Science), pp. 490–497, Auckland, New Zealand, 2017.
[17] A. S. Alsaffar and A. H. Alezzy, "A Lightweight Portable Multithreaded Client-server Docker Containers," Technium: Romanian J. of Applied Sciences and Technol., vol. 4, no. 10, pp. 31–43, 2022.
[18] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang and R. Buyya, "Blockchain-based Trust Management in Cloud Computing Systems: A Taxonomy, Review and Future Directions," Journal of Cloud Computing, vol. 10, no. 1, pp. 1–34, 2021.
[19] P. Raj, J. S. Chelladhurai and V. Singh, Learning Docker, ISBN: 1784397938, Packt Publish. Ltd., 2015.
[20] J. Sun, C. Wu and J. Ye, "Blockchain-based Automated Container Cloud Security Enhancement System," Proc. of the IEEE Int. Conf. on Smart Cloud (SmartCloud), pp. 1–6, Washington, USA, 2020.
[21] A. Mouat, Using Docker: Developing and Deploying Software with Containers, ISBN: 9781491915769, O'Reilly Media, Inc., 2015.
[22] D. Yaga, P. Mell, N. Roby and K. Scarfone, "Blockchain Technology Overview," arXiv preprint, arXiv: 1906.11078, 2019.
[23] V. Bakayov and A. Custură, "Blockchain Evolution," Tech. Rep., Research Institute, Amsterdam, Netherlands, 2020.
[24] S. Zeadally and J. B. Abdo, "Blockchain: Trends and Future Opportunities," Internet Technology Letters, vol. 2, no. 6, p. e130, 2019.
[25] S. Lemeš, "Blockchain-based Data Integrity for Collaborative Cad," Proc. of Mixed Reality and Three-dimensional Computer Graphics, IntechOpen, pp. 1–17, 2020.
[26] R. Jabbar, E. Dhib, A. B. Said, M. Krichen, N. Fetais, E. Zaidan and K. Barkaoui, "Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review," IEEE Access, vol. 10, pp. 20 995–21 031, 2022.
[27] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman et al., "Blockchain Technology: beyond Bitcoin," Applied Innovation, vol. 2, no. 6-10, p. 71, 2016.
[28] J. C. López-Pimentel, O. Rojas and R. Monroy, "Blockchain and Off-chain: A Solution for Audit Issues in Supply Chain Systems," Proc. of the IEEE Int. Conf. on Blockchain (Blockchain), pp. 126–133, Rhodes, Greece, 2020.
[29] S. Chaisawat and C. Vorakulpipat, "Fault-tolerant Architecture Design for Blockchain-based Electronics Voting System," Proc. of the 17th IEEE Int. Joint Conf. on Computer Science and Software Engineering (JCSSE), pp. 116–121, Bangkok, Thailand, 2020.
[30] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu and Y. Xiong, "Security and Privacy in the Internet of Vehicles," Proc. of the IEEE Int. Conf. on Identification, Information and Knowledge in the Internet of Things (IIKI), pp. 116–121, Beijing, China, 2015.
[31] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," Proc. of the 6th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), pp. 1–6, 2018.
[32] S. Kim and G. C. Deka, Advanced Applications of Blockchain Technology, ISBN: 9789811387753, Springer, 2020.
[33] A. Yewale, Study of Blockchain-as-a-service Systems with a Case Study of Hyperledger Fabric Implementation on Kubernetes, PhD Thesis, University of Nevada, Las Vegas, USA, 2018.
[34] D. Efanov and P. Roschin, "The All-pervasiveness of the Blockchain Technology," Procedia Computer Science, vol. 123, pp. 116–121, 2018.
[35] M. Mazzoni, A. Corradi and V. Di Nicola, "Performance Evaluation of Permissioned Blockchains for Financial Applications: The Consensys Quorum Case Study," Blockchain: Research and Applications, vol. 3, no. 1, p. 100026, 2022.
[36] G. Hileman and M. Rauchs, "2017 Global Blockchain Benchmarking Study," SSRN, no. 3040224, p. 122, 2017.
[37] S. Gec, D. Lavbič, M. Bajec and V. Stankovski, "Smart Contracts for Container Based Video Conferencing Services: Architecture and Implementation," Proc. of the 15th Int. Conf. in Economics of Grids, Clouds, Systems and Services (GECON 2018), pp. 219–233, Pisa, Italy, Springer, 2019.
[38] A. Ahmad, A. Alabduljabbar, M. Saad, D. Nyang, J. Kim and D. Mohaisen, "Empirically Comparing the Performance of Blockchain's Consensus Algorithms," IET Blockchain, vol. 1, no. 1, pp. 56–64, 2021.
[39] X. Wu, J. Yan and D. Jin, "Virtual-time-accelerated Emulation for Blockchain Network and Application

Evaluation," Proc. of the 2019 ACM SIGSIM Conf. on Principles of Advanced Discrete Simulation, pp. 149–160, 2019.

[40] S. Pongnumkul, C. Siripanpornchana and S. Thajchayapong, "Performance Analysis of Private Blockchain Platforms in Varying Workloads," Proc. of the 26th IEEE Int. Conf. on Computer Communication and Networks (ICCCN), pp. 1–6, Vancouver, Canada, 2017.

[41] Y. Hassanzadeh-Nazarabadi, A. Küpçü and Ö. Özkasap, "Lightchain: A DHT-based Blockchain for Resource Constrained Environments," arXiv preprint, arXiv: 1904.00375, 2019.

[42] Z. Shi, C. Jiang, L. Jiang and X. Liu, "HPKS: High Performance Kubernetes Scheduling for Dynamic Blockchain Workloads in Cloud Computing," Proc. of the 14th IEEE Int. Conf. on Cloud Computing (CLOUD), pp. 456–466, Chicago, USA, 2021.

[43] G. Volpe, A. M. Mangini and M. P. Fanti, "An Architecture for Digital Processes in Manufacturing with Blockchain, Docker and Cloud Storage," Proc. of the 17th IEEE Int. Conf. on Automation Science and Engineering (CASE), pp. 39–44, Lyon, France, 2021.

[44] N. El Ioini and C. Pahl, "Trustworthy Orchestration of Container Based Edge Computing Using Permissioned Blockchain," Proc. of the 5th IEEE Int. Conf. on Internet of Things: Systems, Management and Security, pp. 147–154, Valencia, Spain, 2018.

[45] D. Tosh, S. Shetty, P. Foytik, C. Kamhoua and L. Njilla, "CloudPoS: A Proof-of-stake Consensus Design for Blockchain Integrated Cloud," Proc. of the 11th IEEE Int. Conf. on Cloud Computing (CLOUD), pp. 302–309, San Francisco, USA, 2018.

[46] K. Awuson-David, T. Al-Hadhrami, O. Funminiyi and A. Lotfi, "Using Hyperledger Fabric Blockchain to Maintain the Integrity of Digital Evidence in a Containerized Cloud Ecosystem," Proc. of the Int. Conf. of Reliable Information and Communication Technology (IRICT 2019), Emerging Trends in Intelligent Computing and Informatics, pp. 839–848, Springer, 2020.

[47] G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar and K.-K. R. Choo, "Blocked: Blockchain-based Secure Data Processing Framework in Edge Envisioned v2x Environment," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5850–5863, 2020.

[48] P. Kumar and M. Shah, "To Build Scalable and Portable Blockchain Application Using Docker," Proc. of Soft Computing: Theories and Applications (SoCTA 2019), Part of the Advances in Intelligent Systems and Computing Book Series, vol. 1154, pp. 619–628, Springer, 2020.

[49] O. Bentaleb, A. S. Belloum, A. Sebaa and A. El-Maouhab, "Containerization Technologies: Taxonomies, Applications and Challenges," The Journal of Supercomputing, vol. 78, no. 1, pp. 1144–1181, 2022.

ملخص البحث:

حظيت تكنولوجيا سلاسل الكُتل بالكثير من الاهتمام في مجالاتٍ علميةٍ وهندسيةٍ متعدّدة. ولتحسين خدمات تكنولوجيا سلاسل الكُتل، لا بُدَّ من معالجة التّحديات التي تواجه تطبيقها. ويُعدّ استخدام ما يسمى "الأوعية الافتراضية" من الطُّرق التي يمكنها إدخال عددٍ من التّحسينات على خدمات تكنولوجيا سلاسل الكُتل من عدّة جوانب، أبرزها الحجم والتّعقيد والأمان وإمكانية التّوسيع لشبكات تكنولوجيا سلاسل الكُتل التّقليدية.

تشرح هذه الورقة تكنولوجيا سلاسل الكُتل، والأسباب التي وَراء دمْجها مع "الأوعية الافتراضية". ومن ناحية أخرى، فإنّ تكنولوجيا الأوعية الافتراضية تَستخدم سلاسل الكُتل لحماية البيانات، وتحسين إدارة الموارد. كذلك تعمل هذه الدراسة على تحليل الدراسات التي تناولت كُلاً من تكنولوجيا سلاسل الكُتل وتكنولوجيا الأوعية الافتراضية. وترتكز الدراسة على أنّ التّكامل بين تكنولوجيا سلاسل الكُتل والأوعية الافتراضية يتيح وضْع كُلّ تطبيقٍ من تطبيقات سلاسل الكُتل في وعاءٍ افتراضي منفصل، بحيث لا يؤثّر أي خللٍ في أحد الأوعية على الأوعية الأخرى أو على شبكة سلاسل الكُتل برُمّتها.

وفي الختام، تستعرض الدراسة الصّعوبات التي تكتنف التّكامل بين سلاسل الكُتل و الأوعية الافتراضية، وتناقش اتّجاهات البحث المستقبلية من أجْل إدخال تحسيناتٍ على نتائج هذا البحث.