Hindawi
Scientific Programming
Volume 2022, Article ID 3944200, 12 pages
https://doi.org/10.1155/2022/3944200

Research Article

The Blockchain Framework for the Sharing of Data between Training Providers Based on the Internet of Things

Sara Jeza Alotaibi

Associate Professor, Web Technologies, Institute of Public Administration, Riyadh, Saudi Arabia

Correspondence should be addressed to Sara Jeza Alotaibi; alotaibisar@ipa.edu.sa

Received 3 August 2022; Revised 18 September 2022; Accepted 23 September 2022; Published 13 October 2022

Academic Editor: Sheng Du

Blockchain technology is recognised as being a key focus when it comes to modern-day studies and interest on a global scale, with the new block of transactions responsible for the continued growth and expansion of a distributed ledger that details transactional data, complete with immutable and verifiable structures. A greater degree of transparency, privacy, security, and traceability is provided by blockchain when a comparison is drawn with more conventional strategies. As a result of its secure and more progressive elements, blockchain is applied in a number of different arenas, including digital transactions, education, the healthcare industry, the Internet of Things (IoT), trade finance, and the training sector. Importantly, a notable effect on all applied fields has been witnessed as a result of blockchain technology, with data and transactional reliability, as well as privacy, recognised as the most important aspects when it comes to data-sharing in the training arena specifically. Very few models and frameworks are aligned with the guidelines put forth in this sector; as such, this report seeks to consider the pressing need to determine a model and framework to facilitate the sharing of data between training providers in line with the IoT. This study, therefore, centres on the creation of a blockchain model, with the creation of a sole recognition system for professionals seen to be advantageous for all such providers, specifically in the mind of providing a greater degree of clarity and simplification to the system in line with the IoT. The suggested model is focused on a number of different elements that have been identified as a result of studied theories, with consideration of the three different standpoints and professional assessments of 16 unique items.

1. Introduction

Blockchain and IoT technology development have together been the focus of much attention from a number of different areas [1], with blockchain recognised as an innovative technology [2] that has been steadily improving and increasing in recognition during recent years [31]. Blockchain is recognised in line with its decentralisation, high credibility, high security, programmability [3], and traceability [4], with true data information expected to be highlighted [5], training provider and user trust to be enhanced, issues pertaining to slow, difficult, and secure relationships to be overcome and efficiency improvements to be witnessed [34]. At a physical level, the exchange of data between two individuals may occur without any third party being involved [4], with such a transaction referred to as a peer-to-peer transaction [33]. At the digital level, however, data exchange are seen to involve a third party [5], such as a government entity, as an example [32].

The interest in blockchain technology, as a distributed ledger [6], is known to have increased in recent years as a result of a number of different elements [35]. During the beginning of the twenty-first century [7, 8], for example, blockchain technology became known for its capability to facilitate the use of cryptocurrencies, such as Bitcoin [36–38]. Blockchain, as a concept, was first detailed in 1991, with this technology recreated by Satoshi Nakamoto [7–9] with the introduction of the first blockchain-based cryptocurrency (Bitcoin) [45–47]. When it comes to the way in which blockchain is defined, it is recognised as a ledger of decentralised data, which benefits from secure sharing [10]. This particular technology facilitates a collective group of different users to participate in data [9]. When it comes to blockchain cloud services, a number of different sources' transactional data may be effortlessly gathered, combined, and shared, with data being broken down into different blocks, which are chained together—all with unique identification codes [8–11], notably in the form of cryptographic hashes—which are then shared. Such technology maintains the integrity of data with an individual source of truth, eradicating the duplication of data and thereby enhancing security as a whole [37–39].

Blockchain technology is believed to be the next big thing, with transaction accountability [10], data transparency [40], nonintermediary transactions, and data symmetry—all elements that are viewed as promising and valuable [41]. Educational systems and the training sector are viewed as being well-positioned to benefit from such a technology [12], with many transformations expected [44]. Furthermore, blockchain could have significant effects when it comes to data analytics [13], trust [14], and a number of other arenas [42, 43].

During the past ten years, blockchain technology has emerged, garnering a great deal of interest in both educational [6] and training arenas [15], with the majority of employers utilising external training entities to deliver training for lower-level staff [45]. There are two key types of training entities [7], namely independent providers and further education colleges, both of which could fall into voluntary [16], private, or public sectors [46].

When it comes to training entities that provide lower-level staff, such as apprentices, with qualifications, some are known to be in receipt of government funding through partnerships with skills agencies [17], whereby some training might be provided through subcontracting agreements with other businesses [48, 49]. Each training provider is seen to be responsible for delivering varied employer-focused support, such as the following:

(i) Training initiatives that direct attention to the needs of the apprentice;

(ii) establishing the most appropriate apprenticeship in line with organisational needs;

(iii) hiring an apprentice;

(iv) authenticating user validation systems;

(v) examining and checking apprentice progress and accordingly providing feedback; and

(vi) delivering training that supports apprentices in terms of knowledge and other learning.

In the main, training providers commonly save such information for employers [18] and other users without involving themselves in data-sharing from one training provider to the next [32], notably through the use of technology, such as IoT [40–47].

There has been much expansion when it comes to IoT development [18], with a third wave witnessed [47, 48]. The most important of all IoT elements is intelligence, which links different elements to uniquely establish and manage data [20], and accordingly realise intelligent management, with the mind of enhancing accessibility, efficiency, and usability [48–50]. IoT technology is centred on achieving Internet expansion, with innovations and developments able to be made in terms of information- and data-sharing, meaning that training providers can gather what is needed [19, 20], with emphasis on doing so both directly and securely [50, 51]. Accordingly, data-sharing may be achieved with the IoT and blockchain in combination. Importantly, there are many IoT devices implemented in mind for reporting [21] and controlling environmental changes [45], facilitating data-sharing, preventing risks, and creating a number of advantageous services [52]. Nonetheless, such advantages could ultimately create issues in line with a number of different privacies [22] and security concerns [49, 50]. In more recent years, blockchain has been seen to be a developing technology that is able to fulfil a number of different use cases beyond cryptocurrency, such as IoT integration with blockchain adoption; however, further research is required in line with resource-limited IoT devices [20–22] and ledger-based blockchain protocol design [52]. Nonetheless, such works have not provided a comprehensive formula on how blockchain frameworks can be designed with the mind of sharing data between government establishments [21], specifically training providers [51–53].

The question underpinning the research is centred on establishing a conceptual model, which may be answered by examining all present system frameworks and articles on the theoretical blockchain framework for data sharing between training providers based on the Internet of things. Accordingly, the question at the core of the study is as follows:

> RQ: What model may be applied to provide conceptual guidance when it comes to the creation of the blockchain framework for data sharing between training providers based on the Internet of things?
>
> In mind of answering the above question, two subquestions have been devised:
>
> RQ1: How may a suggested model be defined? This will be answered in Section 3.
>
> RQ2: How may the suggested model be measured? This will be answered in Section 4.

This report is broken down into five different sections, as follows: Section 2 provides a literature review pertaining to the area in question; Section 3 then provides a critical review and comparison concerning present models, with varying criteria and chosen elements and further highlights how the framework is proposed in line with the various attributes pertaining to the study area. Subsequently, Section 4 showcases the way in which assessment stages are developed and applied in mind of measuring alignment on the different aspects of the suggested model, as well as an expert evaluation. Lastly, Section 5 presents a conclusion and answers to the research question.

2. Related Work

Blockchain technology is receiving much focus as a result of its key benefits, notably concerning trust [2–8], transparency, and decentralisation [52–54]. It is known that the distributed network has a decentralised framework, with the

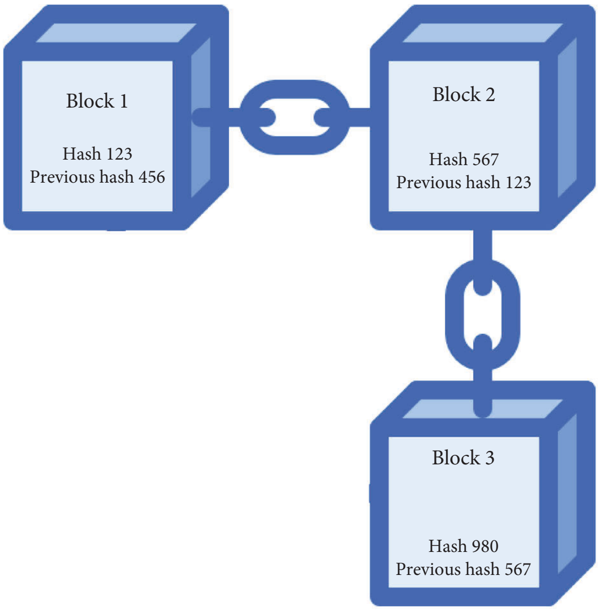

Figure 1: Blockchain components.

ledger determined [5–7]and maintained by network nodes, with trust easily attained without any third-party involvement [53–55]. In the blockchain, trust is essentially ensured by a number of different components within the blockchain [8], all of which are visible to all nodes and the public, thereby attaining transparency [56]. Upon the publication of a block to the blockchain, it then cannot be removed, nor can it be modified [9–11], which ultimately attains non-repudiation, which is 10 ecognized as being the last element of the blockchain [55–57].

When it comes to a clear definition, a blockchain may be recognised as a distributed database facilitating its users [11], i.e., blockchain nodes, to store and share data as blocks, both securely and in real times [54–58]. All blocks are linked to the preceding block, thereby creating a chain. Blockchain is accordingly devised from numerous blocks, each of which contains data needing to be stored, comprising a hash (notably a unique code identifying the data held within the block), and a hash record pertaining to the chain's previous block (see Figure 1) [12–14]. Should any of the blocks be the subject of any interference, whether on the block fingerprint or has, all subsequent chain blocks are notified of the tampering, with the hash of the block being tampered with no longer matching previous records. Through this approach to linking, tampering becomes near impossible [52–59].

As detailed in Figure 2 and Table 1 below, a number of different elements are identifiable in blockchains, though these differ from one type of blockchain to the next.

2.1. Public Blockchains. Permissionless in nature, public blockchains are completely decentralised [23] and allow anyone to join [54–60]. Such blockchains provide all blockchain nodes with equal rights when it comes to access [61], creation, and validation, with access restrictions not in place [23, 24]. Furthermore, owing to its decentralised structure, no single node controls the network [25], with a secure network provided as a result of the data not being modifiable upon network publication, which reduces the risk of a 51% attack [55–59].

When it comes to consensus mechanism, public blockchains tend to align with proof of stake (PoS) and proof of work (PoW), with public blockchain improving trust overall owing to the public distribution of data in the network [61], meaning the modification of data is almost impossible, as is application protection from developers [23–25]. This provides various benefits with low costs, with Bitcoin providing savings when contrasted alongside central party-dependent systems [26]. Nonetheless, there are a number of drawbacks to this type of blockchain, specifically when it comes to the system's computational power [60–62]. Thus far, the main use of public blockchains pertains to the exchange and mining of cryptocurrency, with miners essentially adopting the role of an innovative form of bank teller, with miners receiving a fee for their efforts.

2.2. Private Blockchains. Sometimes referred to as permissioned or managed blockchains [23], private blockchains are managed by an individual entity [25], with a node able to adopt the role of central authority [60–63].

Private blockchains are created and managed by particular businesses when it comes to their requirements and may be recognised as an additional layer of security that achieves access abilities by facilitating particular actions by different identifiable members [24–26]. This particular form of blockchain is not as widely utilised as the public one, although it is the preference when it comes to individuals in need of privacy, security, and a particular identity system [25]. Such a blockchain provides a greater degree of network control flexibility, with greater levels of accountability and fewer network delays when contrasted alongside the public blockchain [53–64].

Furthermore, when it comes to decentralisation, private blockchains are only partly decentralised, owing to the fact that public access is limited [26, 27]. Business-to-business virtual currency exchange, such as that of Ripple, as an example, is a private blockchain, which may be recognised as an umbrella project of open-source blockchain applications [64, 65]. However, both private and public blockchains are seen to have pros and cons, which has therefore encouraged the introduction of the consortium [27] and hybrid blockchains as a means of overcoming the various disadvantages [65].

2.3. Consortium Blockchains. The consortium blockchain is seen to be partially decentralised and recognised as a middle-ground between private [23] and public blockchain [26], bringing together the advantages of both, although consortium blockchain may be recognised at the consensus level [65–67]. Essentially, this system is not so open that blocks can be published and validated by anyone [25], nor can blockchain procedures only be appointed by one individual [66, 67].

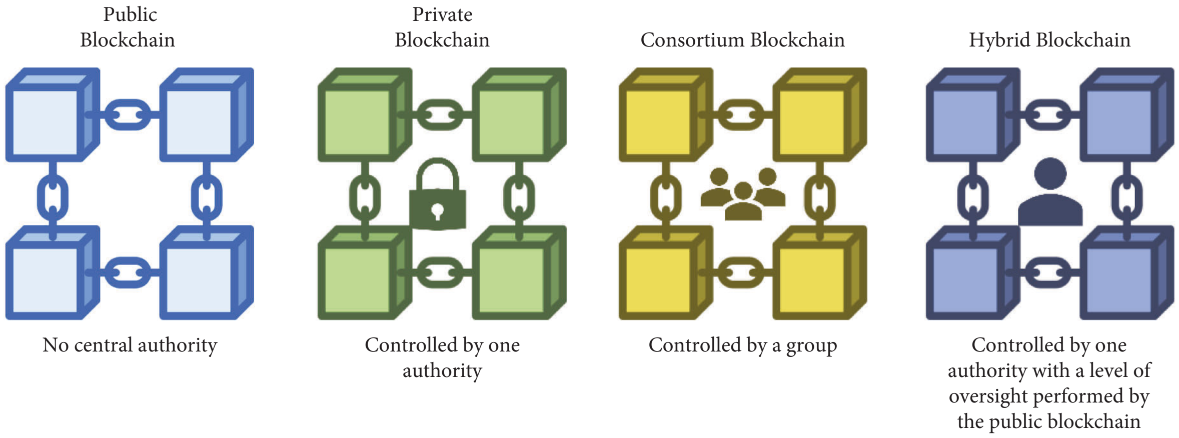
Public Blockchain
Private Blockchain
Consortium Blockchain
Hybrid Blockchain
No central authority
Controlled by one authority
Controlled by a group
Controlled by one authority with a level of oversight performed by the public blockchain

Figure 2: Different types of blockchain structure.

Table 1: Blockchain different elements.

Types	Public	Private	Consortium	Hybrid
Network	Open	Closed	Organization	Organization
Access	Free	DLT authority	Group	Mixed
Permission	No	On	On	Restriction
Ledgers	Shared	Shared	Shared	Mixed
Transparency	Full	Full	Full	Semi

Generally speaking, consortium blockchains are defined as permissioned blockchains that are overseen by a number of different entities, which therefore benefit from a greater degree of decentralisation when compared against private blockchains [67], as well as more security [24–27]. Nonetheless, the process of establishing consortiums can be difficult owing to the need to have cooperation between different entities [27], which therefore means a number of different challenges, in addition to possible risks when it comes to trust and security [26].

2.4. Hybrid Blockchains. This type of blockchain is seen to be controlled by one entity [65], but with the presence of supervision from the public blockchain; this is seen to be necessary when it comes to completing different transaction validations using various new technologies, such as the IoT [23–27]. An example of this type of blockchain would be the model suggested in Section 3.

The IoT is recognised as a modern technology that comprises smart objects, which further encompass physical mechanisms [78], such as actuators and sensors charged with determining the object's internal state, or the external setting [18] and accordingly carrying out various actions in line with the gathered information [67, 68]. The information the sensors generate may undergo subsequent processing [73], with actions then determined after [18, 19]. Such smart objects also comprise software [20], which is embedded into them in the mind of controlling various elements and events [70]. In line with the paper issued by Statista [1], IoT-connected devices are predicted to amount to 75 million by 2025, with the IoT model bringing together the pros of autonomic computing, advances in communication technologies, cloud computing, edge computing, fog computing, wireless body area networks (WBANs) [69], and sensors in such a way so as to create new opportunities in a number of different arenas. Some such arenas that may be affected by IoT developments are, as previously highlighted, training and education [20–28]. Despite being in its infancy, IoT and smart technologies are becoming more and more transactional in such sectors.

Without question, both IoT and blockchain are capable and valuable technologies [20], with both widely utilised and highly appraised in both public and industry sectors [70]. One of the most valuable elements of blockchain is that data are entirely decentralised, which is hugely advantageous when it comes to the ability to eradicate the presence of a strong central authority [21], with control then given back to the individual user [71]. Moreover, when it comes to the sharing of data, blockchain technology provides a number of key advantages, such as in regards to accessibility [74], effectiveness, privacy, and security [20–22]. Moreover, it is used to monitor data quality, quantity [22] and validation, amongst other elements [77]. This provides a greater degree of transparency from which the training sector can benefit, as shown in the following diagram [21]: See Figure 3.

3. The Proposed Blockchain Framework for Data-Sharing between Training Providers Based on the Internet of Things

Although blockchain may be recognised as revolutionary, views may not be consistent [14]. A number of establishment supporters, investors, and developers, for example, could view blockchain as providing the propensity to achieve a

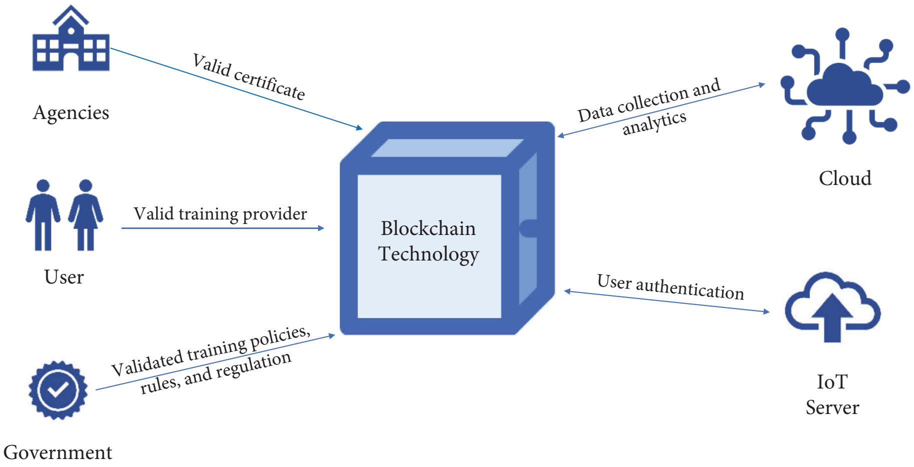

Figure 3: Sharing data using blockchain and IoT in the training sector.

hegemonic shift in economic and societal structures [10], thereby releasing individuals from continuous surveillance and state control [72]. On the other hand, others might adopt a different view [11], considering technology to be more of an innovative driver and high-value approach to attaining a competitive edge [70]. In addition, regulators could potentially perceive a lack of control [9], with criminal activity, therefore, being possible [13], such as in the cases of terrorist financing and money laundering [69]. All viewpoints, however, provide valuable insight and areas for consideration [12, 13], especially when one contemplates the issues surrounding privacy, as presented by blockchain [65–68]. It is important to recognise that blockchain ledgers house a wealth of data that could ultimately increase corporate accountability [8–14]; however, the need for centralised governance and supervision is eradicated, meaning there is a wealth of opportunities when it comes to digital and physical systems and the anonymity of such [73].

As an additional consideration, however, blockchain systems are able to transform a number of different facets of the training and educational arena [15], with progression away from more centrally secured networks and closer to more decentralised structures [22] viewed as being one of the most radical and ground-breaking elements of technology [62–64]. This degree of decentralisation is based on the view that all nodes are provided with equal access to network data; therefore, any additional potential for oversight could have notable consequences, with the propensity to associate an individual with a transaction opening the door to analysis [17–22]. In other words, decentralisation and privacy are therefore closely aligned when it comes to blockchain systems [73].

When it comes to the transference of data and information between devices, in the conventional IoT setting, a cloud-server structure is applied, with data sent to the cloud and accordingly processed back to IoT devices. In order to overcome the potential problems of scalability, a key solution for the scalable environment has been provided by the blockchain. IoT devices are seen to be autonomous and secure, with such information shared in mind of particular needs, which cannot be overridden in mind of making illegal use of confidential data. Such blockchain models can ultimately enhance IoT-based smart objects, autonomy, and security by combining with trust-centred protection devices. The following Figures 4 and 5 highlight the individual stages of the suggested framework for the sharing of data between providers of training, in line with the IoT.

Importantly, all records and data pertaining to trainers, as gathered from separate servers, are connected by the blockchain, as can be seen in Figure 5. As the ultimate considerations, privacy, and security are prioritised in the smart environment, where data are shared through the use of sensors. The IoT is positioned to link a significantly large number of smart devices, including IDs, RFIDs, sensors, and various smart appliances [75]. Moreover, a number of different IT applications have been encouraged to share data, notably through radio frequency and sensor network innovations, with such automation comprising the feature of intelligent devices and appliances that apply both wired and wireless technologies and software to enable the unified incorporation of training and education systems [76].

The suggested model will facilitate training providers in sharing data pertaining to the trainee, providing significant privacy and high security concerning the data of the training, complete with access to the learning, and development platforms delivered by providers. The key vision is concerned with improving the profession and its status overall, such as by providing agencies and those operating within the public domain with the confidence needed to use the suggested framework. Such devices may be able to provide enhancements when it comes to user authentication connections, which ultimately depend on the communication between cyber and physical components in the creation of data and, as a result, information. The data that are gathered may subsequently be transmitted, collected, and accordingly examined to enhance decision-making and ultimately improve upon any inefficiencies, notably through ensuring accuracy, availability, interoperability, security, and trust [1–22]. See Figure 6

The different elements of the suggested model are gathered from previous works, books, papers, conference

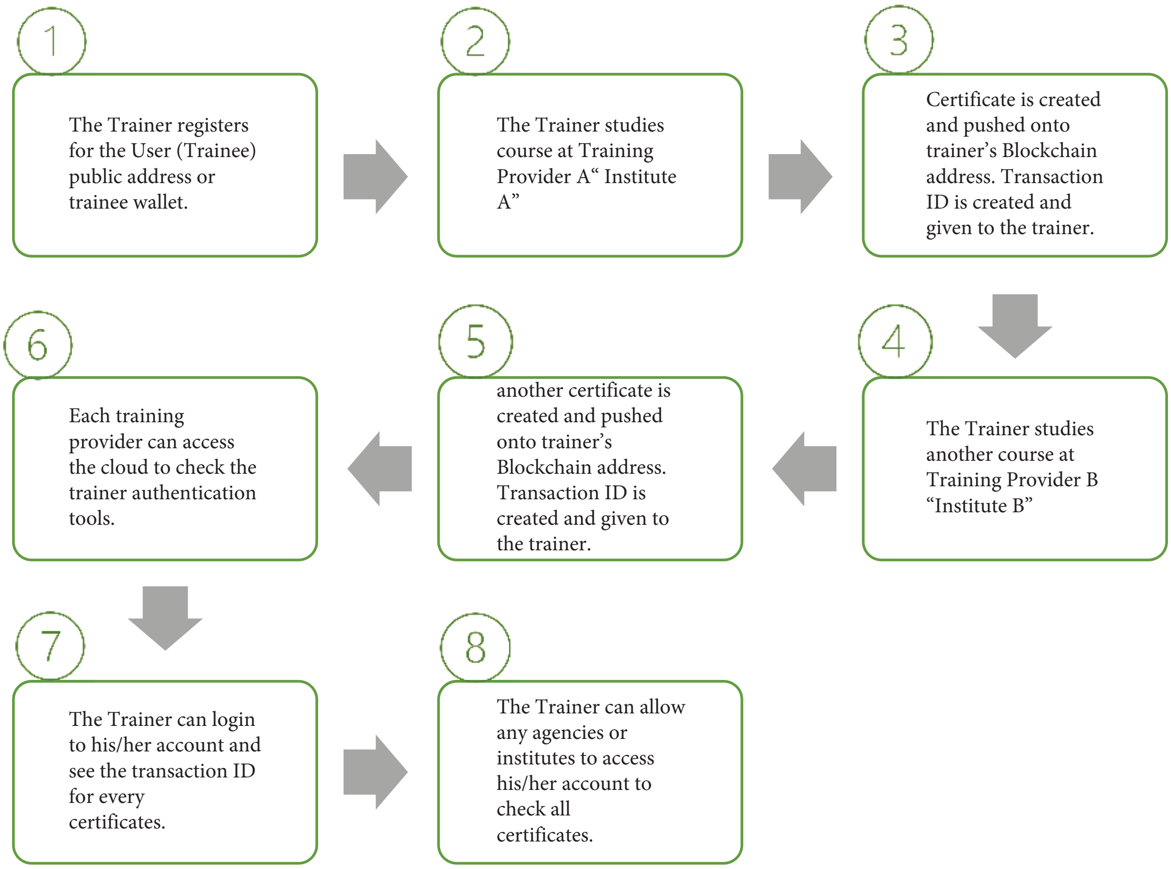
1
The Trainer registers for the User (Trainee) public address or trainee wallet.
2
The Trainer studies course at Training Provider A“ Institute A”
3
Certificate is created and pushed onto trainer’s Blockchain address. Transaction ID is created and given to the trainer.
4
The Trainer studies another course at Training Provider B “Institute B”
5
another certificate is created and pushed onto trainer’s Blockchain address. Transaction ID is created and given to the trainer.
6
Each training provider can access the cloud to check the trainer authentication tools.
7
The Trainer can login to his/her account and see the transaction ID for every certificates.
8
The Trainer can allow any agencies or institutes to access his/her account to check all certificates.

Figure 4: Steps of the proposed framework.

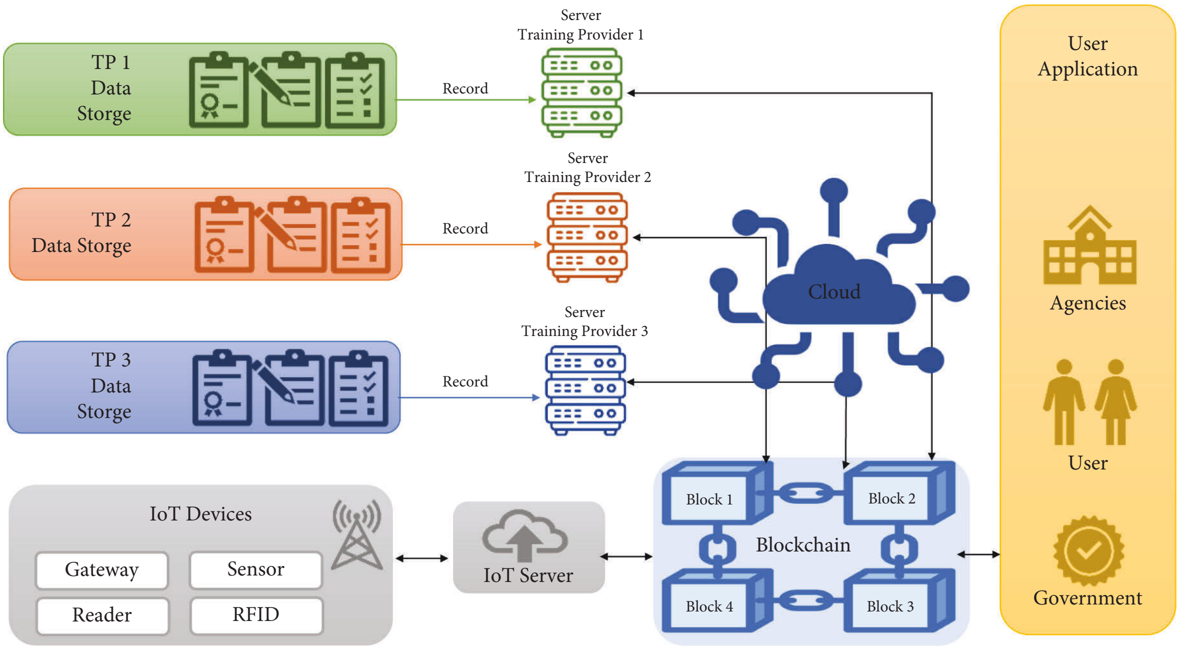

Figure 5: Structure of the suggested framework.

papers, and journals pertaining to the blockchain [52–68]. There are a number of different reports on particular blockchain applications in a number of different areas, all of which offer insight into technical considerations, such as blockchain consensus protocols [22], the educational and training sectors [28], security issues [32], and the Internet of Things [45]. The suggested model is centred on the key characteristics garnered from such perspectives. The model

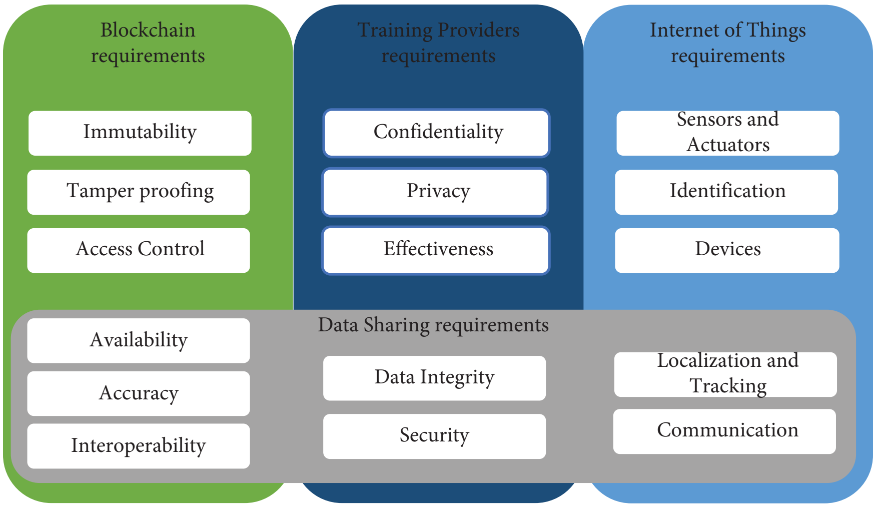

Figure 6: The proposed framework.

enabled the formulation of all elements that are concerned with the researched theories of such perspectives. As a result, professional assessments have been adopted in order to assess the elements of the model.

Such an examination has facilitated the development of the model. Following the finalisation of an extensive examination of the theories available in the relevant arena, the below figures detail a total of 16 characteristics that have been selected in mind for creating a blockchain model for the sharing of data between different providers based on IoT. A greater degree of examination into such elements will be carried out in Section 4 with the objective to determine the most significant of attributes for inclusion in the model.

As is evident from the above figure, the key attribute of the model has been categorized in line with the three perspectives under examination, notably

(i) Blockchain encompasses 6 attributes, namely access control [15–18], accuracy [4–7], availability [17, 18], immutability [45, 46], interoperability [70–72], and tamper proofing [11–14].

(ii) Training provider encompasses 5 attributes, namely confidentiality [5–8], data integrity [33, 34], effectiveness [47, 48], privacy, and security [5–7].

(iii) IoT encompasses 5 attributes, namely communication [8–10], devices, identification [43–45], localization and tracking [9–12], and sensors and actuators [19–22].

4. Validating End Assessment of the Suggested Model

Validity is focused on the degree of alignment between an instrument and a concept, with validating recognised as a critical stage, particularly upon the creation or introduction of a new measure, where no existing measure exists that operationalises the concept [12]. The model assessment is carried out with the application of a realistic assessment method, which depends on professional groups progressing through various stages, as detailed in Figure 7. Realistic assessment is valuable when it comes to validating a model with consideration directed toward the sources and verifiers of the data, not only for issues of recognised importance but also in regard to more debatable concerns.

The model assessment seeks to analyse the patterns of inter-rater alignment between content experts pertaining to the various elements of the suggested model. A number of professionals were asked to provide their insights concerning the value of each of the elements, with consideration directed toward varying standpoints. When it comes to analysing the viewpoints of the professionals, it is considered critical that software be used, which facilitates the performance of data manipulations, in addition to the identification of various elements viewed as critical to establishing the value of various elements present in the proposed model. It is important to emphasise that, throughout this particulate step, SPSS was applied.

Subsequent to the introduction of the list of items pertaining to all aspects of the suggested model, which notably details 6 items from blockchain, 5 training provider elements, and 5 from IoT, all items were given a short explanation concerned with establishing scope and meaning. As a result, each of the items can then be properly appreciated and understood in regard to all dimensions. The questionnaire was created with the goal of measuring the degree of agreement between the professionals, with various questions posed involving items and their respective items. The questionnaire was published online, with the analysis carried out in line with a measurement centred on achieving a score on a 4-point scale. Importantly, on the scale, 1 was seen to represent ‘Not Important’, whereas 4 was ‘Very Important’. Through the application of the SPSS software, the average opinion was identified, with the overall average for all aspects then reviewed and examined. See Figure 8

The questionnaire was made available online in March 2022. A total of 60 experts were given access to the questionnaire, with an explanation pertaining to why the questionnaire was being carried out, as well as why the

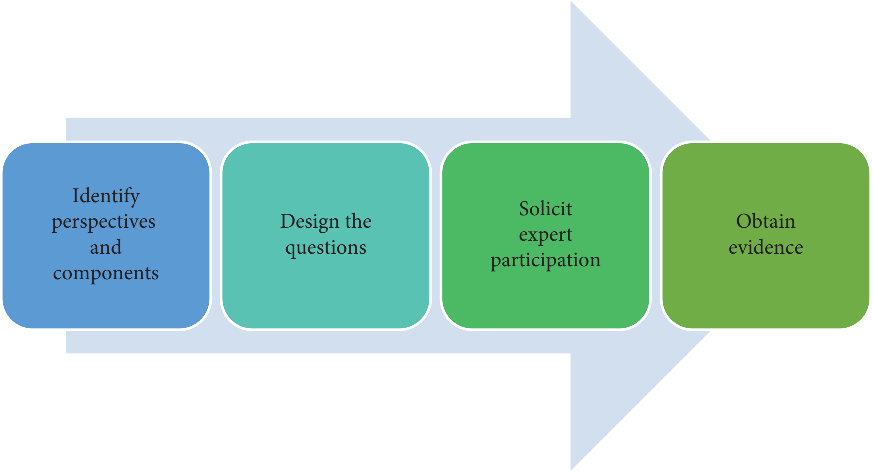
Identify perspectives and components
Design the questions
Solicit expert participation
Obtain evidence

Figure 7: Four steps for validating end assessments of the suggested model.

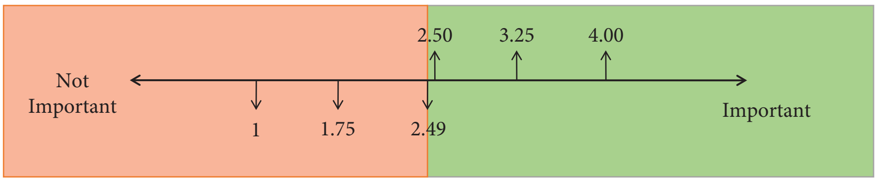

Figure 8: Measured in line with a 4-point scale.

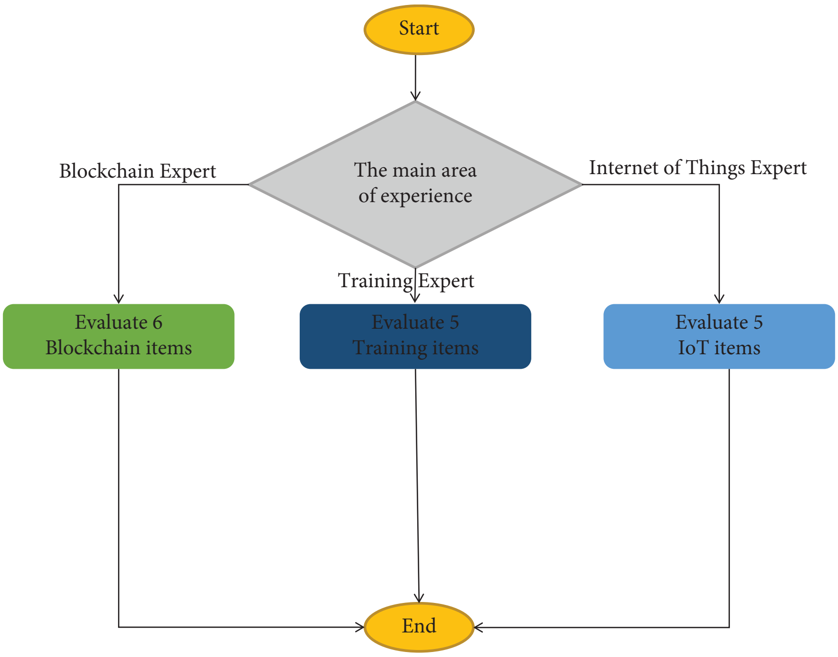
Start
The main area of experience
Blockchain Expert
Internet of Things Expert
Training Expert
Evaluate 6 Blockchain items
Evaluate 5 Training items
Evaluate 5 IoT items
End

Figure 9: Evaluation attributes using professionals' assessment.

experts in question had been invited to participate. Furthermore, the questionnaire's objective and purpose were also detailed, in addition to an assurance of data confidentiality.

A total of 33 of the 60 experts invited completed the questionnaire. A total of 10 of the 33 participants were blockchain experts, who were asked to rate the importance of 6 items. A total of 12 of the 33 participants were training providers, who were asked to rank the importance of 5 items. Finally, 11 of the 33 participants were IoT experts, who were asked to rank the importance of 5 items. This can be seen displayed in Figure 9.

With the application of the SPSS software, there was the completion of data screening with the goal of ensuring any

Table 2: The evaluation results.

Areas	Items	Sig (2-tailed)	Mean	Attitude	Accepted Hypothesis
Blockchain	Item 1:Immutability	0.046	3.25	Very important	Alternative
	Item 2:Tamper proofing	0.012	3.38	Very important	Alternative
	Item 3:Access control	0.002	3.50	Very important	Alternative
	Item 4:Availability	0.002	3.25	Very important	Alternative
	Item 5:Accuracy	0.000	3.63	Very important	Alternative
	Item 6:Interoperability	0.000	3.75	Very important	Alternative
Training Provider	Item 7:Confidentiality	0.000	3.63	Very important	Alternative
	Item 8:Privacy	0.012	3.38	Very important	Alternative
	Item 9:Effectiveness	0.000	3.63	Very important	Alternative
	Item 10:Data integrity	0.000	3.63	Very important	Alternative
	Item 11:Security	0.001	3.50	Very important	Alternative
Internet of things	Item 12:Sensors	0.002	3.25	Very important	Alternative
	Item 13:Identification	0.000	3.75	Very important	Alternative
	Item 14:Devices	0.002	3.38	Very important	Alternative
	Item 15:Localization and tracking	0.000	3.75	Very important	Alternative
	Item 16:Communication	0.000	3.63	Very important	Alternative

missing data were identified and reverse coding was checked. No items were found to be missing and/or reverse-coded.

Table 2 below provides a summarized overview of the results of the descriptive statistics, in addition to the findings of one of the sample t-tests, which are concerned with establishing whether or not the population mean (μ) may be seen to be equal to a hypothesized value (μ 0). In order to draw a conclusion, the significance level, α (alpha), with a typical value of 0.05, is selected. Accordingly:

(i) if Sig. (for each item) is less than or equal to α, H0 is rejected; or

(ii) if Sig. (for each item) is greater than α, H1 is rejected.

Table 1 provides the evaluation results. It is apparent that the significance value (Sig.) for all items is recognised as being below 0.05 $p < 0.05$; this means the null hypothesis (H0) is rejected, with the alternative hypothesis (H1) accepted for all items. Moreover, when it comes to the mean of all times, this is seen to be significantly greater than 2.49; therefore, in the suggested model, all items are seen to be important.

5. Conclusion

The fourth wave of evolution is being witnessed across blockchain and IoT technologies, both of which are viewed as being critical when it comes to enhancing the sharing of data in real time and with end-to-end traceability mechanisms [30]. The apparent variety when it comes to the way in which blockchains are implemented may be seen to be owing to its ability to create decentralised [8–13] and trustless transaction environments [63, 64]. In this regard, blockchains are able to manage critical problems, including data-sharing and automated claim authentication, with the training and education sector seen to be the perfect domain for the adoption of blockchain technology. Importantly, such technology facilities students and trainers in maintaining personal data and accordingly establishing parties for sharing and receiving data, thereby determining data ownership and sharing issues. Moreover, recorded data may also be combined, changed, shared safely, and gathered by the relevant entities with the application of consensus protocols or IoT. This is a key advantage when it comes to this technology and its use within the education and training arena, with current processes and strategies requiring third-party involvement for data storage.

This particular research has been carried out with the mind of gaining insight into the blockchain model for the sharing of data across the training arena. In order to satisfy this goal, this study has created a theoretical blockchain model for the sharing of data between training providers, in line with the IoT, which is authenticated and recognised as able to establish the success of this model. Furthermore, it presents the approaches, strategies, and analyses of professionals' assessments when it comes to the individual elements of the suggested model.

The findings suggest much significance to the professionals' conformity pertaining to the elements of the suggested model. Accordingly, such results provide evidence that the suggested model is centred on sound theoretical underpinnings from studies in regard to all three research perspectives. [29, 77, 78].

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] IoT, "number of connected devices worldwide 2012–2025 Statista," 2016, http://www.statista.com/statistics/976313/global-iot-market-size.

[2] A. Tharatipyakul and S. Pongnumkul, "User Interface of Blockchain-Based Agri-Food Traceability Applications: A Review," *IEEE Access*, vol. 9, pp. 82909–82929, 2021.

[3] A. Vangala, A. K. Sutrala, A. K. Das, and M. Jo, "Smart contract-based blockchain-envisioned authentication scheme for smart farming," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10792–10806, 2021.

[4] A. Welligton dos Santos Abreu, E. F. Coutinho, and C. Ilane Moreira Bezerra, "Performance evaluation of data transactions in blockchain," *IEEE Latin America Transactions*, vol. 20, no. 3, pp. 409–416, 2022.

[5] A. I. Sanka, M. Irfan, I. Huang, and R. C. Cheung, "A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research," *Computer Communications*, vol. 169, pp. 179–201, 2021.

[6] A. N. M. Saif and M. A. Islam, "Blockchain in Human Resource Management: A Systematic Review and Bibliometric Analysis," *Technology Analysis & Strategic Management*, pp. 1–16, 2022.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[8] C. K. Da Silva Rodrigues and V. Rocha, "Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions," *IEEE Latin America Transactions*, vol. 19, no. 7, pp. 1199–1206, 2021.

[9] D. Effah, B. Chunguang, F. Appiah, B. L. Y. Agbley, and M. Quayson, "Carbon emission monitoring and credit trading: the blockchain and IOT approach," in *Proceedings of the 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 106–109, IEEE, Chengdu, China, December 2021.

[10] D. Fakhri and K. Mutijarsa, "Secure IoT communication using blockchain technology," in *Proceedings of the 2018 International Symposium on Electronics and Smart Devices (ISESD)*, pp. 1–6, IEEE, Bandung, Indonesia, October 2018.

[11] D. Folkinshteyn and M. Lennon, "Braving Bitcoin: a technology acceptance model (tam) analysis," *Journal of Information Technology Case and Application Research*, vol. 18, no. 4, pp. 220–249, 2017.

[12] D. M. Rubio, M. Berg-Weger, S. S. Tebb, E. S. Lee, and S. Rauch, "Objectifying content validity: conducting a content validity study in social work research," *Social Work Research*, vol. 27, no. 2, pp. 94–104, 2003.

[13] E. Toufaily, T. Zalan, and S. B. Dhaou, "A Framework of Blockchain Technology Adoption: an investigation of challenges and expected value," *Information & Management*, vol. 58, no. 3, Article ID 103444, 2021.

[14] F. Chen, "Blockchain-based optical network slice rental approach for IoT," in *Proceedings of the 2020 IEEE Computing, Communications and IoT Applications (ComComAp)*, pp. 1–4, IEEE, Beijing, China, December 2020.

[15] G. Dittmann and J. Jelitto, "A blockchain proxy for lightweight IoT devices," in *Proceedings of the 2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 82–85, IEEE, Rotkreuz, Switzerland, June 2019.

[16] G. Liu, J. Wu, and T. Wang, "Blockchain-enabled fog resource access and granting," *Intelligent and Converged Networks*, vol. 2, no. 2, pp. 108–114, 2021.

[17] G. S. Gunanidhi and R. Krishnaveni, "Improved security blockchain for IoT based healthcare monitoring system," in *Proceedings of the 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, pp. 1244–1247, IEEE, Coimbatore, India, February 2022.

[18] G. Wang, Z. Shi, M. Nixon, and S. Han, "ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 166–175, IEEE, Atlanta, GA, USA, July 2019.

[19] G. Wolfond, "A blockchain ecosystem for digital identity: improving service delivery in Canada's public and private sectors," *Technology Innovation Management Review*, vol. 7, no. 10, pp. 35–40, 2017.

[20] H. R. Bokkisam, S. Singh, R. M. Acharya, and M. P. Selvan, "Blockchain-based peer-to-peer transactive energy system for community microgrid with demand response management," *CSEE Journal of Power and Energy Systems*, vol. 8, no. 1, pp. 198–211, 2022.

[21] H. Xiong, C. Jin, M. Alazab et al., "On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1977–1986, May 2022.

[22] I. M. M. A. Sadek and M. Ilyas, "Securing IoT devices using blockchain concept," in *Proceedings of the 2021 International Conference on Engineering and Emerging Technologies (ICEET)*, pp. 1–6, IEEE, Istanbul, Turkey, October 2021.

[23] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's Adoption in IoT: the challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, pp. 251–279, 2019.

[24] J. K. Solomon Doss and S. Kamalakkannan, "IoT system Accomplishment using BlockChain in validating and data security with cloud," in *Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 60–64, IEEE, Palladam, India, October 2020.

[25] J. Ren, J. Li, H. Liu, and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," *Tsinghua Science and Technology*, vol. 27, no. 4, pp. 760–776, 2022.

[26] J. Song, J. Nang, and J. Jang, "Design of anomaly detection and visualization tool for IoT blockchain," in *Proceedings of the 2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 1464-1465, IEEE, Vegas, NV, USA, December 2018.

[27] J. Zhou, G. Feng, and Y. Wang, "Optimal deployment mechanism of blockchain in resource-constrained IoT systems," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8168–8177, 2022.

[28] J. Frizzo-Barker, P. A. Chow-White, P. R. Adams, J. Mentanko, D. Ha, and S. Green, "Blockchain as a disruptive technology for business: a systematic review," *International Journal of Information Management*, vol. 51, Article ID 102029, 2020.

[29] J. Holbrook, "Introduction to blockchain technologies," in *Architecting Enterprise Blockchain Solutions*, pp. 1–28, Wiley, Hoboken, NJ, USA, 2020.

[30] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri, and S. Gupta, "A comparitive analysis on E-voting system using blockchain," in *Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1–4, IEEE, Ghaziabad, India, April 2019.

[31] K. Tulkinbekov and D.-H. Kim, "Storing blockchain data in public storage," in *Proceedings of the 2021 Twelfth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 299–301, IEEE, Jeju Island, Korea, August 2021.

[32] L. An, J. Yue, G. Zhang, and Q. Wang, "BITS: a blockchain-based intelligent teaching system for smart education," in *Proceedings of the 2021 International Conference on Education, Information Management and Service Science (EIMSS)*, pp. 159–162, IEEE, Xi'an, China, July 2021.

[33] L. Kleinknecht, "Can blockchain capabilities contribute to sustainable supply-chain governance?" *IEEE Engineering Management Review*, vol. 49, no. 4, pp. 150–154, 2021.

[34] M. Attaran, "Blockchain technology in healthcare: challenges and opportunities," *International Journal of Healthcare Management*, pp. 1–14, 2020.

[35] M. A. Islam and S. Madria, "A Permissioned Blockchain Based Access Control System for IOT," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 469–476, IEEE, Atlanta, GA, USA, July 2019.

[36] M. A. López Peña and I. Muñoz Fernández, "SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform," in *Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 633–638, IEEE, Limerick, Ireland, April 2019.

[37] M. H. Salih Mohammed, "A Hybrid Framework for Securing Data Transmission in Internet of Things (IoTs) Environment Using Blockchain Approach," in *Proceedings of the 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, pp. 1–10, IEEE, Toronto, Canada, April 2021.

[38] M. Iqbal and R. Matulevičius, "Exploring sybil and double-spending risks in blockchain systems," *IEEE Access*, vol. 9, pp. 76153–76177, 2021.

[39] M. J. A. Baig, M. T. Iqbal, M. Jamil, and J. Khan, "IoT and Blockchain Based Peer to Peer Energy Trading Pilot Platform," in *Proceedings of the 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 0402–0406, IEEE, Vancouver, Canada, November 2020.

[40] M. Janssen, V. Weerakkody, E. Ismagilova, U. Sivarajah, and Z. Irani, "A framework for analysing blockchain technology adoption: integrating institutional, market and technical factors," *International Journal of Information Management*, vol. 50, pp. 302–309, 2020.

[41] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem et al., "A survey on blockchain technology: evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.

[42] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[43] M. Torky and A. E. Hassanein, "Integrating blockchain and the internet of things in precision agriculture: analysis, opportunities, and challenges," *Computers and Electronics in Agriculture*, Article ID 105476, 2020.

[44] N. Furneaux, "Understanding the blockchain," in *Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence*, pp. 39–65, Wiley, Hoboken, NJ, USA, 2018.

[45] N. Bore, S. Karumba, J. Mutahi, S. Darnell, C. Wayua, and K. Weldemariam, "Towards blockchain-enabled school information hub," in *Proceedings of the 9th International Conference on Information and Communication Technologies and Development*, pp. 1–4, Lahore, India, November 2017.

[46] N. Kshetri and J. Voas, "Blockchain in developing countries," *IT Professional*, vol. 20, no. 2, pp. 11–14, 2018.

[47] S. Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, White Paper, 2008.

[48] P. Alemany, R. Vilalta, R. Munoz, R. Casellas, and R. Martinez, "Evaluation of the abstraction of optical topology models in blockchain-based data center interconnection," *Journal of Optical Communications and Networking*, vol. 14, no. 4, pp. 211–221, April 2022.

[49] P. Gupta, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Towards a blockchain powered IoT data marketplace," in *Proceedings of the 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 366–368, IEEE, Bangalore, India, January 2021.

[50] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, no. 1, pp. 85–94, 2021.

[51] P. Urien, "A new IoT trust model based on TLS-SE and TLS-IM secure elements: a blockchain use case," in *Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-2, IEEE, Las Vegas, NV, USA, January 2021.

[52] P. Bhaskar, C. K. Tiwari, and A. Joshi, "Blockchain in Education Management: Present and Future Applications," *Interactive Technology and Smart Education*, 2020.

[53] P. Dutta, T. M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: applications, challenges and research opportunities," *Transportation research part e: Logistics and transportation review*, vol. 142, Article ID 102067, 2020.

[54] R. Chen, F. Shu, S. Huang, L. Huang, H. Liu, and J. Liu, "BIdM: a blockchain-enabled cross-domain identity management system," *Journal of Communications and Information Networks*, vol. 6, no. 1, pp. 44–58, March 2021.

[55] S. Bajoudah, C. Dong, and P. Missier, "Toward a Decentralized, Trust-Less Marketplace for Brokered IoT Data Trading Using Blockchain," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 339–346, Atlanta, GA, USA, July 2019.

[56] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 184–193, IEEE, Atlanta, GA, USA, July 2019.

[57] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Evaluation and demonstration of blockchain applicability framework," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1142–1156, Nov, 2020.

[58] S. R. Niya, "Adaptation of Proof-Of-Stake-Based Blockchains for IoT Data Streams," in *Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 15-16, IEEE, Seoul, Korea (South), May 2019.

[59] S. E. Chang, Y. C. Chen, and M. F. Lu, "Supply Chain Re-engineering Using Blockchain Technology: a case of smart contract-based tracking process," *Technological Forecasting and Social Change*, vol. 144, pp. 1–11, 2019.

[60] S. Fosso Wamba, J. R. Kala Kamdjoug, R. Epie Bawack, and J. G. Keogh, "Bitcoin, Blockchain and Fintech: a systematic review and case studies in the supply chain," *Production Planning & Control*, vol. 31, no. 2-3, pp. 115–142, 2019.

[61] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.

[62] T. Meng, Y. Zhao, K. Wolter, and C.-Z. Xu, "On consortium blockchain consistency: a queueing network model

approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 6, pp. 1369–1382, 2021.

[63] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: applications, opportunities and challenges," *Journal of Network and Computer Applications*, Article ID 102857, 2020.

[64] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019.

[65] V. A. Gasimov and S. K. Aliyeva, "Using blockchain technology to ensure security in the cloud and IoT environment," in *Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, pp. 1–5, IEEE, Ankara, Turkey, June 2021.

[66] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How Blockchain can Impact Financial Services -The overview, challenges and recommendations from expert interviewees," *Technological forecasting and social change*, vol. 158, Article ID 120166, 2020.

[67] W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, "Circuit copyright blockchain: blockchain-based homomorphic encryption for IP circuit protection," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1410–1420, 2021.

[68] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "NutBaaS: a blockchain-as-a-service platform," vol. 7, pp. 134422–134433, IEEE Access, 2019.

[69] X. Guo, Q. Guo, M. Liu, Y. Wang, Y. Ma, and B. Yang, "A certificateless consortium blockchain for IoTs," in *Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, pp. 496–506, IEEE, Singapore, November 2020.

[70] X. Hao, P. L. Yeoh, T. Wu, Y. Yu, Y. Li, and B. Vucetic, "Scalable Double Blockchain Architecture for IoT Information and Reputation Management," in *Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, pp. 171–176, IEEE, New Orleans, LA, USA, June 2021.

[71] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2964–2973, 2021.

[72] Y. Sun, L. Zhang, P. Klaine, B. Cao, and M. A. Imran, "Performance analysis on wireless blockchain IoT system," in *Wireless Blockchain: Principles Technologies and Applications*, pp. 179–199, IEEE, 2022.

[73] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei, and B. Chen, "When blockchain meets SGX: an overview, challenges, and open issues," vol. 8, pp. 170404–170420, IEEE Access, 2020.

[74] Z. Gong-Guo and Z. Wan, "Blockchain-based IoT security authentication system," in *Proceedings of the 2021 International Conference on Computer, Blockchain and Financial Development (CBFD)*, pp. 415–418, IEEE, Nanjing, China, April 2021.

[75] Z. Fang, J. Wang, Y. Ren, Z. Han, H. V. Poor, and L. Hanzo, "Age of information in energy harvesting aided massive multiple access networks," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 5, pp. 1441–1456, 2022.

[76] M. Kim, S. Lee, C. Park, J. Lee, and W. Saad, "Ensuring data freshness for blockchain-enabled monitoring networks," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9775–9788, 2022.

[77] G. Srivastava, J. Crichigno, and S. Dhar, "A Light and Secure Healthcare Blockchain for IoT Medical Devices," in *Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, pp. 1–5, IEEE, Edmonton, Canada, May 2019.

[78] S. Dhar, A. Khare, and R. Singh, *Advanced Security Model for Multimedia Data Sharing inInternet of Things*, wiley, Hoboken, NJ, USA, 2022.