Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

A conceptual architecture for simulating blockchain-based IoT ecosystems

Adel Albshri[1,2*], Ali Alzubaidi[3], Maher Alharby[4], Bakri Awaji[5], Karan Mitra[6] and Ellis Solaiman[1]

Abstract

Recently, the convergence between Blockchain and IoT has been appealing in many domains including, but not limited to, healthcare, supply chain, agriculture, and telecommunication. Both Blockchain and IoT are sophisticated technologies whose feasibility and performance in large-scale environments are difficult to evaluate. Consequently, a trustworthy Blockchain-based IoT simulator presents an alternative to costly and complicated actual implementation. Our primary analysis finds that there has not been so far a satisfactory simulator for the creation and assessment of blockchain-based IoT applications, which is the principal impetus for our effort. Therefore, this study gathers the thoughts of experts about the development of a simulation environment for blockchain-based IoT applications. To do this, we conducted two different investigations. First, a questionnaire is created to determine whether the development of such a simulator would be of substantial use. Second, interviews are conducted to obtain participants' opinions on the most pressing challenges they encounter with blockchain-based IoT applications. The outcome is a conceptual architecture for simulating blockchain-based IoT applications that we evaluate using two research methods; a questionnaire and a focus group with experts. All in all, we find that the proposed architecture is generally well-received due to its comprehensive range of key features and capabilities for blockchain-based IoT purposes.

Keywords Blockchain, IoT, Simulation, Modelling, Performance

Introduction

The Internet of Things (IoT) has enabled the interconnection and management of various types of computing and intelligent objects, including sensors, actuators, edge devices, networks and clouds, enabling the communication and processing of vast quantities of data for many applications [1]. In a typical IoT architecture, *things* are equipped with sensors that gather data about their environment and transmit it to edge devices or cloud servers for processing [2]. Then, collected data is transmitted through gateways, which are the second essential component of the IoT. Gateways serve as intermediaries between *things*, edge devices, and the cloud, facilitating the necessary connectivity, security, and data flow for the Internet of Things [3]. The third and fourth components of the Internet of Things are local edge devices for local data processing and/or cloud infrastructure, which consists of large virtualized resources such as storage and processing devices with high processing and analytical power. These resources enable large-scale data processing and analysis [4].

There have been security, privacy, and trust challenges associated with the IoT, which impair the smooth transition to IoT-enabled applications. One specific

*Correspondence:
Adel Albshri
a.albshri2@newcastle.ac.uk
[1] School of Computing, Newcastle University, Newcastle Upon Tyne, UK
[2] College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia
[3] College of Computing, Umm Al-Qura University, Al-Lith, Saudi Arabia
[4] Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia
[5] College of Computer Science and Information Systems, Najran University, Najran, Saudi Arabia
[6] Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, Skelleftea, Sweden

concern with IoT is that central IoT servers, which manage users' sensitive data, may pose a risk to privacy and potentially lead to privacy violations [5]. IoT has a wide range of applications, including health, environmental, and geospatial applications, which often involve the exchange of sensitive and private data. Given the sensitivity of the data being exchanged in many IoT applications, it is important to consider how to ensure that this data has not been modified, tampered with, or misused. This is especially relevant in the context of centralized IoT architectures, which are vulnerable to single points of failure. In addition, the centralized architecture of some IoT applications, which may involve the exchange of large volumes of data, can negatively impact the performance of these applications, potentially slowing them down to dangerous levels. For example, a hospital may not receive critical patient data in a timely manner if the system is slowed down [6]. Therefore, it is necessary to consider decentralized models for implementing IoT applications to address these performance and security concerns. The peer-to-peer (P2P) model, which enables large exchanges between IoT devices, has the potential to significantly reduce the cost of employing servers [7]. The peer-to-peer model for the Internet of Things also involves distributing processing tasks over a larger number of devices. As a result of this distributed processing, the failure of a single device in the network will not cause the entire system to fail, which meets the requirement for fault tolerance. In addition, using a peer-to-peer network can help to reduce the significant costs associated with servers, their operating systems, and maintenance [8]. However, it is important to note that the peer-to-peer model for the Internet of Things also has well-known security issues [9]. In this context, blockchain technology, which is an extended, secure peer-to-peer network [10], may be an effective solution.

More recently, Blockchain technology emerges with the potential to address the issues associated with centralised systems, such as a single point of failure and security vulnerabilities [11]. That is, Blockchain technology is widely recognized as a tamper-proof and secure technology. The first well-established blockchain-based application is Bitcoin [12], which is a decentralized digital currency based on a peer-to-peer network. Typically, blockchain technology is often used to secure data by providing a tamper-proof, decentralized, and transparent way of storing and managing data. The decentralized, distributed structure of the blockchain makes it difficult for any single entity to tamper with the data, as any changes to the data would have to be agreed upon by multiple network participants.

The transparency of the blockchain also helps to ensure the integrity of the data, as all network participants can see and verify the data stored on the network. In addition, the use of cryptographic techniques helps to ensure the confidentiality of the data. These features make blockchain technology a powerful tool for securing data in a variety of applications. Therefore, there has been growing interest in integrating blockchain technology into the IoT to address the security and scalability challenges that have emerged in traditional IoT architectures. By using blockchain technology, it is possible to create decentralized, secure, and transparent networks for exchanging data between IoT devices. This can help to ensure the integrity and confidentiality of the data being exchanged, as well as provide a tamper-proof record of the data. In addition, the decentralized nature of blockchain networks can help to improve the fault tolerance and scalability of IoT systems, as the failure of a single device or network participant will not compromise the integrity of the network. These features make blockchain technology a promising solution for securing and scaling IoT networks [13]. However, both the IoT and blockchain technologies are complex and have many potential applications, making it important to have accurate and effective simulation tools that can model and evaluate these applications before they are deployed in the real world.

Simulation tools can help to identify potential issues and optimize the performance of these systems, making it possible to test and refine the design of these systems before they are deployed. In the case of IoT and blockchain applications, simulation tools can help to evaluate the scalability, security, and reliability of these systems, as well as the performance of various protocols and algorithms. This can help to ensure that these systems are robust and fit for their intended purpose and can save time and resources by identifying and addressing issues before they arise in the real world. Simulation tools are used to study the behavior and performance of systems by examining various parameters and variables [14]. Thus, simulation tools are particularly useful for studying complex systems that are difficult to analyze or test in the real world [15, 16]. Simulation studies can be a cost-effective way to study the behavior and performance of systems, particularly complex systems. In addition, simulation tools can be used to study the performance of a system under different configurations, helping to identify the optimal configuration for a particular application. By using simulation tools, it is possible to analyze and optimize the performance of a system in a controlled and repeatable manner, providing valuable insights into how the system will behave in the real world.

The paper aims to gather the thoughts and insights of experts on developing a simulation environment for blockchain-based IoT applications. Based on these thoughts and insights, a conceptual model is proposed for the simulation environment. To evaluate this, a

questionnaire and a focus group method are conducted to evaluate the effectiveness of the conceptual model. The following contributions have been made in this paper:

1 We conducted mixed methods research to gather the opinions and insights of experts to understand the primary challenges experts face with these types of applications and to use this information to inform the design of a creation simulation environment for blockchain-based IoT applications. By utilizing a mixed methods approach, we were able to gather both qualitative and quantitative data from a diverse group of experts. This allowed us to gain a more comprehensive understanding of the issues and needs surrounding the creation of this simulation tool. Our findings confirm that the participants had a high level of confidence in the ability of blockchain to alleviate IoT issues but also highlighted the need for more tools to evaluate and test this concept.
2 We proposed a conceptual model for a creation simulation environment for blockchain-based IoT applications that includes various components, mechanisms, and processing elements. The purpose of the proposed conceptual model is to provide a foundation for creating a simulation environment that can be used to test and evaluate the performance of blockchain-based IoT applications.
3 We conducted a questionnaire and a focus group with experts to evaluate the conceptual model against a set of objectives. The result of the evaluation of the conceptual model showed that it is generally well-regarded. The reason underpinning this attitude is the inclusion of a wide range of key features and capabilities that make it a suitable foundation for creating a simulation environment for blockchain-based IoT applications.

Paper organisation

The structure of this paper is as follows: Section Related work provides an overview of related work in the field. The research methodology of the study is outlined in Section Research methodology. The research methods used to gather insights and perspectives on the design of an appropriate simulator for the study are described in Section Utilized methods to gather requirements. The results of the study are presented in Section Findings. Recommendations based on the findings of the study are presented in Section Recommendation. Section Motivating blockchain-based IoT scenario introduces a motivating example of a blockchain-based IoT scenario. The proposed conceptual architecture for the modelling blockchain for IoT application is presented in Section Conceptual architecture, and the results of evaluating this architecture are discussed in Section Evaluation. The paper concludes with a summary of the main findings and future work in Section Conclusion and future work.

Related work

This section describes the prior works that have been done on simulating blockchain and Internet of Things (IoT) systems. In recent years, there has been a significant amount of research on both blockchain and IoT, and many efforts have been made to develop simulators for these technologies. In the literature, there are several examples of simulators for blockchain systems [17] and IoT applications [18].

Blockchain simulators

There have been several efforts to develop simulators for blockchain systems. One of these, VIBES (Visualisations of Interactive Blockchain Extended Simulations) [19], was proposed as a configurable blockchain simulator to enable end-users to perceive empirical insights and analytics about blockchain networks. VIBES can simulate blockchain systems and mimics the effect of specific parameter changes on the system. The merits of VIBES are twofold. First, VIBES is a scalable simulator as it can simulate systems with thousands of interacting nodes. Second, VIBES is a fast simulator able to provide fast simulation results. Faria and Correia [20] proposed a discrete-event blockchain simulator referred to as BlockSim that is a framework assisting in designing, implementing and evaluating blockchains. It can evaluate the implementation of different blockchains that are rapidly modelled and simulated. Therefore, BlockSim is characterised as a dynamic simulator able to simulate systems over a certain time interval. Yet another attempt referred to as BlockSim is proposed by Alharby and van Moorsel [21] that implements proof of work (PoW) as a consensus algorithm for making agreements about the blockchain's state. Moreover, as a discrete-event simulator, BlockSim can test the effect of different parameter configurations on the system's performance. Another simulator BlockSIM [22] is a resilient open-source blockchain simulator that enables blockchain designers to evaluate the performance of their designed private blockchains. The contribution of BlockSIM is twofold. First, it accurately models the stability of the system. Second, it accurately simulates the transaction throughput concerning a given scenario. It can optimise the system's parameters which, in turn, allows for testing various scenarios needed for the build-up of its chains.

IoT simulators

There have been several efforts to simulate Internet of Things (IoT) ecosystems and the applications that operate within these ecosystems. These simulators can be used to study the behavior and performance of IoT systems, as well as to optimize the design and deployment of these systems in the real world. A cloud layer is normally significant for a wide range of IoT applications; therefore, cloud simulators are widely used for simulating IoT applications. The most popular and widely used is the CloudSim toolkit [23], in which tasks are created in the form of cloudlets to be processed using virtual machines in the cloud environment. Moreover, it is mainly designed to simulate discrete-event scenarios while implementing a five-layer structure. An interesting aspect of CloudSim is its ability to model CPU power consumption to shed light on bandwidth and delay parameters. Due to its success, an improved extended version has been introduced and referred to as CloudAnalyst [24]. CloudAnalyst extends the core of CloudSim while adding a set of features to investigate the effect of different configurations on the system's performance. A prominent simulator for modelling applications on the Edge of IoT networks is iFogSim [25] which is the extension of the CloudSim simulator. As an edge layer-dependent simulator, it can simulate real systems that consider the different aspects ranging from sensing to processing the data. The main contribution of this simulator is the simulation of the physical layer. In particular, it can model the physical component of systems.

To our knowledge, none of the simulators mentioned above focuses on simulating IoT scenarios (IoT applications that run on multiple IoT layers, including sensors, edge devices, communication networks, and the cloud). This motivated the development of IoTSim [26]. IoTSim is built over the core of CloudSim to support the task of IoT and big data simulation. IoTSim follows a three-layer architecture (perception, network and application layer). These layers are integrated with the three layers of CloudSim (storage, big data processing and user code). An important point in this simulator is using the MapReduce approach, one of the big data handling approaches. From the practical viewpoint, this is done through two separate functions: MapCloudlet and ReduceCloudLet. Finally, IoTSim-Osmosis [27] is a framework that supports testing and validating IoT applications using the principle of osmotic computing. It is mainly designed to simulate complex IoT applications while being deployed on heterogeneous edge, cloud and SDN environments.

It appears that, despite the many efforts that have been made to develop simulators for blockchain and IoT systems, there are currently no simulators that focus specifically on simulating the integration of these technologies. Table 1 summarizes the previous work in this area and highlights the lack of focus on simulating the integration of blockchain and IoT systems. This lack of focus on simulating integrated blockchain and IoT systems highlights the need for further research in this area and the potential value of a simulator that can model and evaluate the performance of such systems.

Research methodology

This section presents the research methodology steps to design the conceptual model for creating a simulation environment for blockchain-based IoT applications, which contains several steps as shown in Fig. 1.

1 *Survey of blockchain simulators*: The first step in this research methodology is to survey existing blockchain simulators in order to understand the current state of the field and identify potential gaps or areas for improvement. To do this, we carried out a systematic mapping study for existing blockchain simulators [17] to provide a systemic mapping review of blockchain simulators. This study is done with respect to several quality factors in which we shed light on the configuration parameters (inputs) and produced metrics (outputs) by each simulator. For a deep technical review, a code quality comparison is carried out to assess the source code of the covered simulators. The results reveal that blockchain simulation is still in its infancy stages, and further research must be undertaken in this direction. No simulator fully covers the wide operational range of features and capabilities of existing blockchain technologies. Moreover, existing blockchain simulators have little viability for being integrated with other technologies, such as cloud and IoT.
2 *Utilize a mixed-method approach to gather requirements*: The second step of this study is to gather the opinions of experts on the development of a simulation environment for blockchain-based IoT applications using a mixed-method approach. This includes conducting interviews and a questionnaire with experts in the field to understand the needs and preferences of potential users of the simulator. To do this, we conducted this approach including interviews and a questionnaire with domain experts [28]. These methods allowed us to gain insights into the potential contributions and challenges of blockchain-based IoT applications and to formulate the proposed simulation's requirements and mechanisms. This process is outlined in relation to several objectives, as follows:

   (a) To gather the required information from experts in the field regarding:

Table 1 A summary of the related work simulators along with their main features

Simulator	Simulator Scope	Programming language	Core	Simulator Type	Features									
					End to end IoT layers						Blockchain layers			
					IoT device	Edge	Network communication	Network Protocol	Cloud	Support blockchain	Network	Consensus	Data	Support IoT
VIBES [19]	Blockchain	Scala	N/A	Discrete-event								✓	✓	
BlockSim [20]	Blockchain	Python	N/A	Discrete-event							✓	✓	✓	
BlockSim [21]	Blockchain	Python	N/A	Discrete-event								✓	✓	
BlockSIM [22]	Blockchain	Python	N/A	Discrete-event								✓	✓	
CloudSim [23]	Cloud	Java	N/A	Discrete-event					✓					
CloudAnalyst [24]	Cloud	Java	CloudSim	Discrete-event				✓	✓					
iFogSim [25]	Edge	Java	CloudSim	Discrete-event	✓	✓								
IoTSim [26]	IoT	Java	CloudSim	Discrete-event	✓			✓						
IoTSim-Osmosis [27]	End to End IoT	Java	CloudSim	Discrete-event	✓	✓	✓	✓	✓					

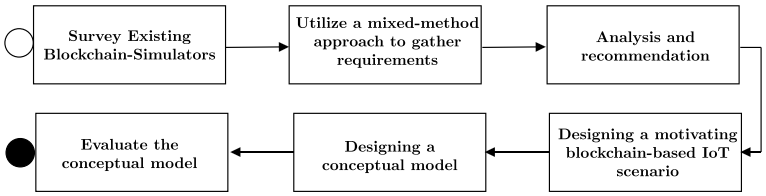

Fig. 1 Steps of Research Methodology

i The usage of IoT in our daily life.
ii The most commonly used blockchain types.
iii The IoT data that should be stored on blockchain.
iv The consensus algorithms required for the simulator.
v The users' needs as regards the blockchain log.
vi The possibility of using IoT nodes as blockchain nodes.

(b) To provide analytical information regarding:

i Participants' opinions about having an integrated blockchain IoT simulator.
ii Participants' opinions on modelling various types of blockchain in the simulator.

(c) To design a simulator to validate the integrated blockchain IoT systems.

3 *Analysis and recommendation*: The third step is to analyze the data collected in the previous steps and make recommendations for designing and implementing a simulation environment for blockchain-based IoT applications. This could involve identifying key features or capabilities that should be included in the simulator, identifying potential challenges or limitations, and suggesting ways to overcome these challenges.

4 *Motivation scenario*: The fourth step of the research methodology involves outlining the potential uses and benefits of a simulation environment for blockchain-based IoT applications through a motivation scenario. The purpose of the motivation scenario is to provide a clear understanding of the potential applications and benefits of the proposed simulator. It helps to guide the development and implementation of the simulator by highlighting the specific needs and goals that the simulator should aim to address.

5 *Designing a conceptual model*: The fifth step is to propose a conceptual model as a foundation for creating a simulation environment for blockchain-based IoT applications. This involves providing a high-level design in order to represent the fundamental principles (e.g., the main components) and relationships of a system or concept.

6 *Evaluate the conceptual model*: The final step is to evaluate the conceptual model using a focus group of experts in the field. This could involve presenting the model to a group of experts and gathering feedback and insights on its strengths, weaknesses, and potential improvements. This feedback can then be used to refine and improve the conceptual model before proceeding with the development of the simulation environment. To do this, it is important to have clear objectives in mind when conducting this evaluation. Therefore, we have applied the SMART criteria [29] to evaluate the feasibility and effectiveness of our objectives. This helps to ensure that our objectives are specific, measurable, attainable, relevant, and time-bound. To ensure that our conceptual model meets the needs and expectations of stakeholders, we conducted a questionnaire and a focus group with ten experts in the field of blockchain and IoT, as outlined in the Evaluation section. The purpose of both approaches was to gather feedback and insights that would inform the evaluation of the conceptual model. By engaging with experts and gathering their feedback and insights, we aimed to ensure that the conceptual model adequately addresses the needs of all relevant parties. This process is described in relation to several objectives, as follows:

- **Objective 1**: *To evaluate the generalizability and quality of the conceptual model.*
  IoTSim-Osmosis [27] is a framework for simulating the behavior and performance of IoT systems across an edge-cloud continuum. It enables users to test different configurations and scenarios in a simulated environment, providing a valuable tool for understanding how different factors may impact the behavior of an IoT system. The IoTSim-Osmosis framework is designed to be flexible and extensible, allowing users to simulate a wide range of IoT systems and scenarios. It offers a set of tools and libraries for building and running simulations, as well as

visualizing and analyzing the results. Assuming that IoTSim-Osmosis is the base IoT simulator in the conceptual model, it is important to gather feedback and insights from a diverse group of experts in the fields of blockchain and IoT. This will help us to determine whether the IoTSim-Osmosis simulator meets the needs and expectations of these experts.

- **Objective 2**: *To determine the extent to which the IoTOsmosis simulator meets the requirements of participants.*

The conceptual model consists of two main components: the IoT side and the blockchain side. The IoT side focuses on modelling and simulating the devices, sensors, and other components that make up an IoT system. The blockchain side, on the other hand, involves modelling and simulating the nodes, consensus mechanisms, and other elements of a blockchain system. Therefore, It is essential to evaluate the effectiveness of the blockchain component of the simulator in meeting the needs of participants.

- **Objective 3**: *To evaluate the effectiveness of the blockchain component of the conceptual model in meeting the needs of the participants.*

Obtaining feedback, criticism, and recommendations from experts can be a useful way to improve the conceptual model for modelling blockchain for IoT applications. Experts in the fields of blockchain and IoT can offer valuable insights and perspectives on the model, which can help identify areas where it may be lacking or where it could be improved.

- **Objective 4**: *To identify areas of the conceptual model that may need improvement.*

Utilized methods to gather requirements

Participants

This paper employed a sequential explanatory design methodology [30] comprising a questionnaire and interviews. Overall, 25 participants represented the target sample of individuals with knowledge of computer science, with a specific specialisation in IoT and/or blockchain.

Research tools

An online questionnaire with nine closed-ended questions was created using the SurveyMonkey website and distributed to the participants. This was followed by online interviews using the Zoom app with a set of participants who consented to participate. At the end of the interview, participants had the opportunity to complete a form with open-ended questions, which enabled the collection of qualitative data for a high level of analysis. To assess the reliability and consistency of the gathered information, we calculated Cronbach's Alpha [31] using SPSS for the 9 questions, resulting in a value of 0.796. This value exceeds 0.5, indicating a high level of reliability and consistency of the gathered data.

Research procedures

First, it was necessary to gather quantitative numerical data through a questionnaire [32], to develop robust conclusions. Second, qualitative data was gathered through interviews with various participants, using a set of open questions [33]. The first approach, the questionnaire, was disseminated to approximately 25 participants, all of whom were IoT and blockchain, developers/researchers. With 25 active participants, the statistical analysis was undertaken using SPSS to understand the participants' attitudes regarding blockchain features. To more effectively communicate the idea, the data analysis results as numeric values are presented in descriptive graphical format. The question responses were provided on a Likert scale from 1 ('strongly disagree') to 5 ('strongly agree'). The findings, presented in the figures, are displayed in the Questionnaire. Regarding the second data collection approach of the interviews, these were undertaken online with six participants who responded to a set of open questions. An in-depth description of this process is presented in Interviews section.

Findings

Questionnaire

The questionnaire began by asking questions to determine the participants' familiarity with the IoT, specifically asking, *"To what extent are you familiar with IoT?"* We received 25 answers, as shown in Fig. 2. The figure shows that the majority of participants (eight, 32%) are moderately aware of the IoT, while six participants (24%) have moderately low familiarity with the IoT. Additionally, four participants (16%) are highly aware of the IoT, and another five participants (20%) have a moderately high awareness of the IoT. On the other hand, the least number of participants (two, 8%) were completely unaware of the IoT. Overall, the selected participants were a good fit as the majority (moderate and higher) were aware of the IoT.

In addition to examining participants' familiarity with the IoT, we also looked at their familiarity with blockchain to gain more confidence in their answers. Thus, participants were asked, *"To what extent are you familiar with blockchain?"* We received 25 responses, shown in Fig. 3. The figure suggests that the majority of participants (seven, 28%) have a moderately high awareness of blockchain, while six participants (24%) are very familiar with blockchain. The least number of participants (two, 8%) are completely unaware of blockchain, while five

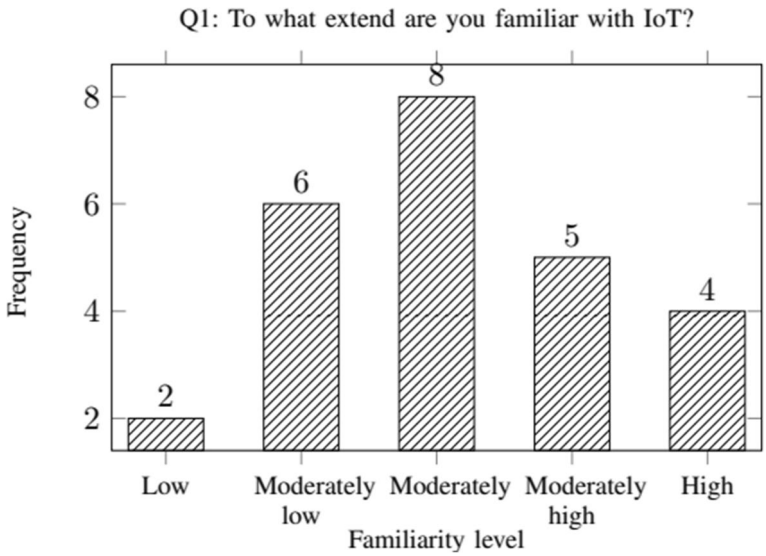

Fig. 2 Participants' familiarity with the IoT

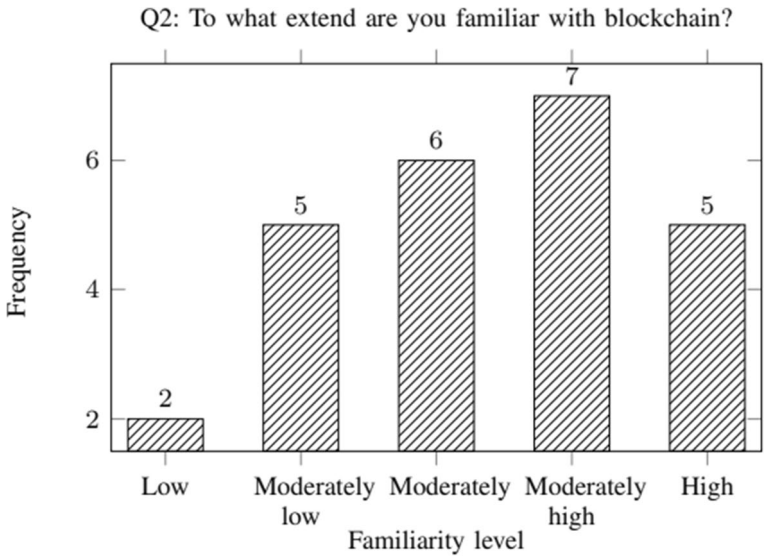

Fig. 3 Participants' familiarity with Blockchain

participants (20%) have a moderately low awareness of blockchain. Additionally, six participants (24%) are moderately aware of blockchain.

Similar to the participants' familiarity with the IoT, the selected participants were a good fit for this question, as the majority are aware of blockchain. Therefore, participants were asked, *"if they believe that there will be an expansion of blockchain with IoT in the future"* All 25 participants responded, with their responses shown in Fig. 4. It was found that the majority (eight, 32%) strongly agreed with this point. Additionally, six participants (24%) expressed a moderately high level of agreement. In total, 11 participants (44%) either moderately or strongly disagreed.

Following this, participants were asked, *"What are your thoughts regarding the need to have an IoT blockchain simulator for helping developers adjust the system's configurations?"* All 25 participants provided their responses, summarized in Fig. 5. As shown in the figure, nine participants (36%) strongly agreed with this idea, while eight participants (32%) agreed with it. In

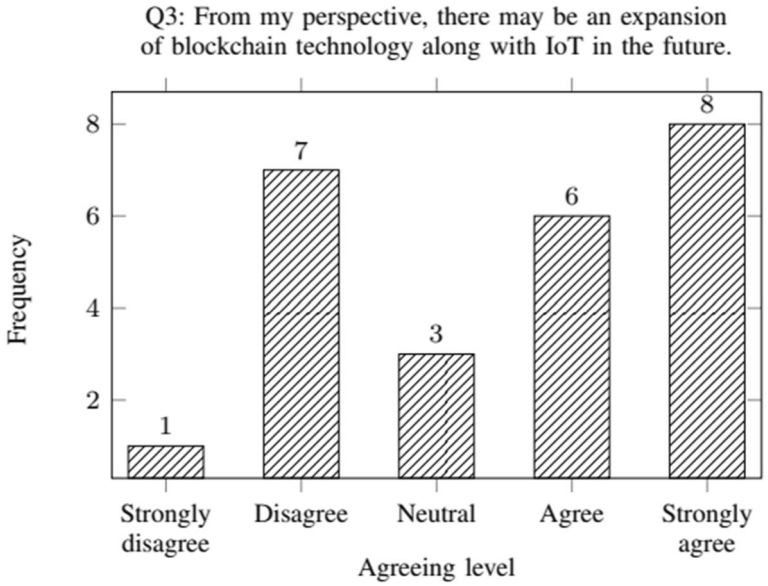

Fig. 4 Participants' thoughts about the IoT's integration with blockchain

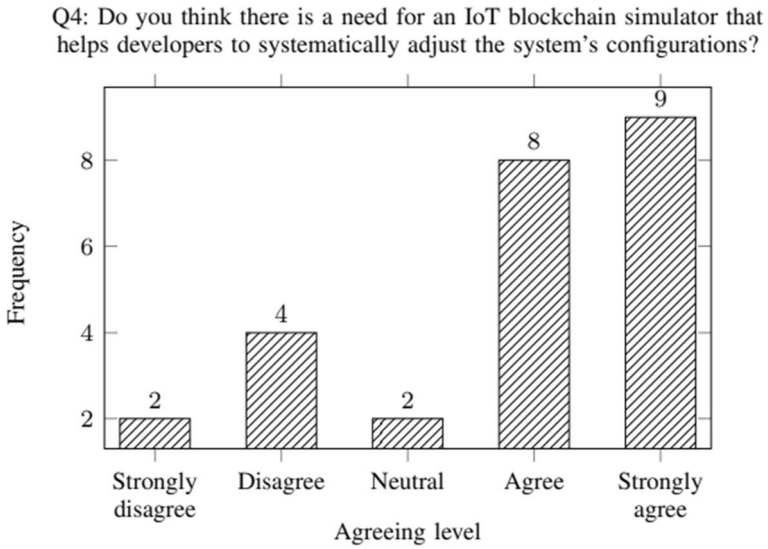

Fig. 5 Participants' thoughts about having an integrated IoT blockchain simulator

total, 10 participants (32%) were either neutral or completely disagreed with the concept

Given that the participants are domain experts, We took the opportunity to ask participants for their perspectives on storing IoT data in the blockchain, asking, *"Do you agree that all IoT data should be stored in the blockchain?"* The participants' responses are shown in Fig. 6. It is clear that the majority disagreed with this statement (13 participants either disagreed or strongly disagreed). This may be due to the various scenarios of using IoT with blockchain. On the other hand, the least number of participants agreed with this statement (eight participants either agreed or strongly agreed), while two participants were neutral.

Consensus algorithms are critical in blockchain because they are used to reach a common agreement (consensus) on the current state of ledger data and enable unknown peers to be trusted in a distributed computing environment. Therefore, we sought to understand participants' needs related to this. Accordingly, participants

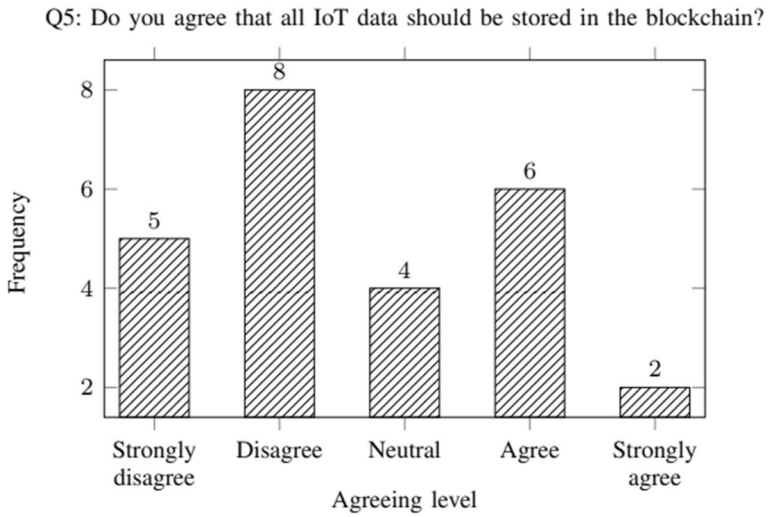

Fig. 6 Participants' thoughts about storing all of the IoT data in the blockchain

were asked, *"What are your thoughts on having multiple consensus algorithms in the simulator?"* The participants' responses to this question are summarized in Fig. 7. Examining the data more closely, it is clear that the majority (eight, 32%) agreed with this idea, while five participants (20%) strongly agreed. In total, 11 participants (38%) either moderately or strongly disagreed.

Considering blockchain in greater depth, it is essential to determine the participants' perspectives regarding investigating the log. This is crucial because it provides the opportunity to compute system latency and throughput. Accordingly, the participants were asked for their opinions concerning investigating the log file. The participants' responses to this question are presented in Fig. 8. The significant point is that the majority (12 participants) either strongly agreed or agreed with this idea. Additionally, five participants expressed neutrality concerning the statement. Meanwhile, eight participants in total expressed either moderate or complete disagreement.

Subsequently, the participants were asked about using IoT devices as blockchain nodes. The participants'

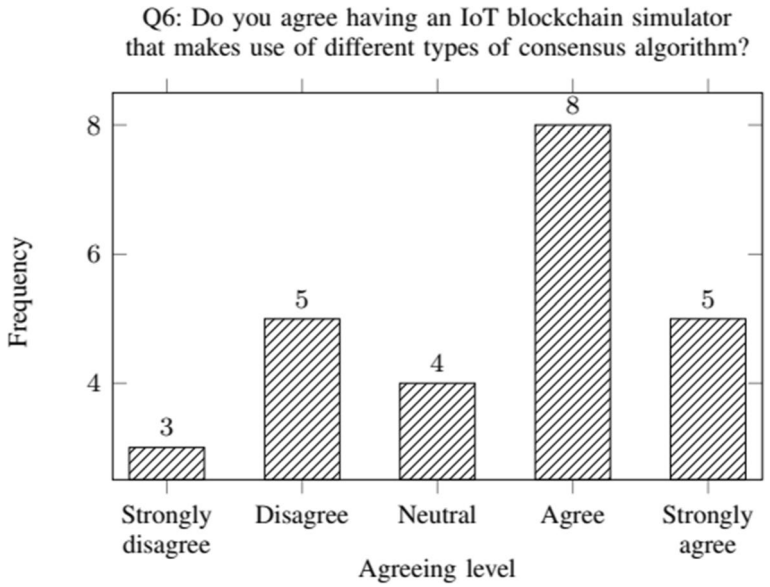

Fig. 7 Participants' thoughts about having multiple consensus algorithms in the simulator

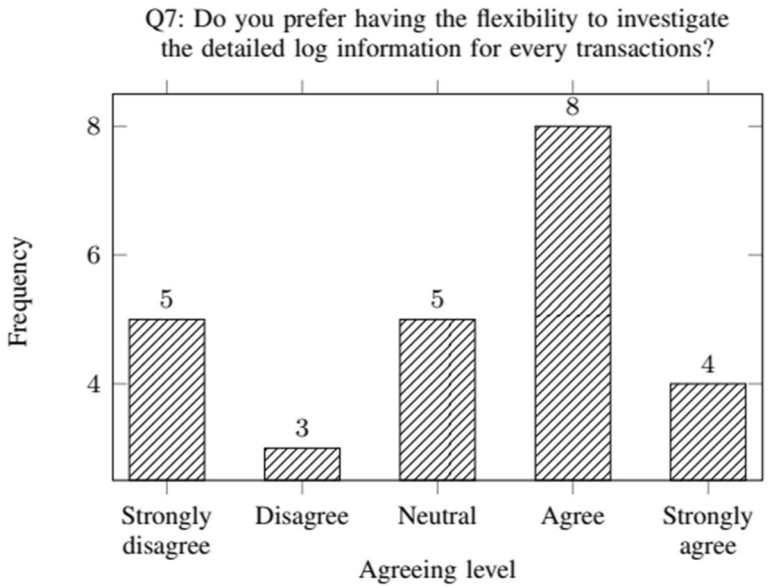

Fig. 8 Participants' thoughts about the ability to investigate the log

responses to this question are presented in Fig. 9, which presents their overall positive perspectives regarding this statement. Ultimately, most participants either strongly agreed (seven participants, 28%) or agreed (five, 20%) with the statement. In contrast, a total of nine participants (36%) either strongly disagreed or disagreed with this notion. Lastly, six participants (24%) expressed neutrality regarding this notion.

Finally, given that there are numerous types of blockchain, there is a need to comprehend if it is essential to have a simulator that can model the diverse types. Accordingly, the participants were asked about this, with their responses to this question presented in Fig. 10. According to the participants' perspectives, the majority (nine participants, 36%) are neutral towards this. Alternatively, four participants (16%) agreed, while two participants (8%) strongly agreed. Finally, ten participants

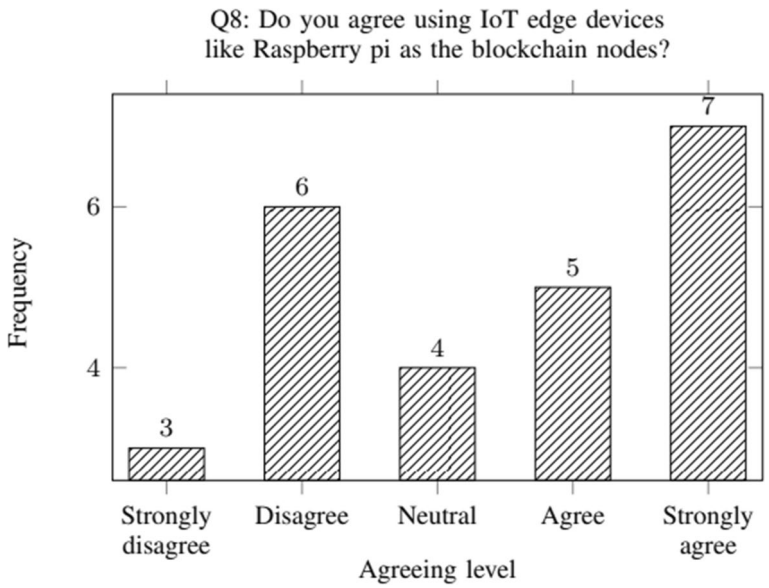

Fig. 9 Participants' thoughts about using IoT edge devices as blockchain nodes

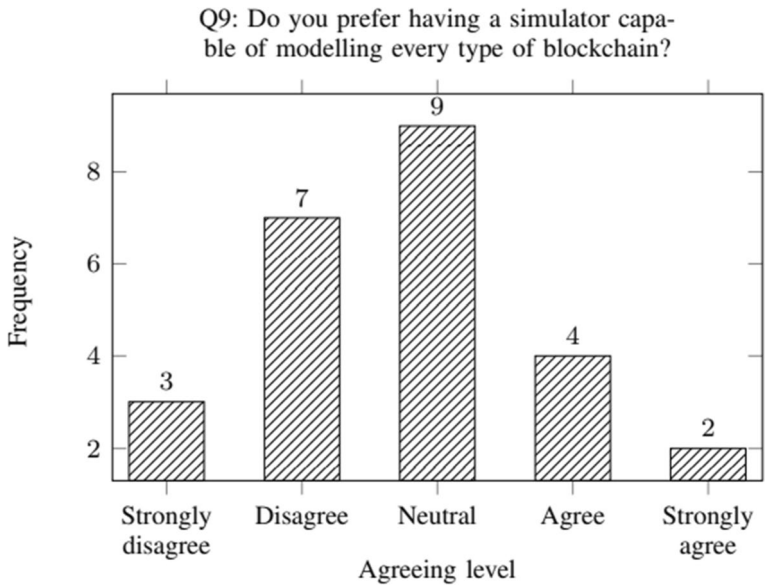

Fig. 10 Participants' thoughts about modelling different blockchain types in the simulator

(40%) either strongly disagreed or disagreed with this notion.

Overall, the results of a questionnaire were given to 25 participants to gauge their familiarity with the Internet of Things (IoT) and blockchain, and their opinions on various topics related to the potential expansion of blockchain with IoT in the future. The results show that the majority of participants are at least moderately familiar with both IoT and blockchain. When asked about the expansion of blockchain with IoT, the majority of participants agreed, with 44% either moderately or highly agreeing. The participants were also asked about the need for an IoT blockchain simulator to help developers adjust system configurations, with 36% strongly agreeing and 32% agreeing. When asked about storing all IoT data in the blockchain, the majority of participants disagreed, while a smaller number agreed. Additionally, the participants were asked about the inclusion of multiple consensus algorithms in a simulator, with the majority expressing agreement. Overall, the results of the questionnaire suggest that the participants are knowledgeable about both IoT and blockchain and see value in the potential expansion of the two technologies. For the picture to be complete, Table 2 matches the questionnaire questions to the predefined objectives.

Interviews

Interviews were conducted with a set of participants to collect information concerning their opinions on using IoT-based Blockchain, as well as comprehending their

Table 2 Matching the questionnaire questions to the predefined objectives. For the question numbering, please refer to Figs. 2 - 10

Question	Objective (a)						Objective (b)		Objective (c)
#	i	ii	iii	iv	v	vi	i	ii	
Q1	✓								
Q2		✓							
Q3	✓	✓							
Q4							✓		✓
Q5			✓						✓
Q6				✓					✓
Q7					✓				✓
Q8						✓			✓
Q9								✓	✓

requirements for the simulation software for assessing blockchain-based IoT. The participants' responses were assessed from active, analytical, and critical perspectives, with their suggestions being clarified. Three questions were posed:

1 *What are the major challenges you face when dealing with blockchain-based IoT for any evaluation purposes?*
2 *Which features make blockchain suitable for the IoT?*
3 *What are the anticipated outcomes of utilising blockchain within the IoT?*

P1 stated that *"There are many challenges based on the current proposed model. The obstacle lies in investigating the performance and cost of these technologies. Also, there are many proposed simulators for Blockchain and IoT in the literature; however, each simulator either focuses on IoT or blockchain. As a researcher, I prefer having a multi-discipline simulator that can simulate IoT devices in sensing and sending data to the edge/fog layer then to cloud, while using blockchain in different layers"*. Regarding the second question, he remarked, *"The majority of IoT applications such as healthcare data is of high importance and needs to be securely handled. I believe blockchain is a strong fit for this scenario because of its features (for example, decentralisation) that dispense a third party to manage data"*. Lastly, for the third question, he suggested that *"With the rapid development of IoT technology and the large number of devices expected to be connected, I believe blockchain would alleviate security issues. For example, identity management and access to the IoT should be more secure and trusted, using a reliable tool for controlling data access"*.

P2 stated concerning the first question, "The main challenge I faced with the IoT and blockchain technologies is the difficulty of monitoring systems' performance. *"The challenge is that it does not cover all of my required features. I often use a cloud simulator to evaluate the system. Having a Blockchain simulator with IoT features that can track every transaction and system throughput will ease my tasks. This could become an efficient simulator, utilising both blockchain and IoT power"*. Concerning the second question, the participant explained that *"not all the IoT data are of high importance, but there is still a need to secure the sensitive data and enhance privacy"*. Finally, he stated that *"I believe blockchain can mitigate several of the IoT issues related to privacy. Also, blockchain can define a set of policies needed to control IoT data access"*.

In reply to the first question, **P3** mentioned that *"One of the most important blockchain-based IoT challenges is system evaluation because of the heterogeneity and mobility of IoT devices. Personally, I prefer to assess the system from different viewpoints, ranging from general performance (computational time, transaction latency and throughput) to security, but there is no simulator permitting this"*. Responding to the second question, he said that *"Data storage is a crucial metric to determine the applicability of blockchain with the IoT. The IoT devices sense the environment and send data in real time. This implies that we have plenty of data per second. Accordingly, blockchain cannot be used as data storage for all data. Hence, I prefer storing only the most important data; I think that this can be reliable"*. Concerning the third question, he asserted that *"Every single device can be identified using a permissioned blockchain network that is used by all parties involved. This implies that data is generated by an identified device (trusted), in the sense that the generated data has a unique identification number, hence ensuring immutability. In this scenario, it could be appropriate to track the data in the supply chain context"*.

P4 noted concerning the first question that *"The challenge is how to obtain various statistics about the system, like the number of generated transactions, number of blocks and time of confirmation, both for the block and transaction. These metrics give me an indicator about the proposed system, which is essentially the same as the real world and enables me to make decisions"*. Regarding question two, the participant stated that *"IoT data can be immutable and distributed over time in the blockchain network. Participants in the blockchain network can ensure the data's authenticity and that it will never be tampered with"*. Finally, concerning question three, he remarked that *"I advise using blockchain to keep sensitive IoT data where security is ensured. Also, as IoT devices are the data source, there is a need for reliable analysis which will not be carried out if there are no device management criteria. I believe this can be carried out by blockchain, for example, using smart contracts"*.

P5 commented that *"Assessing the system performance is very important. In the context of blockchain and the IoT, it is difficult to measure performance without simulation due to the complexity of both technologies. So, from my point of view, the simulator enables me to test the system from diverse aspects. Specifically, I can configure the number of IoT devices and protocols used, while at the same time determining the size of transactions, either for blockchain or the IoT (end to end)"*. Regarding the second question, he suggested that *"One of the advantages of blockchain is decentralisation, as it can prevent a single point of failure and bottlenecks from occurring. I see that blockchain benefits the IoT by ensuring reliable data transfer"*. Finally, he stated *"I believe that blockchain would provide the IoT developers with more secure solutions due to its features"*.

Concerning the first question, **P6** remarked that *"The challenge lies in determining if the simulator supports more than one measure, such as latency, throughput, total time, along with the number of blocks created to analyse the overall performance of blockchain and the Internet of Things. Based on my experience, it is difficult to cover all aspects of the IoT and blockchain simultaneously, but the simulator can cover the general aspects of both technologies in different scenarios"*. Concerning the second question, he stated that by and large *"Due to the limited processing capabilities of IoT devices, third-party service providers are generally used to process additional data. By entrusting sensitive user data to third-party service providers, users must trust data protection and privacy. This trust coincides with the danger of breaking data privacy and policies. Blockchain's traceability can help in these situations"*. Finally, he expressed that *"Blockchain is a promising choice when it comes to ensuring privacy and applying security"*.

The findings of this summary are based on interviews conducted with participants to gather their opinions on using IoT-based blockchain and their requirements for simulation software for evaluating blockchain-based IoT. The participants identified several challenges in using blockchain-based IoT for evaluation purposes, including difficulties in monitoring and evaluating system performance, a lack of simulators with all required features, and the heterogeneity and mobility of IoT devices. They also emphasized the importance of data storage in determining the suitability of blockchain for the IoT, and the need to store only the most important data due to the large amount of data generated by IoT devices. One participant mentioned that blockchain has the potential to enhance security and privacy in the IoT, particularly through the use of permissioned blockchain networks to identify devices and ensure the immutability of data. Another participant highlighted the potential for blockchain to improve supply chain management by tracking data in the supply chain context.

In general, participants are seeking a multi-discipline simulator that can simulate both the IoT and blockchain aspects of a system and provide various metrics and statistics about system performance, security, and data storage. They also stressed the importance of securely handling sensitive data and enhancing privacy through the use of blockchain in the IoT.

Recommendations

The results presented in the previous sections have evidenced a broad belief that blockchain can benefit IoT applications and enhance its applicability by alleviating its limitations. Moreover, the majority of participants in our studies agreed that it is necessary to have an integrated blockchain IoT simulator to aid in the development and evaluation of applications that integrate blockchain and IoT technologies. On this basis, we recommend greater research and exploration of the design and development of an integrated blockchain IoT simulator. Considering the lack of such a simulator in the literature, this calls for greater research and the need to attract the attention of contemporary researchers.

Motivating blockchain-based IoT scenario

The need for a Blockchain-based IoT simulator is motivated by the difficulty of assessing the viability and performance of real deployment. To appreciate this difficulty, assume a blockchain-based IoT ecosystem scenario, presented by [34], where a firefighting station considers outsourcing the IoT infrastructure's deployment and operation to a specialised IoT service provider called IoTSP. For the sake of simplicity, the IoTSP is responsible for promptly reporting fire alerts to the firefighting station. Trust issues may emerge such that fire may occur without being noticed either because the IoTSP fails to report the fire incident or the firefighting station's system fails is unavailable. To resolve potential disputes, there is in place a service level agreement (SLA) that requires the IoTSP to emit fire alerts via a shared blockchain ledger (see Fig. 11). However, the examination of the overall viability and performance using real deployment settings may encounter some or all of the following hurdles, which include, but are not limited to,

- *complexity of real IoT deployment merely for experiments*: The complexity of real IoT deployment can be a major challenge when it comes to testing and evaluating the viability and performance of a blockchain-based IoT system. Setting up a real IoT deployment can be a time-consuming and resource-intensive process, as it requires the deployment of physical hardware and infrastructure, as well as the integration of various components and technologies. This complexity can make it difficult to conduct experiments and tests in a real deployment setting, particularly if the deployment is large or complex.
- *Lack of resources*: The lack of resources can be a significant challenge when it comes to testing and evaluating the viability and performance of a blockchain-based IoT system. Conducting experiments and tests in a real deployment setting can be resource-intensive, as it requires the deployment of physical hardware and infrastructure, as well as the integration of various components and technologies. This can be particularly challenging for organizations that do not have access to the necessary resources, such as funding, personnel, or technical expertise.

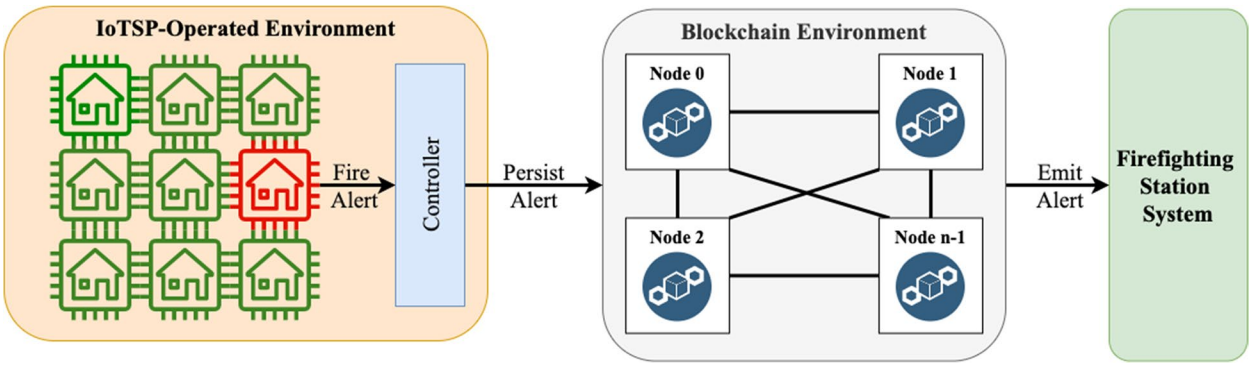

Fig. 11 Motivating Blockchain-based IoT Scenario: A firefighting station and IoT service provider (IoTSP) engage in an SLA where the conformance of the IoTSP is measured based on monitoring logs stored on a shared blockchain ledger

- *Lack of technical workforce*: The lack of a technical workforce can be a major challenge when it comes to testing and evaluating the viability and performance of a blockchain-based IoT system. Setting up a real IoT deployment can be a complex and technical process that requires specialized skills and expertise. This can be particularly challenging for organizations that do not have access to a sufficient number of technical personnel or do not have the necessary expertise in-house.
- *Cost inefficiency*: Conducting experiments and tests in a real deployment setting can be costly and inefficient, particularly if the deployment is large or complex. Setting up a real IoT deployment requires the deployment of physical hardware and infrastructure, as well as the integration of various components and technologies. This can be a time-consuming and resource-intensive process that may not be cost-effective for organizations, particularly if the deployment is only being used for testing and evaluation purposes.

Alternatively, simulation tools can help to overcome the complexity of real IoT deployment by providing a virtual environment for testing and experimentation, allowing for the creation of virtual IoT deployments without the need for physical hardware or infrastructure. They can also help to overcome the lack of resources and technical workforce by providing a more cost-effective and resource-efficient way to conduct experiments and tests and can help organizations assess the viability and performance of a blockchain-based IoT system even if they do not have access to the necessary resources or expertise. Finally, simulation tools can help to reduce the cost inefficiency associated with real deployment by providing a more cost-effective and efficient way to conduct experiments and tests, and by helping organizations to identify potential issues or bottlenecks before deployment.

Conceptual architecture

This section illustrates the conceptual architecture for the proposed Blockchain-based IoT simulator. As Fig. 12 depicts, the architecture is divided into three main components, namely, ***Configurator*** 8.1, ***Generator*** 8.2, ***Simulation core*** 8.3, and ***Reporter*** 8.4.

Configurator

The configurator component in the proposed conceptual model is responsible for setting various parameters for the IoT infrastructure and the blockchain network. This component allows you to specify the required workload for the IoT side using IoTsimOsmosis [27], which is an extension of CloudSim [23] that enables you to define various properties related to an IoT architecture, such as sensors, actuators, devices, edge units, networks topology, data centres, computing resources, tasks scheduling, and allocation policies.

On the blockchain side, the configurator enables you to specify an enterprise blockchain network, which should include essential elements such as the number of participating nodes (e.g. miners based on the IoT topology), block settings (e.g. size and difficulty), transaction settings (e.g. size, transaction delay, etc.), consensus algorithm (e.g. proof of work, Raft, etc.), and simulation setups (e.g. the number of running simulators).

The configurator component is an important part of the simulation process, for customising the parameters of the IoT infrastructure and blockchain network to meet the specific needs and requirements. By setting these parameters, you can better understand how different configurations might impact the performance and viability of the system.

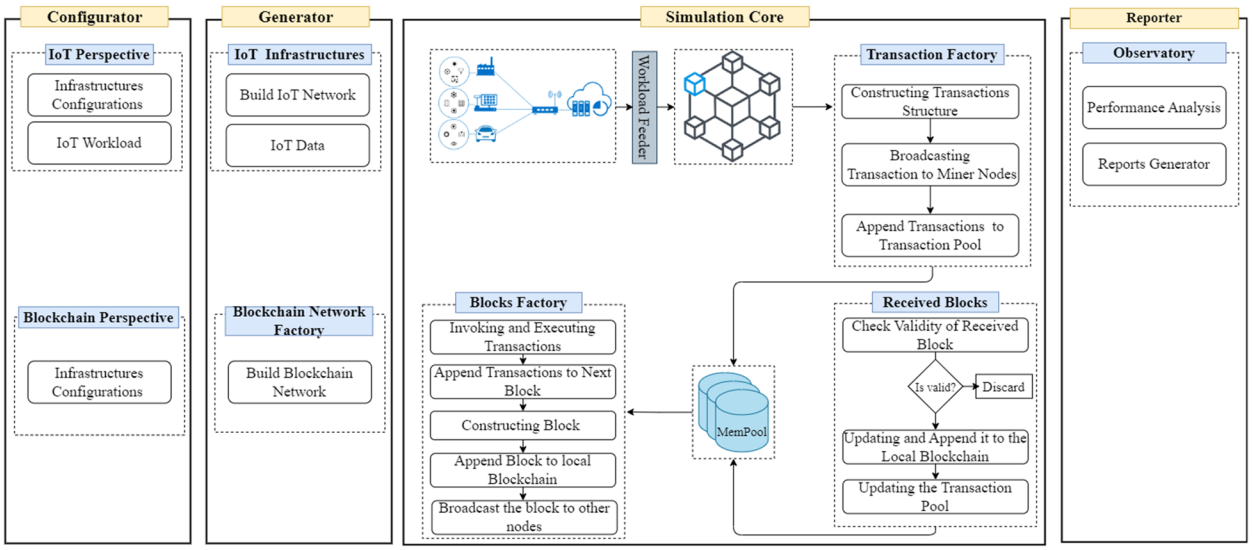

Fig. 12 An overview of the Conceptual Model for Simulating Blockchain-based IoT Ecosystems

Generator

Based on the specified configurations as we discussed in the Section Configurator 8.1, the generator component in the proposed conceptual model is responsible for creating the required infrastructure for the IoT application and the blockchain network based on the specified configurations. The generator component uses the parameters set by the configurator component to create the necessary components and connections for the IoT topology and the blockchain network.

For example, the generator component may create the necessary sensor nodes and edge units for the IoT topology, as well as the protocols for transmitting and receiving data. It may also create the participating nodes for the blockchain network, such as miners or validators, and configure the block settings, transaction settings, and consensus algorithm.

The generator component is an important part of the simulation process, for creating a realistic and functional model of the IoT application and blockchain network based on the specified configurations. This can be useful in testing and evaluating the performance and viability of the system under different scenarios and conditions.

Simulation core

The simulation Core in the proposed conceptual model typically consists of several main components that work together to simulate the operation of the system. These components include:

- *The transaction factory and workload feeder* are components in a simulation environment for a blockchain-based IoT system. The transaction factory is responsible for generating transactions based on the data collected from the workload feeder, while the workload feeder manages the flow of transactions and ensures that they are processed efficiently and accurately. The transaction factory follows a specific process to create and broadcast transactions, including:

  – *Construct a Transactions Structure*: The transaction factory prepares the format of the transactions to match the structure required by the blockchain network. This includes defining the data structure and required fields for the transactions, as well as any other requirements or constraints.
  – *Broadcast transactions to miner nodes*: Once construct a transaction structure, then broadcasts the prepared transactions to all nodes in the network in order to inform them of the new transactions.
  – *Appending the transactions to the transaction pool* a collection of pending transactions that are waiting to be added to the blockchain.

  The process of generating and managing transactions is typically repeated until no more transactions are being fed into the system by the workload feeder. Overall, the transaction factory and workload feeder play important roles in the simulation process by generating and managing the

flow of transactions within the system, and by helping to test and evaluate the performance and viability of the blockchain-based IoT system. In a blockchain network, miner nodes are responsible for creating blocks of transactions and adding them to the blockchain. When a miner receives transactions in its transaction pool, it will typically try to create a block by selecting a subset of the transactions from the pool and adding them to a new block. The process of creating a block is often referred to as an "event," as it represents a significant event in the operation of the blockchain network. In order to create a block, a miner must typically perform a consensus algorithm such as a proof of work, which involves using cryptographic algorithms to demonstrate the work that has been done to validate and include the transactions in the block. In a simulation environment, the aim may be to simulate the process of creating blocks and adding them to the blockchain in order to test and evaluate the performance of the network and the miner nodes. In the conceptual mode, we create a Block Factory component.

- **The block factory** is a component in a simulation environment for a blockchain-based IoT system. It is responsible for simulating the process of creating blocks and adding them to the blockchain. The block factory follows a specific process to create and execute transactions, including:

  – *Invoking and Executing Transactions*: The miner selects a subset of pending transactions from the transaction pool based on certain criteria, such as the time the transactions were created, the gas price associated with them, or the order in which they were received.
  – *Append Transactions to Next Block*: When a miner node receives transactions in its transaction pool, it will typically try to create a block by selecting a subset of the transactions from the pool and adding them to a new block. This process is known as "appending" the transactions to the block, as it involves adding the transactions to the block and preparing them for inclusion in the blockchain.
  – *Constructing block and append it to the local blockchain*: After the block has been created with its set of transactions.
  – *Append Block to local Blockchain*: Once the block has been constructed, it is ready to be appended to the local copy of the blockchain. This involves adding the block to the end of the local copy of the blockchain and updating the local copy to reflect the new block.
  – *Broadcast the block to other nodes*: The miner broadcasts the newly added block to all other nodes in the network in order to inform them of the new block and update their copies of the blockchain.

  Overall, the block factory plays a crucial role in the simulation process by helping to simulate the operation of the blockchain network and by providing valuable insights into its performance and viability. Once a block has been broadcasted to the blockchain network, it becomes the responsibility of the block receivers to validate the block and decide whether to accept it and add it to their copy of the blockchain. The process of validating a block involves verifying that the block meets all of the requirements and standards of the blockchain network. This may include checking the block header to ensure that it includes a valid reference to the previous block in the blockchain, and verifying the transactions contained in the block to ensure that they are valid and properly formatted. In the conceptual mode, we create the Received Blocks component.

- *Received Blocks*: a component in a simulation environment for a blockchain-based IoT system. It is responsible for receiving blocks that have been broadcasted to the network and deciding whether to accept them and add them to the local copy of the blockchain. The received blocks component typically follows a specific process when receiving a new block, which may include the following steps:

  – *Check Validity of Received Block* when receiving a new block, one of the key tasks of the Received Blocks component is to check the validity of the received block. This involves performing a series of validation checks on the block to ensure that it meets all of the requirements and standards of the blockchain network.
  – *Updating and Append it to the Local Blockchain* if the received block is deemed to be valid, the next step in the process is to update the local copy of the blockchain and append the received block to it. This involves adding the received block to the end of the local copy of the blockchain and updating the local copy to reflect the new block.
  – *Updating the transaction pool* Once the new block has been added to the local blockchain, the node will update the transaction pool by removing the transactions that were included in the

block. This leaves the transaction pool with only the transactions that have not yet been included in a block, allowing the node to continue the process of verifying and adding new transactions to the blockchain.

Reporter

The benchmark report is an important part of the simulation process, as it provides detailed information about the performance and viability of a blockchain-based IoT system. In our proposed conceptual model, once the simulation is finished, the simulator will prepare the benchmark report as an Excel file, which consists of several sheets each of which provides specific information about different aspects of the system as shown below

- *Configuration*: This provides important information about the parameters used to conduct the experiment, such as the type and number of nodes, the blockchain protocol used, and any other relevant system parameters. This information is important for understanding the context in which the simulation was conducted, and can help to identify any factors that may have influenced the performance of the system.
- *Overall result*: A benchmark report provides a summary of the overall performance of a blockchain-based IoT system. This includes a range of statistics that can be useful for understanding the system's performance and identifying any issues or opportunities for improvement. Some examples of the types of statistics that might be included in the "Overall result" section include:
  - Total number of blocks: This is the total number of blocks that were added to the blockchain during the simulation.
  - Total number of blocks including transactions: This is the total number of blocks that contained at least one transaction.
  - Total number of blocks without transactions: This is the total number of blocks that did not contain any transactions.
  - Average block size: This is the average size of the blocks in the blockchain.
  - Total number of transactions: This is the total number of transactions that were processed during the simulation.
  - Average number of transactions per block: This is the average number of transactions included in each block.
  - Average transaction inclusion time: This is the average time it took for a transaction to be included in a block.
  - Average transaction size: This is the average size of the transactions processed during the simulation.
  - Total number of pending transactions: This is the total number of transactions that were waiting to be processed at the end of the simulation. Average block propagation time: This is the average time it took for a block to be propagated (i.e., disseminated) to all nodes in the network.
  - Average transaction latency: This is the average time it took for a transaction to be processed and added to the blockchain.
  - Transaction execution: This is the percentage of transactions that were successfully processed during the simulation.
  - Transaction throughput: This is the number of transactions that were processed per second.
- *Blocks overview*: A benchmark report provides details about the individual blocks that were added to the blockchain during the simulation. This includes information such as the block ID, previous block ID, block depth, block timestamp, block size, number of transactions, and the minter (the node responsible for creating the block). This information can be useful for understanding the overall performance of the system at the block level.
- *Transactions latency overview*: A benchmark report provides details about the latency of individual transactions in a blockchain-based IoT system. Latency refers to the time it takes for a transaction to be processed and added to the blockchain, and it can have a significant impact on the overall performance of the system. Included in this section are details about the transaction latency of each transaction, including the transaction ID, creation time, confirmation time, and transaction latency. This information can be useful for understanding the overall performance of the system at the transaction level.
- *Pending Transactions overview*: A benchmark report provides details about transactions that were not executed during the simulation. These transactions may not have been executed for a variety of reasons, such as being delayed due to insufficient resources or other issues.
- *Statistic*: A benchmark report provides statistical information about the performance of a blockchain-based IoT system. Specifically, it provides details about the distribution of block time and block latency, including the minimum, maximum, mean, and standard deviation of these metrics.

Evaluation

During the evaluation process, we presented the conceptual model of the blockchain simulator to a group of experts and invited them to discuss and provide feedback on the model. We clarified any unclear areas and used a questionnaire to gather structured feedback from the participants based on their knowledge and experience. The questionnaire-based approach allowed us to gather detailed and structured feedback on the model and its various components, and we used this information to test the validity of the conceptual model. We had defined objectives for the evaluation process and will be presenting our findings in the following sections.

Participants

Our planned initiative is intended for experts in the fields of the Internet of Things (IoT) and blockchain technology. We conducted a study with 10 participants, all of whom were doctoral candidates with a focus on research related to blockchain, smart cities, and other IoT topics. The participants' research interests included cloud computing, edge computing, smart contract-based service level agreements in the IoT, and blockchain-based IoT. The scientific interests of each participant are summarized in the Table 3.

Procedure

The evaluation of the conceptual model was conducted using a focus group and a questionnaire. Focus groups are a useful technique for gathering detailed and in-depth feedback from a group of individuals. During the focus groups, we discussed the conceptual model with the participants and invited them to provide their thoughts and opinions. The participants then completed a questionnaire that included both closed-ended and open-ended questions to provide more detailed feedback on the model. The use of both focus groups and a questionnaire allowed us to gather a wide range of perspectives and insights on the model.

The focus group began with a presentation on the challenges of implementing Blockchain and IoT. We also mentioned the limitations of current simulators. Next, the participants were asked to read and analyze the framework of the IoTOsmosis simulator [27]. To further clarify the concept, we provided a use case example. Finally, we introduced the conceptual model and asked the participants to complete a questionnaire consisting of four closed-end questions and two open-end questions related to the conceptual model.

- *Questionnaire*

  1 *To what extent are you satisfied with the conceptual model?*
  2 *To what extent are you satisfied with the conceptual model's generality?*
  3 *Assuming that IoTOsmosis is the base IoT simulator in the conceptual model, to what extent do you agree that it covers your requirements?*

  – ease of use
  – configurability
  – extensibility
  – maintainability
  – network topology

  4 To what extent does the blockchain part cover your requirements?

- *Focus Group*

  1 *What are your overall thoughts on the conceptual model for the blockchain simulator?*
  2 *Do you believe the conceptual model for the blockchain simulator is comprehensive and well-designed, or are there any areas that you feel need further improvement or refinement?*

Table 3 A brief description of participants' research interests

Participant	Research Interest
1	Blockchain technology and IoT applications
2	Blockchain performance
3	Blockchain-based SLA in the context of IoT
4	Data privacy in the context of IoT via blockchain
5	Allocating Cloud resources & blockchain
6	Optimization blockchain with the internet of Vehicles (IoV)
7	IoT & Blockchain
8	Research related to IoT, Cloud and Blockchain
9	IoT data management, and blockchain
10	Remote health monitoring using IoT and blockchain

Experimental results

Questionnaire

To validate the proposed conceptual model, we distributed a questionnaire to 10 participants. The questionnaire began by asking about their satisfaction with the conceptual model and its applicability. Specifically, we asked the participants, "To what extent are you satisfied with the conceptual model?" The results, shown in Fig. 13, indicate that the majority of participants were satisfied, with 60% expressing satisfaction and 30%

Fig. 13 Participant satisfaction with the conceptual model

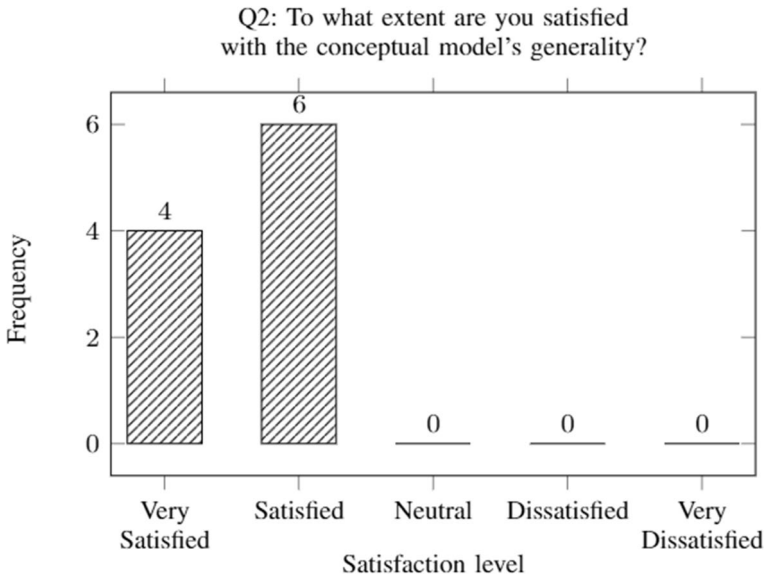

Fig. 14 Participant satisfaction with the conceptual model's generality

expressing complete satisfaction. 10% were neutral about the model.

Next, the participants were asked about their thoughts on the applicability of the conceptual model. The results of this question are shown in Fig. 14. It's worth noting that there is complete agreement about the model, with 40% of participants indicating that they were completely satisfied and 60% indicating that they were satisfied. Based on these results, we can confirm that the proposed conceptual model is a good fit.

Four questions were asked to assess the usability, configurability, maintainability, and available network topology of the IoTOsmosis simulator, which is at the core of the proposed conceptual model. Specifically, the participants were asked about their level of agreement with the ease of use of the simulator ("To what extent do you agree with its ease of use?"). The results, shown in Fig. 15, indicate that 30% completely confirm the simulator's usability, while 40% agree with its ease of use. 20% were neutral about the simulator, and 10% disagree with its ease of usability.

Additionally, the participants were asked about the configurability of the IoTOsmosis simulator ("To what extent do you agree with its configurability?"). The

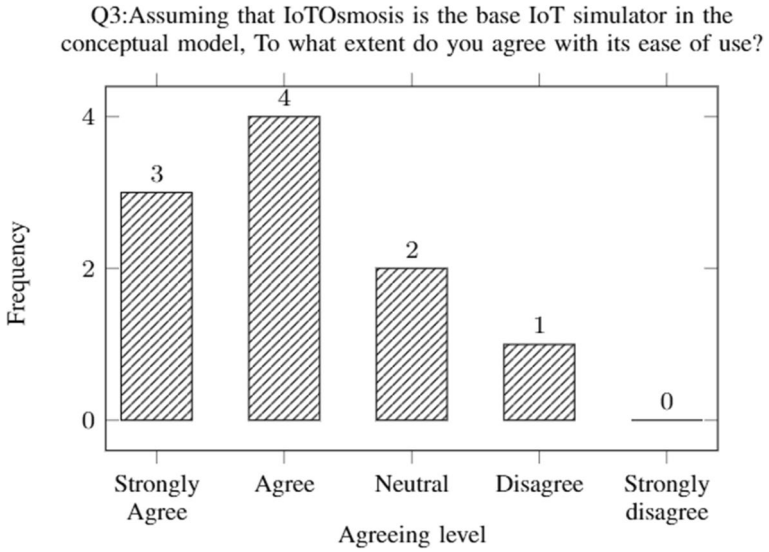

Fig. 15 Participant agreement with the ease of use of the IoTOsmosis simulator

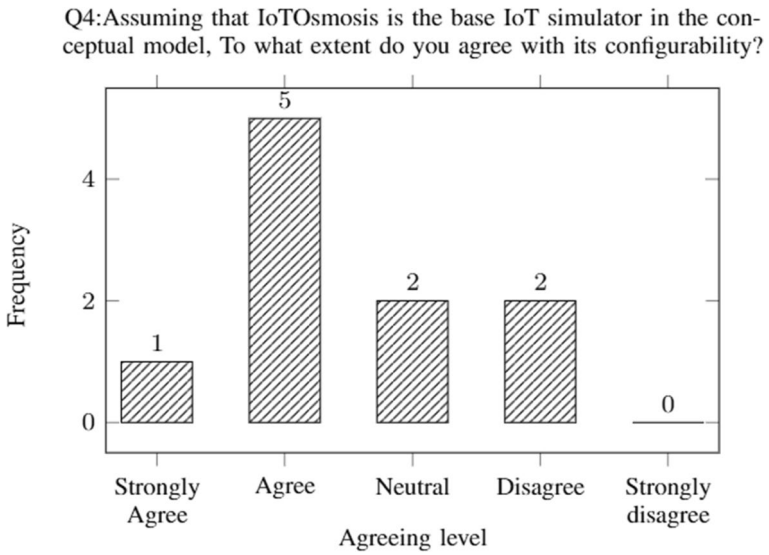

Fig. 16 Participant agreement with the configurability of the IoTOsmosis simulator

results, shown in Fig. 16, show that 60% of participants (10% completely agree and 50% agree) are satisfied with the simulator's configurability. 20% had neutral or disagreeing opinions. The participants were also asked about the maintainability of the simulator ("To what extent do you agree with its maintainability?"). The results, shown in Fig. 17, indicate a clear agreement with 70% of participants (20% strongly agree and 50% agree) indicating satisfaction. 20% disagreed with the ease of maintainability, while 10% were neutral. A final question about the IoTOsmosis simulator was "To what extent do you agree with the network topology?" The results are shown in Fig. 18.

Finally, the questionnaire concluded by asking the participants about their thoughts on the ability of blockchain to meet their requirements. The results are shown in Fig. 19. A closer look at the figure reveals a high level of agreement (30% strongly agree and 50% agree) in the usefulness of blockchain. There was an equal number of neutral (10%) and disagreeing (10%) opinions.

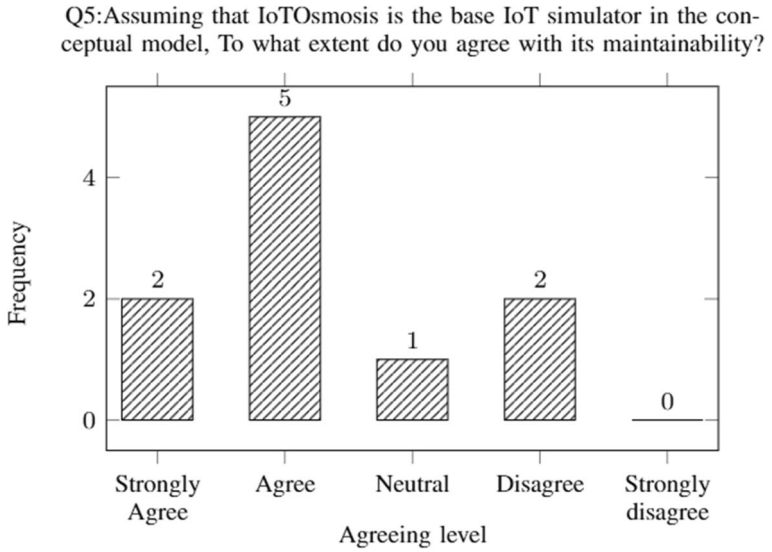

Fig. 17 Participant agreement with the maintainability of the IoTOsmosis simulator

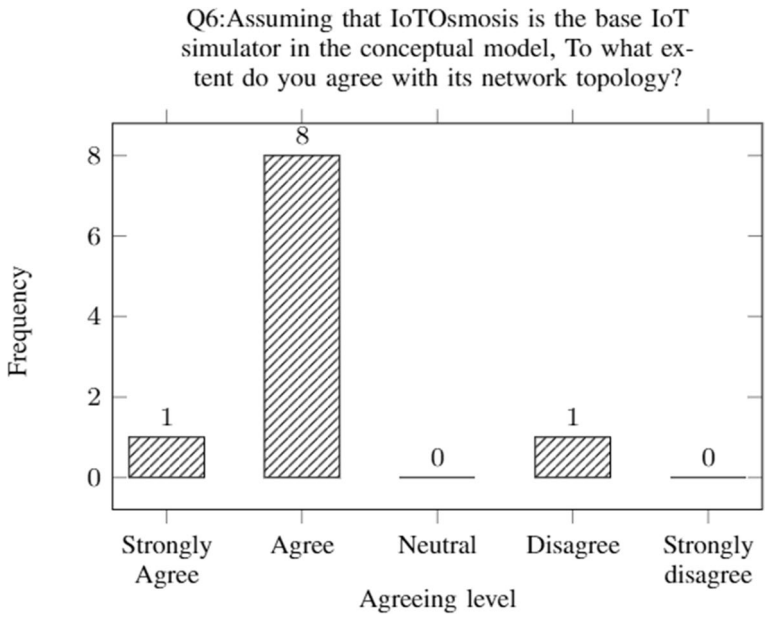

Fig. 18 Participant agreement with the effectiveness of the blockchain part in meeting their requirements

Overall, a questionnaire was distributed to 10 participants to validate the proposed conceptual model for a blockchain-based Internet of Things (IoT) simulator. The questionnaire asked participants about their satisfaction with the conceptual model and its applicability, as well as their thoughts on the usability, configurability, maintainability, and network topology of the IoTOsmosis simulator, which is at the core of the proposed model. The participants were also asked about the effectiveness of the blockchain part in meeting their requirements. The results of the questionnaire showed that the majority of participants were satisfied with the conceptual model and its applicability, with 40% expressing complete satisfaction and 60% expressing satisfaction. The results also indicated that the IoTOsmosis simulator was generally well-received, with most participants expressing satisfaction with its usability, configurability, maintainability, and network topology. Additionally, a high level of agreement

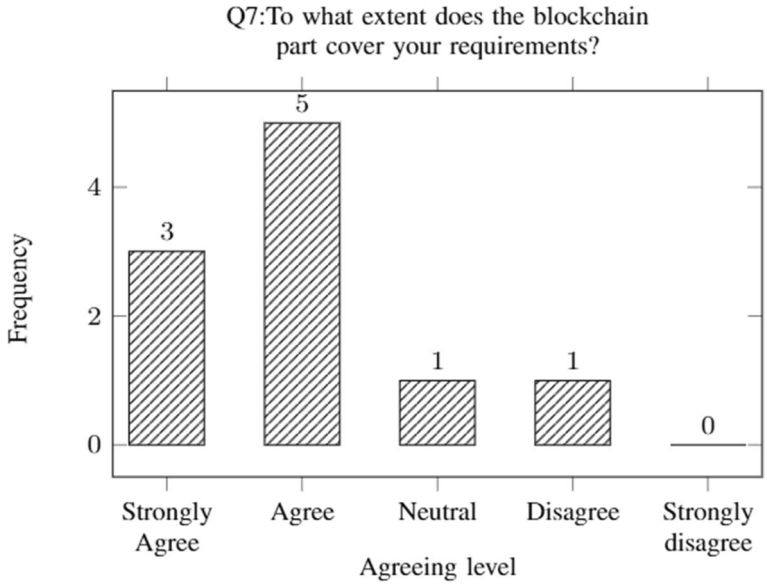

Fig. 19 Participant agreement with the effectiveness of the blockchain part in meeting their requirements

Table 4 Aligning the questionnaire questions with the predefined objectives

Question	Objective (1)	Objective (2)	Objective (3)
Q1	✓		
Q2	✓		
Q3		✓	
Q4			✓

was observed regarding the usefulness of blockchain in meeting participants' requirements, with 30% strongly agreeing and 50% agreeing. Based on these results, it can be concluded that the proposed conceptual model is a good fit. To provide a complete overview, Table 4 shows how the questionnaire questions align with the predefined objectives.

Focus group

P1 stated that *"I believe that the conceptual model is well-designed and comprehensive, and it appears to include a set of key features and capabilities necessary for effectively simulating and evaluating blockchain-based IoT systems. I think that these capabilities will be crucial for understanding and optimizing the performance of blockchain-based IoT systems and for identifying any potential issues or challenges that may arise during deployment".*

P2 stated that *"Overall, I think the conceptual model is solid and well thought-out. It covers all of the key components and functions that I would expect to see in a simulator of this kind, and it seems like it would be relatively straightforward to implement based on the design that has been presented. There are a few areas where I think the model could be improved. For example, it might be helpful to have more granular control over the various parameters and settings of the simulator, such as the ability to specify the type of consensus algorithm or the block size".*

P3 stated that *"I believe the conceptual model is a promising concept. The wide range of features and capabilities included in the conceptual model is impressive. Also, the simulation core seems to be well-designed, with components such as the transaction factory and workload feeder, the consensus component, and the monitoring and evaluation components. However, it might be helpful to have more options for customizing the simulation, such as the ability to specify different types of transactions or to customize the workload feeder in greater detail".*

P4 stated that *"As a beginner in the fields of blockchain and IoT, I found the conceptual model of the simulator to be easy to understand and well-structured. It effectively explains the various components and their functions and provides a helpful overview of how they work together. While the concept model is clear, it would be beneficial to include more information about the specific consensus algorithms that will be implemented in the implementation phase. This added detail would help to further clarify the inner workings of the simulator".*

P5 stated that *" The conceptual model of the simulator appears to be very promising, as it includes a number of metrics that allow users to get a sense of how it will perform in the real world. However, it might be useful to make*

the model more flexible by allowing it to be deployed in different layers rather than just the edge layer. This would give users more control over where and how they deploy the blockchain network and make it easier to adapt to different use cases and environments".

P6 stated that *"The conceptual model of the simulator is well-designed. It provides a means to evaluate the performance of different blockchain and IoT solutions and helps users to identify potential challenges and issues. The inclusion of a monitoring component is a particularly useful feature that enables users to track the performance of the system over time and identify any changes".*

P7 stated that *"In my opinion, the architecture of the simulator is well-designed and comprehensive. It includes most of the necessary features for evaluating blockchain-based IoT systems. However, there may be potential for further improvement in terms of its ability to simulate enterprise blockchain environments and its integration with other simulators beyond IoTSim-Osmosis. Enhancing these capabilities would increase the versatility and usefulness of the simulator for a wider range of applications".*

P8 stated that *"I think the conceptual model is good because it includes a variety of features. One aspect of the model that I really appreciate is the generator component, which makes the model integrated with different simulators".*

P9 stated that *"I think the model is a strong foundation for further research and development. It covers a wide range of important features and capabilities, and it seems like it would be useful for a variety of different applications. I do think there are a few areas where the model could be improved or expanded upon. For example, simulation capabilities to evaluate the performance of the simulator under different conditions. Additionally, it would be helpful to have more options for generating and analyzing results, such as the ability to compare different simulation scenarios or to run simulations over longer periods of time".*

P10 stated that *"I think the proposed conceptual model is good, and the inclusion of the configurator component is a great idea, as it allows users to customize the parameters of the simulation to meet their specific needs and requirements. However, I think it would be helpful to have more options for configuring the blockchain network, such as the ability to specify different types of consensus algorithms or to customize the block settings in greater detail".*

Through analysing the participants' responses as shown in Table 5, the result of the evaluation of the conceptual model showed that it is generally well-regarded. The reason underpinning this attitude is the inclusion of a wide range of key features and capabilities that make it a suitable foundation for creating a simulation environment for blockchain-based IoT applications. However, there are also a few areas where the model could be improved or expanded upon. Some participants have suggested adding more granular control over the various parameters and settings of the simulator. Others have suggested including more information about the specific consensus algorithms that will be implemented in the implementation phase and making the model more flexible by allowing it to be deployed in different layers. To provide a complete overview, Table 6 shows how the questionnaire questions align with the predefined objectives.

Table 6 Aligning the questionnaire questions with the predefined objectives

Question	Objective (1)	Objective (4)
Q1	✓	
Q2	✓	✓

Table 5 Summary of feedback on the conceptual model for the blockchain simulator from participants in the evaluation process. Participants provided overall thoughts on the model, as well as suggestions for areas of improvement

Participant	Overall Thoughts	Areas for Improvement
P1	Well-designed and comprehensive	
P2	Solid and well-thought-out	More granular control over parameters and settings
P3	Promising concept	More options for customizing the simulation
P4	Easy to understand and well-organized	Consensus algorithms
P5	Very promising	Flexibility to deploy BC in different IoT layers
P6	Well-designed	
P7	Comprehensive and well-designed	Ability to simulate enterprise blockchain and support different IoT simulators
P8	Good	
P9	Strong foundation	Configuring the blockchain network
P10	Good	

Conclusion and future work

IoT systems are becoming increasingly common, but their centralization introduces limitations. However, it is expected that blockchain technology could potentially overcome these limitations and unlock new opportunities for IoT. A major challenge is that there is currently no reliable simulator for evaluating the use of blockchain as a solution for IoT problems. This drives our current efforts to research and design a simulator for this purpose. To gain a deeper understanding of this notion, we conducted two studies, which included a questionnaire and interviews with experts. The questionnaire results showed a high level of familiarity with both IoT and blockchain, as well as a strong belief that blockchain could address various challenges faced by IoT. This belief was further supported by the expert interviews. Through these studies, we discovered that a major challenge is the lack of a simulator environment that can accurately simulate blockchain-based IoT applications. Motivated by this, we have developed a conceptual model as a foundation for creating a simulation environment for blockchain-based IoT applications. To ensure the effectiveness of the conceptual model, we employed two research methods which included a questionnaire and a focus group with experts. The evaluation of the conceptual model revealed that it is generally well-received due to its comprehensive range of key features and capabilities that make it an ideal foundation for building a simulation environment for blockchain-based IoT applications. Our future work aims to create and validate a simulation environment for blockchain-based IoT applications, allowing for the testing and validation of blockchain-based IoT systems before they are deployed in the real world.

Acknowledgements
We thank the Program Committee of IEEE SmartIoT for inviting us to extend our previous study [28] and submit it to this Journal.

Authors' contributions
Designing and collecting data for investigating the requirements for building a blockchain simulator for IoT Applications was carried out by A. Albshri and B. Awaji; A. Albshri analyzed the results. The methodology was developed by A. Albshri and A. Alzbuaidi; The conceptual architecture was developed by A. Albshri and A. Alzbuaidi; A. Albshri and A. Alzbuaidi designed and executed the data collection and evaluation; A. Albshri analyzed the results. The manuscript was drafted by A. Albshri; then, reviewed and edited by A. Albshri, E. Solaiman, A. Alzbuaidi, M. Alharby, K. Mitra and B. Awaji; E. Solaiman is the principal investigator (lead supervisor) of the project. All authors have reviewed and approved the manuscript.

Funding
This work is funded in part by the EPSRC, under grant number EP/V042017/1. Scalable Circular Supply Chains for the Built Environment.

Availability of data and materials
All data created during this research are available at GitHub\footnote{\url{https://github.com/AlbshriAdel/conceptual-architecture-data}}.

Declarations

Ethics approval and consent to participate
This study was conducted under the ethical approval referenced as 9845/2020 and obtained from the Ethics Committee of Newcastle University-United Kingdom.

Competing interests
The authors declare no competing interests.

Received: 31 December 2022 Accepted: 1 July 2023
Published online: 14 July 2023

References

1. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): A vision, architectural elements, and future directions. Futur Gener Comput Syst 29(7):1645–1660
2. Da Xu L, He W, Li S (2014) Internet of things in industries: A survey. IEEE Trans Ind Inform 10(4):2233–2243
3. Ejaz M, Kumar T, Ylianttila M, Harjula E (2020) Performance and efficiency optimization of multi-layer IoT edge architecture. In: 2020 2nd 6G Wireless Summit (6G SUMMIT), IEEE, pp 1–5
4. Zhong CL, Zhu Z, Huang RG (2015) Study on the IoT architecture and gateway technology. In: 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), IEEE, pp 196–199
5. Vangala A, Das AK, Kumar N, Alazab M (2021) "Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective,". IEEE Sensors J 21(16):17591–607. https://doi.org/10.1109/JSEN.2020.3012294.
6. Li W, Wu J, Cao J, Chen N, Zhang Q, Buyya R (2021) Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions. J Cloud Comput 10(1):1–34
7. Hosseinian H, Damghani H (2019) Smart home energy management, using IoT system. In: 2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI), IEEE, pp 905–910
8. Delgado-Segura S, Pérez-Solà C, Herrera-Joancomartí J, Navarro-Arribas G, Borrell J (2018) Cryptocurrency networks: A new P2P paradigm. Mob Inf Syst 1–16
9. Washbourne L (2015) A survey of P2P network security. arXiv preprint https://arxiv.org/abs/1504.01358
10. Li J, Wu J, Chen L (2018) Block-secure: Blockchain based scheme for secure P2P cloud storage. Inf Sci 465:219–231
11. Samaniego M, Deters R (2018) Zero-trust hierarchical management in IoT. In: 2018 IEEE International Congress on Internet of Things (ICIOT), pp 88–95. https://doi.org/10.1109/ICIOT.2018.00019
12. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus Rev 21260. https://nakamotoinstitute.org/bitcoin/.
13. Memon RA, Li JP, Nazeer MI, Khan AN, Ahmed J (2019) Dualfog-IoT: Additional fog layer for solving blockchain integration problem in internet of things. IEEE Access 7:169,073–169,093
14. Haverkort BR (1998) Performance of computer communication systems: a model-based approach. John Wiley & Sons Inc
15. Ferretti S, D'Angelo G (2020) On the ethereum blockchain structure: A complex networks theory perspective. Concurr Comput Pract Experience 32(12):5493
16. Harbers M, Bargh M, Pool R, Van Berkel J, Van den Braak S, Choenni S (2018) A conceptual framework for addressing IoT threats: challenges in meeting challenges. In: Proceedings of the 51st Hawaii International Conference on System Sciences. https://scholarspace.manoa.hawaii.edu/items/834983e4-a18b-442f-8c57-16aab8efbb21.
17. Albshri A, Alzubaidi A, Awaji B, Solaiman E (2022) Blockchain simulators: A systematic mapping study. In: 2022 IEEE International Conference on Services Computing (SCC), pp 284–294. https://doi.org/10.1109/SCC55611.2022.00049
18. Markus A, Kertesz A (2020) A survey and taxonomy of simulation environments modelling fog computing. Simul Model Pract Theory 101:102042

19. Stoykov L, Zhang K, Jacobsen HA (2017) Vibes: fast blockchain simulations for large-scale peer-to-peer networks. In: Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos. New York, Association for Computing Machinery. pp 19–20. https://dl.acm.org/doi/10.1145/3155016.3155020.
20. Faria C, Correia M (2019) Blocksim: blockchain simulator. In: 2019 IEEE International Conference on Blockchain (Blockchain), IEEE, pp 439–446
21. Alharby M, van Moorsel A (2019) Blocksim: a simulation framework for blockchain systems. ACM SIGMETRICS Perform Eval Rev 46(3):135–138
22. Pandey S, Ojha G, Shrestha B, Kumar R (2019) Blocksim: A practical simulation tool for optimal network design, stability and planning. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, pp 133–137
23. Calheiros RN, Ranjan R, Beloglazov A, De Rose CA, Buyya R (2011) Cloudsim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Softw: Pract Experience 41(1):23–50
24. Wickremasinghe B, Calheiros RN, Buyya R (2010) Cloudanalyst: A cloudsim-based visual modeller for analysing cloud computing environments and applications. In: 2010 24th IEEE International Conference on Advanced Information Networking and Applications, pp 446–452. https://doi.org/10.1109/AINA.2010.32
25. Gupta H, Vahid Dastjerdi A, Ghosh SK, Buyya R (2017) ifogsim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments. Softw: Pract Experience 47(9):1275–1296
26. Zeng X, Garg SK, Strazdins P, Jayaraman PP, Georgakopoulos D, Ranjan R (2017) IoTSim: A simulator for analysing IoT applications. J Syst Archit 72:93–107
27. Alwasel K, Jha DN, Habeeb F, Demirbaga U, Rana O, Baker T, Dustdar S, Villari M, James P, Solaiman E, Ranjan R (2021) IoTSim-osmosis: A framework for modeling and simulating IoT applications over an edge-cloud continuum. J Syst Architect 116(101):956
28. Albshri A, Awaji B, Solaiman E (2022) Investigating the requirement of building blockchain simulator for IoT applications. In: 2022 IEEE International Conference on Smart Internet of Things (SmartIoT), pp 232–240. https://doi.org/10.1109/SmartIoT55134.2022.00044
29. Doran GT et al (1981) There'sa smart way to write management's goals and objectives. Manag Rev 70(11):35–36
30. Creswell JW, Clark VLP (2017) Designing and conducting mixed methods research. Sage Publications
31. Nunnaly JC, Bernstein IH (1978) Psychoneric theory, 2nd edn. McGraw-Hil
32. Pope C, Ziebland S, Mays N (2000) Analysing qualitative data. BMJ 320(7227):114–116
33. Gill P, Stewart K, Treasure E, Chadwick B (2008) Methods of data collection in qualitative research: interviews and focus groups. Br Dent J 204(6):291–295
34. Alzubaidi A, Mitra K, Solaiman E (2021) Smart contract design considerations for SLA compliance assessment in the context of IoT. In: 2021 IEEE International Conference on Smart Internet of Things (SmartIoT), pp 74–81. https://doi.org/10.1109/SmartIoT52359.2021.00021

Publisher's Note