future internet

MDPI

Article

Validating the Adoption of Heterogeneous Internet of Things with Blockchain

Lulwah AlSuwaidan * and Nuha Almegren

College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Riyadh 11432, Saudi Arabia; namoqren@imamu.edu.sa

* Correspondence: lnsuwaidan@imamu.edu.sa

Received: 9 May 2020; Accepted: 9 June 2020; Published: 21 June 2020

Abstract: Emerging technologies such as Internet of Things (IoT) and blockchain have affected the digital transformation. Blockchain, on the one hand, was initially developed for the purpose of financial trading due to its robustness especially for fault tolerance and cryptographic security in addition to its decentralized architecture. IoT, on the other hand, is an open interconnected network of smart devices able to communicate simultaneously. This arises a challenge in privacy and security, specifically for the data being exchanged. To overcome this, studies have focused on the blockchain to resolve the security and privacy issues of IoT. Indeed, limited studies have proposed to assess blockchain's viability for IoT and the associated challenges. In this paper, a conceptual model has proposed to identify the crucial factors affecting the adoption of blockchain in IoT. The model consists of four dimensions of factors that we assume will affect the adoption of the two technologies. The dimensions are: attitude-related factors, social influence related factors, data-related factors, and security-related factors. This model is validated through a survey that was distributed between professionals in blockchain and IoT. The findings show a significant impact of data-related factors on the adoption of blockchain in IoT and the intention to use them. The model can play an important role in the development of strategies, standards, and performance assessment.

Keywords: conceptual model; blockchain; internet of things; IoT

1. Introduction

The importance of Internet of Things (IoT) has been demonstrated by the innovative and intelligent technologies and services that it can provide. It is composed of numerous physical objects that are linked to the Internet and are able to communicate with each other. These objects eventually generate a massive amount of data and thereby gather and broadcast them into information systems and technologies such as the cloud, Service-oriented Architecture (SoA), and workflow management system. The integrated technologies have proven their effectiveness in enhancing IoT systems' availability as services worldwide.

An IoT system can be described as a network of interconnected smart devices and objects that are able to communicate and transfer data using unique identifiers. Communications are processed without the intervention of humans or other computers. IoT has been a platform for different domains, including business, health, and education, which have generated considerable recent research interest. Furthermore, a distributed trust technology, scalability, security, and privacy, is fundamental to the growth of IoT applications [1]. Therefore, blockchain technology requires these underlying features in order to build a solid transaction process. Blockchain first appeared as a solution for the crypto-currency Bitcoin founded by Satoshi Nakamoto in 2008 [2] which relies on security features such as digital signatures and distributed consensus mechanisms [3,4]. Its transaction flows in a peer-to-peer network of nodes by generating a chain of data structure that contains blocks of encrypted data and information in a chronological order. Blockchains basically form a distributed ledger that provides a data storage service and records secure transactions or transactional events using cryptography.

Integrating blockchain with the IoT environment will inherit some of IoT's challenges which prevent the direct deployment of blockchain for IoT. In the following, we will discuss critical issues and challenges behind the integration.

The crucial challenge has centered around the use of consensus protocol. Makhdoom et al. [5] have shown the lack of IoT centric consensus protocol through testing a case scenario of an IoT-based supply chain monitoring system. In addition, Viriyasitavat et al. [6] have analyzed some challenges related to the use of consensus protocol specifically in the time required to reach a finality settlement. They claimed that most IoT applications require a time-critical operations which indeed affect the finality settlement. The delay is also influenced by the number of nodes which is a primary step in the selection of consensus protocol either public, private, and permissioned blockchain systems. Additionally, storage and trust are critical issues in IoT devices, and blockchains usually generate massive data as composing transaction blocks. The challenge is that IoT devices are unable to verify the transactions generated by others while sender needs historical data. Wang et al. [7] have stated that the IoT devices should either trust itself by taking the storage load, or trust remote servers, which impose extra communication overhead and secured communication between the IoT devices and the trusted servers. They also claimed that reducing the storage load is done by dealing with IoT devices as a light node in the blockchain system which only save the block headers. Security and privacy have received significant attention in the studies. Wang et al. [7] have raised an important concern in ensuring the secure input of sensor data to the blockchain. Security should also be confirmed in communication between the IoT devices and the trusted servers. A survey on privacy protection has been presented by Feng et al. [8]. They classified the privacy attacks into de-anonymization and transaction pattern exposure. These threads could be reduced by considering two privacy requirements: identity and transaction. Wang et al. [7] have discovered other challenges such as computation, energy, storage, communication, mobility, latency, and capacity.

The rest of the paper is organized as follows: related works are discussed in Section 2 to study the prior researches in adopting blockchain and IoT, it also emphasizes the significance of the topic. In Section 3, the conceptual model and research hypotheses are presented. The methodology and data analysis are illustrated in Section 4 to validate the proposed model. Discussion is presented in Section 5. Finally, Section 6 concludes the paper.

2. Related Works

The concept of a connected world was started in the early 1960s and followed by a series of developments up until modern day technology. IoT holds the same concept of connected machines, and was first introduced in 2006 by Adelmann et al. [9] in a conference paper entitled "Toolkit for bar code recognition and resolving on camera phones-jump starting the internet of things". In recent years, IoT research has experienced growth and development in an interdisciplinary manner. Different fields of knowledge including technology, applied engineering, economics, business, industry, management, etc., have been discussed as underlying issues for IoT. This can lead to confusion in understanding the direction that IoT development is progressing in [10]. Most businesses or industrial sectors look to adopt IoT functions and features in an attempt to find novel solutions to their problems [11]. Dachya et al. [10] mentioned the top industries that have adopted IoT, which include manufacturing, agriculture, public service, health, electronics, and energy [11]. In fact, adopting IoT in any industry requires understanding its underlying architecture which consists of four levels. The first is a perception layer composed of different sensors and data collectors, followed by a network layer that controls the transmission of the data; the next layer is the middleware layer, which involves the information processing systems; finally, the fourth level is the application and services level [12].

Recently, interest has been generated regarding integrating blockchain into IoT process. Negka et al. [13] examined the effect of employing blockchain technology to overcome the problems in IoT ecosystems when handling counterfeit copycat devices. They proposed an approach that depends on identifying each one of the used components through the use of Physical Unclonable Functions (PUF) responses, and employs blockchain technology in order to set-up a platform for tracking the supply chain of both component and IoT devices, without requiring the existence of any central authority. In the same context, Rejeb et al. [14] presented a methodology of deploying blockchain technology with IoT infrastructure to facilitate and flatten the process of modern supply chains and enhance value chain networks. Moreover, Mendki [15], in his study of edge and fog computing, discovered the use of blockchain based decentralized application to enable IoT edge processing and scaling via enabling resource owner to join the ecosystem and lend the compute resources as needed. As regards leveraging the IoT and blockchain technology to detect distributed denial of service (DDoS) attacks, Spathoulas et al. [16] installed lightweight agents in multiple IoT installations to detect DDoS attacks conducted through the use of IoT-device botnets. Blockchain ledgers govern information exchanged between IoT smart devices and control the integrity of both the procedure and the information. Finally, Tseng et al. [17] proposed an architecture that implements blockchain in managing heterogeneous IoT systems, as well as presenting the related challenges in terms of integration and development.

The benefit of using blockchain is to provide a decentralized digital database of transactions, called the distributed ledger, which is maintained and updated by a network of computers that verify a transaction before it is approved and added to the ledger. This allows transaction parties to exchange ownership of digitally represented assets in a real-time and immutable peer-to-peer system without the use of intermediaries. Aloqaily et al. [18] highlighted the impact of blockchain in P2P energy trading. They proposed a distributed trading framework and smart contracts to recognize the benefits of blockchain with energy. Morkunas et al. illustrated the six steps of asset exchange between two economic actors using blockchain technology [19]. The transaction process has to be maintained and controlled via blockchain consensus protocols, therefore, Zhang and Lee [20] compared and analyzed different types of protocols in terms of their strengths, weaknesses, and application scenarios. They reached the conclusion that a good consensus protocol should consider fault tolerance and make the best use of it in the appropriate application scenario.

Any newly introduced technology faces resistance in terms of its adoption in other platforms or environments. Therefore, the Technology Acceptance Model (TAM) is a powerful model developed to measure and analyze the factors involved in the resistance to the adoption of the new technology [21]. This model was derived from the Theory of Reasoned Action (TRA) [22], in which the reasoned action is explicitly concerned with behavior; thereby, this theory demonstrates the influence of situations or factors on the attitude and behavior. However, the TAM model concentrates on explaining user acceptance of information technologies through predetermined factors that measure the success of integrating new technologies into a current platform. Boer et al. [23] presented a description of the TAM in which the user perception on perceived usefulness (PU) and perceived ease of use (PEoU) influence one's attitude towards a technology, which, in turn, influences the actual technology use or intention to use it. Moreover, the model factors are associated with and influenced by each other, therefore, PEoU influences PU, and PU can be directly associated with the use of technology or the intention to do so. In this model, PU refers to the extent to which someone trusts that the technology will improve their performance. PEoU can be described as the extent to which someone trusts that using the technology is effortless [23,24]. Mital et al. [24] described the studies that have extended the TAM model in different contexts by introducing new factors into the TAM framework, such as underlying belief factors, and antecedent, moderator, and mediator variables. Such extensions consider usage adoption in different contexts: the office context, in mobile marketing, Internet banking, computer center resources, e-shopping, social networks, and smartphones. The challenges involved in theory improvement and adding more factors for each specific context are complicated, therefore, Mital et al. [24] cited various studies that proposed general factors that can be associated with the original TAM, such as trust, cognitive and social factors, demographic variables, perceived enjoyment, and trust.

3. Conceptual Model and Research Hypotheses

In this section, we discuss the proposed conceptual model, which consists of the most influential factors that affect the adoption of blockchain in the IoT. The model is shown in Figure 1 and is demonstrated in detail in the following subsections.

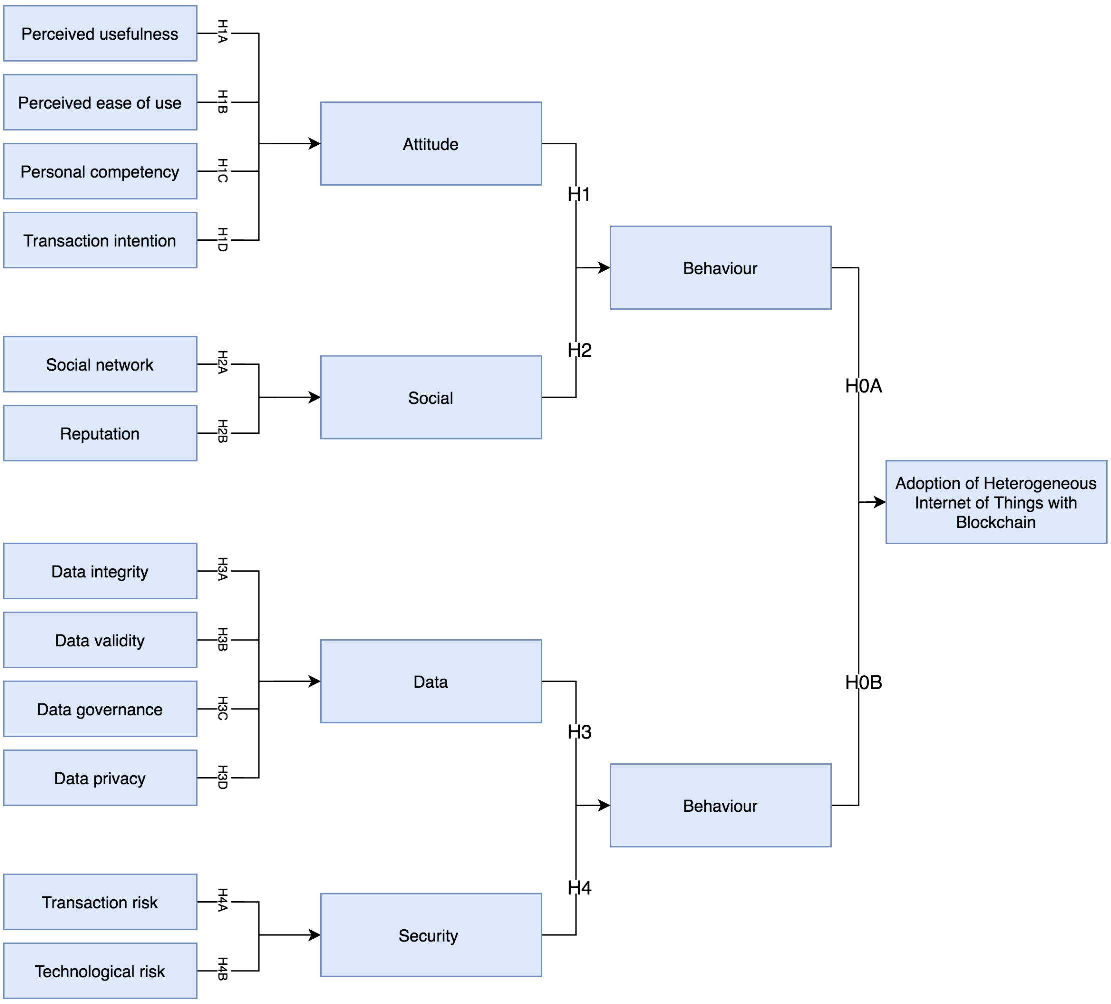

Figure 1. Technology Acceptance Model (TAM) model for adopting blockchain technology in Internet of Things (IoT) environment.

3.1. Behaviour Factors

3.1.1. Attitude Related Factors

Attitude influences all aspects of user decisions and actions. Attitudes involve responses to opportunities and challenges associated with the emergence of modern technologies. Acceptance of IoT and blockchain technology could be influenced by attitude. Previous studies have shown that the key factors in the study of attitudes assume a positive correlation between IoT systems and blockchain to include perceived usefulness, perceived ease of use, personal competency, and transaction intention, which are described below in detail [25–27]:

Perceived usefulness. Defined as the degree that a user believes that a technology would enhance system performance within an organizational context [21]. There are many benefits and advantages gained from technology which increase the perceived benefit [28]. They can affect the quality of work done by improving performance, increasing productivity, and enhancing effectiveness [25]. The TAM specifies that perceived usefulness is one of the most important factors since it focuses on the user's behavioral intention for the adoption of new technology. In the context of IoT and blockchain systems, perceived usefulness was found to be an important influencer of the intention to adopt these technologies in different studies [25,26,29,30]. Perceived usefulness is a significant predictor of the intention to use IoT services with blockchain. Therefore, the following is hypothesized:

Hypothesis 1A (H1A). *Perceived usefulness positively influences the intention to use blockchain technology in an area of IoT.*

Perceived ease of use. Referred to by Davis as the "degree to which a person believes that using a particular system would be free of effort" [21]. According to Alanazi and Soh [25], perceived ease of use can be measured in several dimensions regarding the adoption of new technology: easy to learn, control and use, clear and understandable, easy to become skillful, and flexible to interact with. A number of studies have indicated that a perceived ease of use has a significant effect on the intention and behavior of IoT systems [12,25,31,32]. According to Knauer and Munn [30], they recommend focusing on ease of use to increase the perceived ease of use when applying blockchain technology to improve operations and enhance the user experience. Therefore, the role of perceived ease of use in the TAM is a significant factor enabling users to obtain advantages from Information Technology. Thus, on the basis of the above discussion, in this study, the effect of perceived ease of use on behavioral intention for the adoption of IoT systems integrated with blockchain is expected to play a significant role. Consequently, the following is hypothesized:

Hypothesis 1B (H1B). *Perceived ease of use has a positive effect on IoT blockchain technology adoption.*

Personal competency. Building technical competency is complex and a collection of factors are involved, including people, knowledge, new skills, and effective abilities to fulfill tasks and responsibilities. Personal competence is made up of self-awareness, self-regulation, and self-motivation [33]. In the growth of this new technology, people need training in new tasks as well as with the IoT-enabled equipment and blockchain devices. The status of a self-aware person adds a new dimension to IoT devices integrated with blockchain because most of the operations are managed from the Internet for efficiency, reliability, and to reach the required level of security. Self-regulation can help to properly and safely operate technological equipment and can increase productivity through learning from operational data [34]. Pokrovskaya et al. [27] referred to knowing the personal features of candidates, and their motivations and interests as presented through a human resources portfolio; however, this seems more appropriate to the practice of creating infrastructure and requires a high level of security. Therefore, personal competency with the IoT with blockchain technology must be advocated to achieve successful adoption.

Hypothesis 1C (H1C). *Personal competency has a significant effect on IoT blockchain technology adoption.*

Transaction intention. Using information technology is a powerful method that contributes to the development of transaction intention. Blockchain technology is widely used in transactions to save time and resources, which allow individuals to conduct their transactions in the place and time that suits them. Jaoude and Saade [26] found transaction intentions to be one of the factors affecting consumer acceptance through blockchain technology. Thus, on the basis of the above discussion, in this study, the effect of transaction intention on behavioral intention is expected to play a significant role. Accordingly, the following is hypothesized:

Hypothesis 1D (H1D). *Transaction intention has a significant positive effect on IoT blockchain technology adoption.*

3.1.2. Social Related Factors

Social factors refer to the factors in the social environment that are important to the adoption of new technology. A network of social relationships is an important source of support and appears to be an important factor influencing behavior and decision-making. In addition, social factors depend on the ability of people to form and enhance a reputation with others as regards adopting specific technologies. Thus, we divided the social impact into two specific factors: the social network and reputation.

Social Network. Social networks trace a significant amount of user behavioral data. Therefore, analyzing this behavioral data can provide great advantages. The Social Internet of Things (SIoT) is one of the concepts in which social networks meet IoT systems to support networking services in more effective and efficient ways [35]. According to Guo et al. [36], communication between people is the core of forging social connections. In opportunistic IoT systems, contacts between nodes are fundamentally linked with user social behaviors and social features. Opportunistic IoT architecture allows the deployment and use of smart objects for collaboration between users who influence each other. Thus, peer influence becomes more important than ever, offering a tremendous opportunity for new business [36]. Blockchain technology plays an important role in user behavior management for network media and ensuring transaction security [37,38]. There are many models designed with blockchain technology that apply decentralized contracts to motivate trust networks, and therefore, to secure information exchange contracts [39–41]. Blockchain, as an effective technology for decentralized distributed storage, supports trusted social networks, and different studies have shown the consistent relationship between social networks and behavioral intention regarding the adoption of new technology [42–44]. Thus, the following is hypothesized:

Hypothesis 2A (H2A). *Social networks have a positive effect on IoT blockchain technology adoption.*

Reputation. Reputation refers to the general belief in or estimation of something. When the technology is trustworthy and brings benefits, it has a good reputation. In previous literature [45], reputation is used to assess the quality of the system where IoT devices for data trading are centralized and lack a reputation system. As a result, the IoT system was integrated with the Ethereum blockchain to ensure data quality and improve user behavior. Zheng et al., in 2017 [46], discussed the most commonly used blockchains in the financial domain that allow one to store the user's reputation on the blockchain to improve performance. Therefore, we can conclude that there is a positive relationship between reputation and behavioral intention towards the adoption of IoT systems integrated with blockchain:

Hypothesis 2B (H2B). *Reputation has a significantly positive social effect on IoT blockchain technology adoption.*

3.2. Trust Factors

3.2.1. Data Related Factors

Data in this context indicates the extent to which data are produced and exchanged in IoT systems. It also influences the decision makers in adopting blockchain into IoT environments. Different models and studies have suggested a number of data-related factors that could influence the decision makers trust and thus affect adoption. On the basis of the literature, a number of factors have been defined, as listed below.

Data integrity. This focuses on acquiring data assurance, completeness, consistency, and reliability over the entire data life-cycle. Most of the issues related to data integrity have appeared because of the cloud services attached to IoT; one of the drawbacks is the lack of control over the data available in cloud storage [47–49]. The essential design of blockchain is a series of growing blocks hashed with cryptography to provide data integrity by enabling a fully decentralized system. Liu et al. [47] proposed a blockchain-based framework to enable decentralized data integrity verification for IoT data stored in the semi-trusted cloud. Moreover, Wei et al. [48] presented an integrated model using a blockchain technology. The distributed virtual machine agent model is deployed in the cloud using mobile agent technology. It is able to ensure reliability for data storage, monitoring, and verification, which is also essential for building a blockchain integrity protection mechanism. In essence, blockchain technologies can enable decentralized and trustworthy features for the IoT, thus, blockchain technology has an impact regarding IoT adoption.

Hypothesis 3A (H3A). *Data integrity has a positive effect on IoT blockchain technology adoption.*

Data validity. This factor is concerned with the correctness of the data. The challenge has broadened because of the vast scale of IoT systems, distributed agents, and network partitioning. Thus, blockchain technology has integrated with other supported technologies: P2P networks, distributed ledgers, asymmetric encryption, and smart contracts. These technologies overcome the limitations of IoT data validity to ensure secure, reliable, open, fair, efficient, and intelligent communication [50]. Wang et al. [51] introduced a testbed to evaluate the impact of blockchain on validating data through accelerating block mining rates and network conditions on the capacity of public blockchains. The integration of IoT and blockchain systems becomes increasingly important to secure IoT data; thus, the following is hypothesized:

Hypothesis 3B (H3B). *Data validity has a positive influence on IoT blockchain technology adoption.*

Data governance. This refers to the process of formal coherence of people, processes, and technology to enable organizations to leverage data as an enterprise benefit. This is part of most data-driven capabilities such as change management, data warehousing, database design, and other related data processes and repositories. It focuses on defining data strategy, policies, standards, procedures, and metrics. It is involved in tracking the delivery of data management projects and services. Regulations on data are always updated to control privacy or other rules for each domain. In health, Dasgupta et al. [52] claimed the lake on how effectively construct data governance for IoT enabled digital IS ecosystem. Thus, they improved the 4I framework, which is iteratively developed and updated using the Design Science Research (DSR) method. This method addresses the organization's processing need to maintain the robustness of the governance model and provide coverage across the entire data life-cycle in IoT-enabled digital IS ecosystems. In addition, Sicari et al. [53] overcame the issue by concentrating on how to present, secure, protect, and integrate data. They presented a distributed architecture for managing IoT data extraction and processing that also includes algorithms for the assessment of data quality and security levels of the considered sources. Therefore, we can conclude that, in order to gain better blockchain technology that leads to IoT adoption, good data governance is crucial. Hence, we will assume the following:

Hypothesis 3C (H3C). *Data governance has a significant effect on IoT blockchain technology adoption.*

Data privacy. It has been of high significance since it concerns of how the data is controlled, used, and who has access to it. The European Union (EU) issued the General Data Protection Regulation (GDPR), which an organization must fulfill when using others data. In particular, data privacy seeks to empower the users to make their own decisions about who can process their data and for what purpose. Organizations that adopt blockchain in IoT systems expect a massive amount of data generated by IoT sensors and devices, yet this contains sensitive and private user data. Therefore, it is crucial to limit the types of data that can be uploaded to the blockchain functions. Moreover, data privacy laws, for instance the GDPR, are very strict, and following the regulations in terms of ensuring the data is not linked with individuals is a challenging process. A number of studies on data privacy for blockchain and IoT systems have been published [54–56]; one such study by Zyskind et al. [54] proposed a decentralized personal data management system that ensures users own and control their data. The system is integrated with a protocol that turns a blockchain into an automated access-control manager that does not require trust in a third party. The transactions embedded in the system are able to carry instructions, involving, for example, the storing, querying, and sharing of data. In addition, Liang et al. [55] designed a decentralized and trusted cloud data provenance architecture using blockchain technology called ProvChain. Decentralized systems have dominated in terms of data privacy in IoT Blockchain Platforms; Cha et al. [56] presented a decentralized system to preserve user privacy on IoT devices using the Ethereum platform. Consequently, it is evident that, for any new IoT blockchain technology or service entering a new market, data privacy must be taken into the account. Thus, the following is hypothesized:

Hypothesis 3D (H3D). *Data privacy has a positive influence on IoT blockchain technology adoption.*

3.2.2. Security Related Factors

Security factors are concerned with the crucial pillars that affect the adoption of blockchain in the IoT infrastructure. Considering security, privacy, and reliability of technology and transactions has a noteworthy impact on stakeholder trust. Most of the literature suggests that there is some relationship between security and adoption of blockchain technology in the IoT systems [57–60]. In conclusion, this focuses attention on defining security-related factors, which can be divided into transaction risk and technological risk.

Transaction risk. Blockchain was initially introduced through cryptocurrencies for traditional banking and financial systems. Nowadays, the effect of blockchain technology has expanded to cover other industries, including technology-based applications in supply chain management, marketing, and finance. Stakeholders seek to ensure decentralization, streamlining, and risk-free transactions within IoT infrastructures [60]. It is important to consider the transaction costs, which have an impact on final decisions [60–62]. Schmidt and Wagner [61] argued that blockchain provides transparent and valid transactions which critically affect the IoT services produced. Roy et al. [62] presented a strong security-based blockchain service along with some encryption approaches for secure communication. This solution limits the risk of cyber attacks targeting the centralized systems. Hence, securing transactions throughout blockchain services supports the the safe transmission of data.

Hypothesis 4A (H4A). *Transaction risk has a positive impact on the intention to use blockchain technology in IoT systems.*

Technological risk. IoT systems have proven their effectiveness for many organizations, but its adoption has tremendous and unforeseen risks which require critical transformations. The risks have been highlighted in various techniques and domains; Brous et al. [58] presented an analysis on the synthesis of potential risks generated by IoT adoption in organizations. They argued that some changes associated with IoT adoption in regard to technology implementation costs, difficult interoperability and integration, and limited trust in IoT services result in low quality benefits. Some long standing assumptions regarding the influencing factors have been questioned [57,59,63,64]. In line with these discussions, the technological risks associated with the adoption of blockchain in IoT systems are included in the research model, hence, the following is hypothesized:

Hypothesis 4B (H4B). *The technological risk positively affects the intention to use blockchain technology in IoT systems.*

Table 1. The survey questions' description.

Dimension Hypotheses	Domain Hypotheses	Description of Survey Questions
H1 Attitude-related factors have a positive influence on behavior intention towards IoT technology adoption	**H1A:** Perceived usefulness has a positive effect on IoT blockchain technology adoption.	To measure the increase in the operating efficiency and system performance within the work environment.
	H1B: Perceived ease of use has a positive effect on IoT blockchain technology adoption.	To measure the ease of apply IoT technology and its integration with other technologies.
	H1C: Personal competency has a significant effect on IoT blockchain technology adoption.	To measure the level of cognitive knowledge.
	H1D: Transaction intention has a significant positive effect on IoT blockchain technology adoption.	To measure the level of transparency and clarity.
H2 Social influence related factors have a positive influence on behavior intention towards IoT	**H2A:** Social network has a positive effect on IoT blockchain technology adoption.	To study social impact through a secure network and open source.
	H2B: Reputation has a significant positive effect of social on IoT blockchain technology adoption.	To measure the role of IoT blockchain technology in managing data and trusting it through distributed systems.
H3 Data related factors have a positive influence on trust towards IoT	**H3A:** Data integrity has a positive effect on IoT blockchain technology adoption.	To study the effect of IoT blockchain technology on the data integrity that are consistent with the objective of the data creators.
	H3B: Data validity has a positive influence on IoT blockchain technology adoption.	To study the level of IoT blockchain technology outputs in correctly and reasonably.
	H3C: Data governance has a significant effect on IoT blockchain technology adoption.	To measure the contributions of IoT blockchain technology to ensuring the preservation, protection and control of data by the authorized persons.
	H3D: Data privacy has a positive influence on IoT blockchain technology adoption.	To measure the extent of IoT blockchain technology in ensuring the privacy and confidentiality of data.
H4 Security related factors have a positive influence on trust towards IoT	**H4A:** Transaction risk has a positive impact on the intention to use blockchain technology in IoT.	To measure the operations executed through IoT blockchain technology led to reduce the risk percentage.
	H4B: Technology risk positively affects the intention to use blockchain technology in IoT.	To measure IoT technology led to reduces the risk of thirdparty service failures.

4. Methodology

4.1. Data Collection and Measurement

This study revealed the level of integration between blockchain and IoT technologies, and the benefits and opportunities they achieved. The Technology Acceptance Model (TAM) [21] constitutes the conceptual framework of this study. The survey provides a method of collecting data that allows the researcher to discover knowledge about the phenomena under study. We developed a web-based survey to collect data from specialists in blockchain technology and IoT systems in Saudi Arabia. The survey was distributed to individuals who were randomly selected throughout LinkedIn as well as author contacts. A questionnaire was conducted for the collection of data from an intended sample of 120 people interested in the adoption of blockchain and IoT technologies. The survey was conducted over a period of three months, starting from 5 October 2019 to 7 January 2020. A link to the survey was sent to 120 potential respondents and 85 responses were received. After removing the incomplete responses (e.g., missing data or unengaged respondents), 82 valid questionnaires were selected for data analysis and interpretation. Therefore, the percentage of respondents out of 120 was 68.33%, which is acceptable in terms of generalizing the study, according to Dillman [65].

The survey questions were developed based on relevant studies. The variables for the current study are divided into four categories: Attitude-related factors (8 items) and Social influence-related factors (6 items), both of which are related to behavioral intention; Data-related factors (7 items); Security-related factors (4 items), which are related to trust. The questionnaire consisted of 25 questions in total, all of which were designed to be multiple choice questions and to cover the hypotheses described in Table 1.

The data collected were interpreted, classified, and transferred into coded form, entered into Microsoft Excel, and transferred in the Statistical Package for Social Sciences (SPSS). The respondents were asked to rate their agreement on each statement using a 1–5 Likert scale [66]. The response distributions clearly demonstrated that the majority of factors were either strongly accepted or accepted. Only the personal competency factor demonstrated a limited degree of disagreement.

4.2. Data Analysis and Results

The measurement model was examined for internal consistency, convergence, and discriminant validity. In the first stage, the reliability and validity of the model were measured, and the hypotheses shown in the conceptual model, see Figure 1, were tested in the second stage. Cronbach's Alpha test is commonly used to evaluate survey reliability in order to measure the internal consistency of the survey items. Thus, Cronbach's Alpha test was utilized, as shown in Table 2. The Cronbach's alpha results of each framework's dimension of factors were analyzed to consider their reliability based on the theoretical model. According to Cavana et al. [67], the values must be above 0.6 in order to confirm the model's consistency and reliability. All four categories for the sample of 82 participants have Cronbach's Alpha values ranging between 0.72 to 0.84, which indicates good internal consistency and reliability among the items. As shown in Table 2, the mean of the items range from 3.57 to 4.35, while the standard deviations of all the items range from 0.57621 to 1.05105, indicating that all the constructs have great internal consistency and adequate convergence.

The validity of the conceptual model was examined based on variables and corresponding items in the model. The validity test on the study variables was dependent on the correlation coefficients that are summarized in Table 3. The results imply that the coefficient value between constructs lies between 0.65 and 0.33, which indicates a strong and medium correlation. Furthermore, the results show that all the instruments are valid, with a p-value $< 0.5\%$. Therefore, the results of convergent validity and discriminant validity are sufficient to support the proposed constructs of the conceptual model.

4.3. Hypotheses Testing

Regression is used to test a proposed research model by presenting the model's constructs with their dependence relationships. Then, the hypotheses are tested to prove relationships between the different constructs. The hypothesis test was based on several related statistical tests, such as squared multiple correlations (R^2), which indicate the variance of the dependent constructs, and standardized path coefficients (β), which indicate the strengths of the relationships between the independent and dependent variables. The test also produces a t-value and p-value, which revealed that there is a significant difference regarding the effect of the acceptance and usage of IoT blockchain technology. On the basis of the results summarized in the Table 4, each of the hypotheses was either supported or rejected.

Table 2. The reliability test.

SI.No	Item/Construct	No. of Items	Mean	Standard Deviation	Cronbach's Alpha Value
1	Perceived Usefulness	2	4.35	0.68211	0.898
2	Perceived Ease of Use	2	3.98	0.87286	0.9
3	Personal Competency	2	3.57	1.05105	0.91
4	Transaction Intention	2	4.23	0.66655	0.896
5	Social Network	3	4.13	0.63175	0.898
6	Reputation	3	3.98	0.73201	0.897
7	Data Integrity	2	4.3	0.64556	0.903
8	Data Validity	2	4.25	0.57621	0.899
9	Data Governance	2	4.27	0.68488	0.896
10	Data Privacy	2	4.23	0.75849	0.894
11	Transaction Risk	2	4.12	0.74804	0.9
12	Technology Risk	2	3.93	0.78164	0.9

Table 3. Pearson Correlation.

		PU	PEoU	PC	TI	SN	RE	DI	DV	DG	DP	TRR	TER
PU	Pearson Correlation	1											
	Sig. (2- tailed)												
PEoU	Pearson Correlation	0.592	1										
	Sig. (2- tailed)	0.000											
PC	Pearson Correlation	0.330	0.509	1									
	Sig. (2- tailed)	0.004	0.000										
TI	Pearson Correlation	0.652	0.560	0.390	1								
	Sig. (2- tailed)	0.000	0.000	0.000									
SN	Pearson Correlation	0.486	0.380	0.212	0.549	1							
	Sig. (2- tailed)	0.000	0.000	0.057	0.000								
RE	Pearson Correlation	0.550	0.554	0.410	0.491	0.515	1						
	Sig. (2- tailed)	0.000	0.000	0.000	0.000	0.000							
DI	Pearson Correlation	0.401	0.219	0.186	0.414	0.550	0.487	1					
	Sig. (2- tailed)	0.000	0.050	0.097	0.000	0.000	0.000						
DV	Pearson Correlation	0.436	0.373	0.349	0.547	0.545	0.504	0.771	1				
	Sig. (2- tailed)	0.000	0.001	0.001	0.000	0.000	0.000	0.000					
DG	Pearson Correlation	0.582	0.414	0.439	0.550	0.590	0.582	0.561	0.588	1			
	Sig. (2- tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000				
DP	Pearson Correlation	0.513	0.523	0.506	0.604	0.428	0.483	0.336	0.484	0.535	1		
	Sig. (2- tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.002	0.000	0.000			
TRR	Pearson Correlation	0.441	0.402	0.327	0.555	0.477	0.487	0.336	0.356	0.434	0.616	1	
	Sig. (2- tailed)	0.000	0.000	0.003	0.000	0.000	0.000	0.002	0.001	0.000	0.000		
TER	Pearson Correlation	0.333	0.387	0.455	0.367	0.664	0.395	0.369	0.426	0.426	0.633	0.469	1
	Sig. (2- tailed)	0.002	0.000	0.000	0.001	0.000	0.000	0.001	0.000	0.000	0.000	0.000	

Table 4. Summary of the hypothesis testing results.

Path Relationship	**Pathcoefficient Standardized Coefficients (β)**	***p*-Value**	***t*-Value**	**R^2**	**Hypothesis Validation**
H1: Attitude—Behavior Intention	0.832	0	24.864	0.885	Supported
H1A: Perceived Usefulness—Attitude	0.728	0.005	10.648	0.581	Supported
H1B: Perceived Ease of Use—Attitude	0.626	0	14.149	0.711	Supported
H1C: Personal Competency—Attitude	0.47	0	10.687	0.588	Supported
H1D: Transaction Intention—Attitude	0.754	0.005	11.059	0.605	Supported
H2: Social—Behavior Intention	0.828	0.002	15.602	0.755	Supported
H2A: Social Network—Social	0.799	0	14.295	0.721	Supported
H2B: Reputation—Social	0.722	0.002	17.362	0.792	Supported
H3: Data—Trust	0.94	0	26.357	0.898	Supported
H3A: Data Integrity—Data	0.627	0	9.964	0.557	Supported
H3B: Data Validity—Data	0.762	0	12.237	0.655	Supported
H3C: Data Governance—Data	0.676	0	14.513	0.727	Supported
H3D: Data Privacy—Data	0.568	0	11.593	0.63	Supported
H4: Security—Trust	0.728	0	17.013	0.786	Supported
H4A: Transaction Risk—Security	0.745	0	14.347	0.723	Supported
H4B: Technology Risk—Security	0.724	0	15.232	0.746	Supported
H0A: Behavior Intention—Adopting Blockchain in IoT	0.904	0	34.336	0.936	Supported
H0B: Trust—Adopting Blockchain in IoT	0.923	0	24.331	0.882	Supported

Table 4 shows the squared multiple correlations of the various variables in the model R^2 in the range 0.755 to 0.898, which means the model (Attitude-related factors; Social influence-related factors; Data-related factors; Security-related factors) can explain 76% to 90% of the variations of the adoption of IoT blockchain technology.

According to Table 4, the perceived usefulness, perceived ease of use, personal competency, transaction intention, social network, and reputation had a positive and significant effect on behavioral intention. Further, factors related to behavioral intention and social factors had a positive effect on the behavioral intention to the adoption of IoT blockchain technologies, with the standardized path coefficient being (β = 0.832 and sig. = 0.000), (β = 0.828 and sig. = 0.002), respectively. In this manner, H1, H2, and H0A were emphasized as the main and sub-hypotheses. On the other hand, factors related to data in terms of integrity, validity, governance, and privacy had a positive effect (β = 0.940 and sig. = 0.000) on trust towards IoT blockchain technology adoption, thereby confirming H3. The risk of transaction and technology had a significant relationship with trust in IoT blockchain technology adoption (β = 0.728 and sig. = 0.000), thus H4 was supported.

5. Discussion

This study measures the effect of integrating blockchain technology into IoT technology. We firstly identified the critical factors related to the adoption of blockchain and IoT technologies. The significance of the study concentrates on developing a comprehensive theoretical conceptual model that can explain a large proportion of variance in the intention to adopt blockchain with IoT technology. The Technology Acceptance Model (TAM) was used and developed to assess the level of integration of blockchain and IoT technology. The results of the data analysis gathered throughout the survey show the strength of the proposed blockchain IoT technology model. The statistical analysis on the four dimensions of factors revealed a significant positive influence in terms of adopting blockchain IoT technology. The study confirmed the hypotheses with strong correlations in four dimensions of factors and sub-factors. This was done by including the opinions of specialists in both blockchain and IoT technologies.

The dimensions of factors were evaluated using the survey. When comparing the different dimensions and factors of the model with respect to mean, data-related factors were found to be the most influential in relation to the other factors. In particular, data validity was the most critical factor, and more attention should be paid to it. Thus, professionals and users of blockchain and IoT systems have to be aware of data validation strategies and regulations. As was discussed in Section 3.2, data validity focuses on the correctness of data, since the methodology involved in blockchain IoT technology requires a level of distribution and partitioning. This maintains an open environment that produces massive data that requires reliable and efficient communication between connected devices. Adaptive buffers, error detection values, and thresholds are some example of techniques to guarantee data validity [68].

When it comes to the coefficient of determination R^2, which measures the proportion of the variance in the dependent variable that is predictable from the independent variable(s), it is notable from Table 4 that the behavioral intention factor and its sub-factors had the highest value of 0.94. This indicates the importance of attitude towards blockchain and IoT systems in addition to social influencers. In particular, social networks and reputation have a critical impact on behavioral intention since they have the highest R^2 values [36,38,45].

In terms of the Pearson correlation shown in Table 3, the greatest correlation was demonstrated between perceived usefulness and transaction intention. This correlation had an indirect effect on the other factors. Generally, the results illustrate that PU not only has a direct effect on the intention to use a technology, but also it has an indirect effect through the TI on the intention to use a technology. Thus, the results show that TI has a direct effect on the intention to use blockchain and IoT technology [26].

With regard to the negative impact on the conceptual model, the results show no significant negative impact except security factors and the personal competency in attitude factor. The values are very close to the other factors in the model, and they only show a slight difference when compared with the rest of the factors (see Table 4). In this case, security risks should not be covered in this type of technology unless security threats have encountered [57–60]. In today's digital interconnected platforms especially for IoT systems, which consist of open and connected devices which are exposed to attacks and possibilities for cybercriminals. As discussed in Section 3.2.2, guaranteeing decentralization, streamlining, and risk-free transactions within IoT infrastructures is critical to limit cyber attacks targeting centralized systems [60].

In summary, trust-related factors in the adoption of blockchain IoT technology were more significant than behavioral intention factors. This is because of the importance of data-related factors on trust. Thus, professionals should consider this in terms of increasing the level of trust. The findings additionally revealed that social-related factors are important for the adoption of blockchain IoT technology, but the consequences of this are limited in terms of behavioral intention. To explain, professionals may have a solid reputation, good social networking skills, a good level of interest, and can commit, but they have low or no personal competency, which affects the overall behavioral intention to use the technology.

6. Conclusions

In conclusion, this paper addresses the close connection between blockchain and IoT technologies. In the digital era, new technologies such as blockchain and IoT systems have come to dominate in several industries because of the robustness and effectiveness they can offer. In this paper, we propose a conceptual model that identifies the critical factors that have an impact on integrating blockchain and IoT technology. The analysis of the study reveals the positive impact of data-related factors, i.e., data integrity, data validity, data governance, and data privacy. Moreover, behavioral intention and the related factors have a significant effect in terms of adopting these two technologies. In contrast, security-related factors are less significant as compared with the other factors, which is reasonable since these types of technology require open communication and form an open network of connected devices. This study has some limitations that need to be addressed. The first limitation concerns the generalizability of the findings. The study was conducted in Saudi Arabia, which highly promotes the emergence of technologies and tools that support the 2030 vision. This involves enhancing business and investment in the country and empowering the financial industry to a tremendous degree. Thus, countries with a limited technological infrastructure will not able to adopt the proposed model effectively. In addition, these technologies are novel and professionals with a limited technical background will struggle to adopt them in their business. Therefore, knowledge of the factors that effect their integration is not sufficient in terms of attaining the potential benefits.

Future work may further explore the problem under study, extending it to encompass more factors or enhancing the current model to fit any improvements in both technologies. Since this model is directed at applications and domains that exist in Saudi Arabian sectors, the model could be improved and aligned with cultural beliefs and/or governmental regulations. In terms of practical enhancements, some changes in practical standards or performance indicators could effect the model's adoption, thus more factors could be adopted. Lastly, to verify the validity of the proposed model, a real-world experiment should be performed in real industries to tackle any limitations and/or to reveal avenues for further research.

Author Contributions: These authors contributed to this work as conceptualization, L.A.; data curation, N.A.; formal analysis, L.A. and N.A.; methodology, L.A. and N.A.; project administration, L.A.; resources, L.A.; validation, L.A. and N.A.; visualization, N.A.; writing—original draft, L.A. and N.A.; writing—review and editing, L.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]
2. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; 2008.
3. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2018**, *36*, 55–81. [CrossRef]
4. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
5. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2018**, *125*, 251–279. [CrossRef]
6. Viriyasitavat, W.; Anuphaptrirong, T.; Hoonsopon, D. When blockchain meets internet of things: Characteristics, challenges, and business opportunities. *J. Ind. Inf. Integr.* **2019**, *15*, 21–28. [CrossRef]
7. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
8. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2018**, *126*, 45–58. [CrossRef]
9. Adelmann, R.; Langheinrich, M.; Floerkemeier, C. Toolkit for bar code recognition and resolving on camera phones-jump starting the internet of things. In *INFORMATIK 2006—Informatik für Menschen—Band 2, Beiträge der 36. Jahrestagung der Gesellschaft für Informatik eV (GI)*; Gesellschaft für Informatik eV: Bonn, Germany, 2006.
10. Dachyar, M.; Zagloel, T.Y.M.; Saragih, L.R. Knowledge growth and development: Internet of things (IoT) research, 2006–2018. *Heliyon* **2019**, *5*, e02264. [CrossRef]
11. Balasubramanian, V.; Zaman, F.; Aloqaily, M.; Al Ridhawi, I.; Jararweh, Y.; Salameh, H.B. A mobility management architecture for seamless delivery of 5G-IoT services. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–7.
12. AlHogail, A. Improving IoT technology adoption through improving consumer trust. *Technologies* **2018**, *6*, 64. [CrossRef]
13. Negka, L.; Gketsios, G.; Anagnostopoulos, N.A.; Spathoulas, G.; Kakarountas, A.; Katzenbeisser, S. Employing Blockchain and Physical Unclonable Functions for Counterfeit IOT Devices Detection. In Proceedings of the International Conference on Omni-Layer Intelligent Systems, Crete, Greece, 5–7 May 2019; pp. 172–178.
14. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. *Future Internet* **2019**, *11*, 161. [CrossRef]

15. Mendki, P. Blockchain Enabled IoT Edge Computing. In Proceedings of the 2019 International Conference on Blockchain Technology (ICBCT 2019), San Diego, CA, USA, 25–30 June 2019; ACM: New York, NY, USA, 2019; pp. 66–69. [CrossRef]
16. Spathoulas, G.; Giachoudis, N.; Damiris, G.P.; Theodoridis, G. Collaborative Blockchain-Based Detection of Distributed Denial of Service Attacks Based on Internet of Things Botnets. *Futur. Internet* **2019**, *11*, 226. [CrossRef]
17. Tseng, L.; Wong, L.; Otoum, S.; Aloqaily, M.; Othman, J.B. Blockchain for managing heterogeneous internet of things: A perspective architecture. *IEEE Netw.* **2020**, *34*, 16–23. [CrossRef]
18. Aloqaily, M.; Boukerche, A.; Bouachir, O.; Khalid, F.; Jangsher, S. An Energy Trade Framework Using Smart Contracts: Overview and Challenges. *IEEE Netw.* **2020**. [CrossRef]
19. Morkunas, V.J.; Paschen, J.; Boon, E. How blockchain technologies impact your business model. *Bus. Horiz.* **2019**, *62*, 295–306. [CrossRef]
20. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2019**, *6*, 93–97. [CrossRef]
21. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340. [CrossRef]
22. Fishbein, M.; Ajzen, I. *Belief, Attitude, Intention, and Behavior Addison-Wesley*; Wesley Publishing Co.: Reading, MA, USA, 1975.
23. de Boer, P.S.; van Deursen, A.J.; Van Rompay, T.J. Accepting the Internet-of-Things in our homes: The role of user skills. *Telemat. Inform.* **2019**, *36*, 147–156. [CrossRef]
24. Mital, M.; Chang, V.; Choudhary, P.; Papa, A.; Pani, A.K. Adoption of Internet of Things in India: A test of competing models using a structured equation modeling approach. *Technol. Forecast. Soc. Chang.* **2018**, *136*, 339–346. [CrossRef]
25. Alanazi, M.; Soh, B. Behavioral Intention to Use IoT Technology in Healthcare Settings. *Eng. Technol. Appl. Sci. Res.* **2019**, *9*, 4769–4774.
26. Jaoude, J.A.; Saade, R. Blockchain Factors for Consumer Acceptance. *Int. J. Bus. Manag. Technol.* **2017**.
27. Pokrovskaia, N.N.; Spivak, V.A.; Snisarenko, S.O. Developing Global Qualification-Competencies Ledger on Blockchain Platform. In Proceedings of the 2018 XVII Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES), St. Petersburg, Russia, 14–15 November 2018; pp. 209–212.
28. Venkatesh, V.; Morris, M.G.; Davis, G.B.; Davis, F.D. User acceptance of information technology: Toward a unified view. *MIS Q.* **2003**, *27*, 425–478. [CrossRef]
29. Folkinshteyn, D.; Lennon, M. Braving Bitcoin: A technology acceptance model (TAM) analysis. *J. Inf. Technol. Case Appl. Res.* **2016**, *18*, 220–249. [CrossRef]
30. Knauer, F.; Mann, A. What is in It for Me? Identifying Drivers of Blockchain Acceptance among German Consumers. *J. Br. Blockchain Assoc.* **2019**, *3*, 10484. [CrossRef]
31. Dong, X.; Chang, Y.; Wang, Y.; Yan, J. Understanding usage of Internet of Things (IOT) systems in China. *Inf. Technol. People* **2017**, *30*, 117–138. [CrossRef]
32. Jaafreh, A. The Effect Factors in the Adoption of Internet of Things (IoT) Technology in the SME in KSA: An Empirical Study'. *IRMBR Int. Rev. Manag. Bus. Res.* **2018**, *7*, 135–148. [CrossRef]
33. Goleman, D. *Emotional Intelligence*; Bantam Books: New York, NY, USA, 2006.
34. Gronau, N.; Ullrich, A.; Teichmann, M. Development of the industrial IoT competences in the areas of organization, process, and interaction based on the learning factory concept. *Procedia Manuf.* **2017**, *9*, 254–261. [CrossRef]
35. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (siot)—When social networks meet the internet of things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]
36. Guo, B.; Yu, Z.; Zhou, X.; Zhang, D. Opportunistic IoT: Exploring the social side of the internet of things. In Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Wuhan, China, 23–25 May 2012; pp. 925–929.
37. Buccafurri, F.; Lax, G.; Nicolazzo, S.; Nocera, A. Overcoming limits of blockchain for IoT applications. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017; pp. 1–6.

38. Xu, R.; Zhang, L.; Zhao, H.; Peng, Y. Design of network media's digital rights management scheme based on blockchain technology. In Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, Thailand, 22–24 March 2017; pp. 128–133.
39. Fu, D.; Fang, L. Blockchain-based trusted computing in social network. In Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 14–17 October 2016; pp. 19–22.
40. Al-Saqaf, W.; Seidler, N. Blockchain technology for social impact: Opportunities and challenges ahead. *J. Cyber. Policy* **2017**, *2*, 338–354. [CrossRef]
41. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
42. Barger, V.; Peltier, J.W.; Schultz, D.E. Social media and consumer engagement: A review and research agenda. *J. Res. Interact. Mark.* **2016**, *10*, 268–287. [CrossRef]
43. Salloum, S.A.; Mhamdi, C.; Al Kurdi, B.; Shaalan, K. Factors affecting the adoption and meaningful use of social media: A structural equation modeling approach. *Int. J. Inf. Technol. Lang. Stud.* **2018**, *2*, 96–109.
44. Alsaleh, D.A.; Elliott, M.T.; Fu, F.Q.; Thakur, R. Cross-cultural differences in the adoption of social media. *J. Res. Interact. Mark.* **2019**. [CrossRef]
45. Javaid, A.; Zahid, M.; Ali, I.; Khan, R.J.U.H.; Noshad, Z.; Javaid, N. Reputation System for IoT Data Monetization Using Blockchain. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Antwerp, Belgium, 7–9 November 2019; Springer: Cham, Switzerland, 2019; pp. 173–184.
46. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
47. Liu, B.; Yu, X.L.; Chen, S.; Xu, X.; Zhu, L. Blockchain based data integrity service framework for IoT data. In Proceedings of the 2017 IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, 25–30 June 2017; pp. 468–475.
48. Wei, P.; Wang, D.; Zhao, Y.; Tyagi, S.K.S.; Kumar, N. Blockchain data-based cloud data integrity protection mechanism. *Future Gener. Comput. Syst.* **2020**, *102*, 902–911. [CrossRef]
49. Machado, C.; Fröhlich, A.A.M. Iot data integrity verification for cyber-physical systems using blockchain. In Proceedings of the 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC), Singapore, 29–31 May 2018; pp. 83–90.
50. Lu, Y. The blockchain: State-of-the-art and research challenges. *J. Ind. Inf. Integr.* **2019**, 15, 80—90. [CrossRef]
51. Wang, X.; Yu, G.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Zheng, K.; Niu, X. Capacity of Blockchain based Internet-of-Things: Testbed and Analysis. *Internet Things* **2019**, *8*, 100109. [CrossRef]
52. Dasgupta, A.; Gill, A.Q.; Hussain, F.K. A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems. *DATA* **2019**. [CrossRef]
53. Sicari, S.; Rizzardi, A.; Cappiello, C.; Miorandi, D.; Coen-Porisini, A. Toward data governance in the internet of things. In *New Advances in the Internet of Things*; Springer: Cham, Switzerland, 2018; pp. 59–74.
54. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
55. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 14–17 May 2017; pp. 468–477.
56. Cha, S.C.; Chen, J.F.; Su, C.; Yeh, K.H. A blockchain connected gateway for BLE-based devices in the internet of things. *IEEE Access* **2018**, *6*, 24639–24649. [CrossRef]
57. Park, C.; Kim, Y.; Jeong, M. Influencing factors on risk perception of IoT-based home energy management services. *Telemat. Inform.* **2018**, *35*, 235–2365. [CrossRef]
58. Brous, P.; Janssen, M.; Herder, P. The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *Int. J. Inf. Manag.* **2019**. [CrossRef]
59. Nikou, S. Factors driving the adoption of smart home technology: An empirical assessment. *Telemat. Inform.* **2019**, *45*, 101283. [CrossRef]

60. Ahluwalia, S.; Mahto, R.V.; Guerrero, M. Blockchain technology and startup financing: A transaction cost economics perspective. *Technol. Forecast. Soc. Chang.* **2020**, *151*, 119854. [CrossRef]
61. Schmidt, C.G.; Wagner, S.M. Blockchain and supply chain relations: A transaction cost theory perspective. *J. Purch. Supply Manag.* **2019**, *25*, 100552. [CrossRef]
62. Roy, D.G.; Das, P.; De, D.; Buyya, R. QoS-aware secure transaction framework for internet of things using blockchain mechanism. *J. Netw. Comput. Appl.* **2019**, *144*, 59–78.
63. Macaulay, T. Chapter 3—Requirements and Risk Management. In *RIoT Control*; Macaulay, T., Ed.; Morgan Kaufmann: Boston, MA, USA, 2017; pp. 57–79. [CrossRef]
64. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2019**, 100081. [CrossRef]
65. Dillman, D. *Mail and Internet Surveys: The Tailored Design Method*; Wiley & Sons: New York, NY, USA, 2000.
66. Likert, R. A technique for the measurement of attitudes. *Arch. Psychol.* **1932**, *22*, 140.
67. Cavana, R.; Delahaye, B.; Sekeran, U. *Applied Business Research: Qualitative and Quantitative Methods*; John Wiley & Sons: Hoboken, NJ, USA, 2001.
68. Alduais, N.; Abdullah, J.; Jamil, A.; Audah, L.; Alias, R. Sensor node data validation techniques for realtime IoT/WSN application. In Proceedings of the 2017 14th International Multi-Conference on Systems, Signals & Devices (SSD), Marrakech, Morocco, 28–31 March 2017; pp. 760–765.