# Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community

Wan Nurhidayat Wan Muhamad[1], Noor Afiza Mat Razali[2], Muslihah Wook[3], Khairul Khalil Ishak[4]
Norulzahrah Mohd Zainudin[5], Nor Asiakin Hasbullah[6,] Suzaimah Ramli[7]
National Defence University of Malaysia, Sungai Besi, Kuala Lumpur, Malaysia[1,2, 3, 5, 6, 7]
Management and Science University, Shah Alam, Selangor, Malaysia[4]

*Abstract*—**Intelligence data are among the critical elements used as a reference for risk-assessment and decision-making regarding national security. The intelligence data are shared among intelligence agencies in the intelligence community in improving the efficiency of their services. Centralised data with central authority is highly exposed to being an easy target of attackers. Leaked or unauthorised access of the intelligence data to a non-intelligence community will bring severe effect to a state. Blockchain as immutable and high-security technology is capable of providing cryptographic data in a decentralised environment and potentially can be applied for data sharing among the intelligence community. However, the acceptance and readiness of users on blockchain usage in the intelligence community are yet to be systematically studied. Considering the statement, this paper proposed an evaluation method to study the acceptance of blockchain technology by integrating a reliable acceptance model for blockchain technology implementation in the intelligence community. The acceptance model consisted of constructs from the Technology Acceptance Model 3 (TAM 3) and Technology Readiness Index 2 (TRI 2) and was analysed using partial least squares structural equation modelling (PLS-SEM). In this study, the result indicates that TAM 3 and TRI 2.0 integration model could contribute to determining the acceptance level in developing blockchain-based intelligence data sharing for the intelligence community.**

***Keywords—Technology acceptance model; technology readiness index; blockchain acceptance; PLS-SEM; data sharing***

## I. Introduction

Information sharing in a community becomes easier with the assistance of technology. The intelligence community also benefitted from this technology advancement by shifting its technique of gathering data from traditional Human Intelligence (HUMINT) to a more sophisticated and advanced method of Signal Intelligence (SIGINT) [1]. Information or data collected at the intelligence centre are varied and could be derived from devices and sensors. Analysed data are essential in providing tactical and operational data to organisation, governments, agencies and warfighters [2], [3]. Intelligence community need efficient information sharing among agencies involved to avoid intelligence failure. Example of intelligence failure is such as missing or inadequate data [4]. The process of intelligence data dissemination in the intelligence community is undeniably complicated and challenging. Ensuring accurate and precise data are appropriately disseminated is essential. There is no doubt that the risk of handling such clandestine and important intelligence data is excessive. Leaked or breached intelligence data could deadly affect country sovereignty which also significantly affect the civilian community such as politics, cultural, economy or even lives [1], [5].

Besides, such data shall only be handled by respected authorised agencies that are recognised as the intelligence community. Unauthorised access of data by non-intelligence agency posits grave effect to not only the intelligence community but also the security of a country [6]. Hence, past studies suggested the implementation of access control to heighten data security. As an example, multi-factor authentication technique [1]. However, in this pervasive usage and advancement of the Internet, such authentication technique is insufficient [7], [8]. Thus, there is a suggestion by researchers to consider blockchain as the additional weapon in preserving better security of data [9].

Past and current studies show a significant result of success through the implementation of blockchain in preserving better security of data [10]. Considering that intelligence data are needed to be shared among agencies in a time-wise manner without neglecting the accuracy, blockchain is good to consider to be implemented. However, the study on the implementation of blockchain in the intelligence community is yet to be done. In addition, doubt in using and accepting new technology remains the biggest challenge in introducing new technology.

Therefore, to overcome such challenges, it is highly recommended to investigate users' readiness and acceptance level towards the usage of new technology [11]. Thus, this paper will propose a conceptual model of acceptance and readiness on blockchain-based access for the intelligence community based on constructs in Technology Acceptance Model 3 (TAM 3) and Technology Readiness Level 2 (TRI 2).

The next section of this article will review the background and relevant literature on the intelligence community, blockchain technology, and acceptance studies includes TAM 3, TRI 2.0, and previous acceptance studies on blockchain technology. The conceptual model and hypotheses development are discussed in the proposed model to evaluate blockchain-based data sharing among the intelligence community. The methodology used, result and findings, discussions and conclusion are presented in the latter part of this article.

## II. Intelligence Community

National security is about a state of being free from any external or internal danger or threat to its core values. For example, social threats may include animosity from the nation that share the same border, attack by a radical group, and situation of global economic trends that may affect the welfare of the country. In similar scenario, threats or dangers could be defined as a natural disaster or a viral disease outbreak. Such threats could risk the harmony and sovereignty of the affected country. The government must be ready to mobilise its national security system when a nation faces direct or indirect threats. This is where the intelligence community played its vital role. Intelligence community must capable in providing the information needed by a country for security purposes. The primary role of the intelligence community includes to acquire and perform data analysis and share it with their client such as National Security Council (NSC), Defence Agency and more [4]. Such responsibility is given to them due to the confidential level of the information obtained in ensuring the security of a country. Information acquired are stored as intelligence data and given to any organisation that required it. The literature stated that the intelligence community operated based on the intelligence cycle. The cycle consists of planning and directions, collection, process, analyses production and dissemination [4]. The intelligence community could be any government agencies and organisation involved in the management of intelligence environment for the benefit of the country. Besides, the private sector also plays a crucial role in handling intelligence-related projects or systems with intelligence agencies [1].

## III. Blockchain Technology

Big data is an enormous and vast pooled data that is too huge for a conventional database to manage. Data is now a key asset for an organisation. Examples of pooled data are such as climate information, GPS signal, online shopping records and more [12]. With big data, there is a new challenge that arises related to the privacy and security of data [13]. Data should exhibit the CIA attributes, which are confidentiality, integrity, and accessibility to be trusted. However, systems that managed big data are prone to exploitation and have a risk to be compromised [14]. Such risk exposure bound to happen due to the wrong configuration of access control and authentication [15], [16]. The statement shows good configuration access control and authentication is indispensable in preserving data security. This is where blockchain integration in big data management come to the surface. The prior study suggests integrating blockchain in handling data, especially risky and confidential data due to its capability of protecting data [7], [9], [17].

Blockchain is defined as a number of blocks that holding information about the respective chain of the individual transaction where each block is linked to the previous block [18]**.** The linkage of blocks is based on the hash value of the previous block, or also known as the parent block. To illustrate, a block can transverse through the whole blockchain and find back each transaction that has been made through its parent block. Block that first to be created and have no parent is called the genesis [19]. According to [20], blockchain is different from any existing scalable database due to its two main features of, i) cryptography by design and ii) lack of control party. Cryptography by design referred to cryptography implementation in preserving the user identity, ensuring the ledger's integrity and the authenticity of data. The cryptography of each block is differ depending on protocol [19]. The hashing algorithms are implemented as a way to ensure blocks are well-formed, to preserve the security of block being tamper-free and be virtually unbreakable [19].

From a software architecture perspective, blockchain enables the development of a new distributed and decentralised software architecture, where confidential transaction or agreement can be made across the chain with untrusted people [10], [13], [21]. Blockchain's criteria of no-human intervening during a process of transaction made it widely applied in various field. As an example, in public services [22]–[24], healthcare [25]–[27], IoT [12], [28] rather than only on the financial system. Nowadays, usage of blockchain is increasing as its source is made as an open-source, which mean anyone can use the entire history of it or modify it legally without need of paying for the service [29].

Blockchain is proposed as the technology that could give the assurance for the intelligence data integrity since there is no central authority and fully automated that enables a safe manner of information passing. No central authority meaning anyone has rightfully approved the transaction being made. However, blockchain is still not widely used and implemented. Hence lack of awareness among the target group requires a preliminary assessment be done on blockchain acceptance and readiness that need to be addressed before the implementation decision could be made.

## IV. TAM 3 and TRI 2.0

### A. *Technology Acceptance Model 3 (TAM 3)*

Technology acceptance defined as the willingness of an individual to embrace the usage of new technology as per its designated task [30]. As a result, the Technology Acceptance Model (TAM) is established to investigate an individual's level of acceptance in adopting new technology [31], [32]. To emphasise, established TAM by [33], [34] is widely used as the research model in studies of the determinants of technology acceptance in predicting user acceptance and intentions of embracing new technology from individual's perspective. The determinants of TAM are comprising of Perceived if Usefulness (PU) and Perceived Ease of Use (PEoU). PU is defined as the degree of an individual believes that usage of the respected technology would enhance the job quality and their life. While PEoU focused on the degree of individual believes that usage of specific technology will be less of effort and easy to figure.

Researchers have proven that PU and PEoU have positively affected the attitude of an individual's towards intention to use and acceptance of the technology. Investigation on user acceptance towards the usage of technology has been done for over two decades with several models that have been established. As an example, TAM, the extension version of TAM (TAM 2) and TAM 3 [35]. Researchers suggested the application of TAM 3 due to its ability in investigating new relationship compared to TAM and TAM 2 [35], [36]. TAM 3 posits constructs on measuring individuals' acceptance and adoption of the use of technology which give more illustration on the individual's perspective upon the technology acceptance and exhibit a complete representation of constructs to observe individuals' IT adoption and use [35] thus, also suitable to study the individual acceptance of blockchain.

[35]. The relationships are i) relationship between PU and PEoU, (ii) relationship between computer anxiety and PEoU, and (iii) PEoU with behavioural intentions.

TAM 3 is established theoretically based on four factors of acceptance which is i) Social Influences, ii) Individual Differences, iii) System Characteristic and iv) Facilitating Conditions. These four factors are differently wielded influences towards PU and PEoU determinants [37]. Fig. 1 shows the essential four main criteria of TAM theoretically

All the factors and determinants are clustered into their respective criteria. This is to avoid the cross-influence by PU and PEoU. Social Influences described as representing the importance of people believe in the benefit of system usage. While System Characteristics illustrated by the cognitive instrumental process which people believe in positive advantages acquired upon technology usage. Individual Differences heightened the general belief of individual towards computer and computer usage. The last criteria, of Facilitating Condition represent the perception of external control determinants related to the availability of support and resources of an organisation while facilitating usage of technology. Table I illustrate the cluster of respected factors and determinants.

### *B. Technology Readiness Index 2 (TRI 2)*

Technology readiness can be defined as the eagerness of people to accept and adopt the changes in technology which indirectly will incorporate the technology in their work and life [38]. Meanwhile, the Technology Readiness Index (TRI) is a model in measuring people's tendency to embrace new modern technologies [39]**.** Prior studies have shown the excellent result of this model in finding people's tendency to embracing new technology, especially in an organisation. There are four main dimensions of the model including;

*1) Optimism:* Optimism refers to a positive approach by people towards the use of new or changes in technology [40]. This indirectly plays as a positive factor in the TRI model.

*2) Discomfort:* Opposite to optimism, discomfort refers to the negative response of people to any changes upon technology. To emphasise, most people find it is uncomfortable to handle new technology or any changes been made upon the technology, as they find the changes are complicated to keep up. Thus, this plays as a negative factor in the TRI model.

*3) Insecurity:* Insecurity refers to sceptical behaviour, where people lose trust or do not have any trust in technology [41]. To emphasise, most companies reluctant to implement new technologies as they felt insecure regarding the cost of implementing, plus the future direction of the technology remains uncertain [42].

*4) Innovativeness:* Innovativeness illustrates the level of innovations that are being embraced by people and organisation towards upon the development of cutting-edge technology [40]. This construct also represents the positive construct in the TRI model.

According to [43], optimism and innovativeness are the two positives construct, while discomfort and insecurity are clustered as the negative construct in the TRI model. Consistent with [43], these positive and negative factors enable researchers to investigate the necessity of implementing new technology upon people's behaviour towards the usage of technology. Positive factors will posit the result of people's attraction to new technology. While negative factor's result will postulate that there might be hinder or delay in the overall acceptance to the company or individual. Most of the organisation instigated the TRI model upon the implementation of new technology in their organisation. This is due to the criteria of the TRI model that established based on the psychological assessment of individual or organisation either they will accept or reject the technology that will be used.

The original establishment of TRI model consists of 36-items and divided into four dimensions for each factor, which is (i) optimism [10-items], (ii) innovativeness [7-items], (iii) discomfort [10-items], and (iv) insecurity [9-items] [44]. However, studies show that TRI has a setback result due to the pace of technology advancement [38], [41]. Therefore, TRI 2 is established due to the prior challenge on the first TRI model [43]. Based on the literature, there is evidence that TRI 2 is more robust and have concise result compared to TRI. Compared to 36-items of TRI, TRI 2 only have 6-items with 4-items on each factor. Therefore, TRI 2 is applicable to be implemented in a survey that measures multiple variables aside from the TRI model. Hence, this study adopted the TRI 2.0 model due to the conciseness and robustness, which can be used across time and technology [43], thus making it suitable to be implemented in blockchain acceptance study. Previously, TRI has been suggested to be integrated with TAM, as the TRI factors can be acted as the positive and negative factor that affects PU and PEoU of TAM [11], [45] [46].

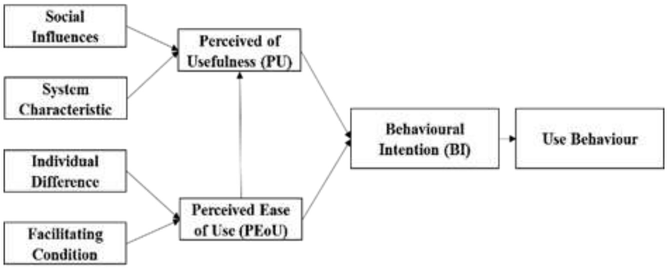

Fig. 1. TAM Theoretically Main Criteria.

TABLE I. THE CLUSTER OF RESPECTED FACTORS AND DETERMINANTS

| **Variables** | **Factors** | **Determinants** |
|---|---|---|
| Social Influences | Subjective Norm | PU |
| System Characteristic | Image | |
| Individual Differences | Job Relevance, Output Quality, Result Demonstrability | PEoU |
| Facilitating Conditions | Computer Self-Efficacy, Computer Anxiety, Computer Playfulness | |

Additionally, the studies by [46]–[48] shows that TRI construct does significantly related to behavioural acceptance of the individual. Consequently, this study opted to integrate constructs from TAM 3 and TRI 2 in the proposed model of Blockchain-Based Data-sharing Acceptance Model as elaborated in the next section of this paper.

### C. Previous Acceptance Study on Blockchain Technology and Cryptocurrency

Technology Acceptance Model had been utilized to study the acceptance and adoption of many kinds of technology, including in the realm of cryptocurrency for individual and target group. Thus, this research considers this model as a suitable model to determine the acceptance and adoption of blockchain. In [49], the authors adopted the Unified Theory of Acceptance and Use of Technology (UTAUT) to investigate elements that are possibly influencing Malaysian banking institutions behavioural intention to adopt blockchain technology. Meanwhile, in [50], the authors proposed a research model which integrates the particular dimension of cryptocurrency into UTAUT and UTAUT2. The integration enables the group to study the factors that influence the acceptance of cryptocurrency in Malaysian individuals' context. The study involved a pilot study of 36 respondent and analysis conducted using PLS-SEM analyses.

In [51], to measure target group intention to use research data sharing system that applied the blockchain-based technologies, researchers had developed a prototype by applying the extended TAM-based model. The authors found that this study gave a basic understanding of the acceptance level on the blockchain-based data sharing; however, no empirical data available to support the finding.

Furthermore, researchers also used TAM to measure blockchain and cryptocurrency acceptance and adoption in [51]–[55]. However, most studies only include few constructs from whether TAM or TRI to study blockchain acceptance; meanwhile, other significant constructs are neglected. The use of incomplete construct might affect the balance of the constructs and scale of TRI compared to the original version of TRI [43], [44]. Hence, this study proposes to integrate TAM3 and TRI2.0, as suggested in the previous study [46], [56].

## V. Proposed Model on Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community

### A. Conceptual Model

Integration of two paradigms between TAM 3 and TRI 2 is considered an established integration model that could deliver the excellent result in previous research. Selected constructs from TAM 3 are Job Relevance for System Characteristics, Computer Self-Efficacy and Computer Anxiety for Individual Difference Factor, Perception of External Controls for Facilitating Condition Factor as shown in Table II.

This selection is made upon the conformity of the target audience, which is the intelligence community.

Bala [35] illustrated that Job Relevance needs to be selected as it is crucial to investigate either people can trust the usage of technology and their belief if the technology improves their life and work. As an example, intelligence community personnel believe that blockchain technology can improve the workflow of information sharing in the intelligence community. The author also highlights the significance of Computer Self-efficacy, Computer Anxiety and Perception of External Control. Computer Self-efficacy enables investigation upon the effect of competency of intelligence personnel upon the acceptance and readiness of blockchain technology implementation.

In comparison, Computer Anxiety examines how intelligence personnel feels upon on the blockchain usage, which will indirectly affect their acceptance of blockchain technology, the PEoU. Perception of External Control will study regarding the available resource and support that can be provided to the intelligence community upon the implementation of blockchain implementation. On the other hand, this study selected all construct from TRI 2, as suggested by [11]. The conceptual model were adapted from previous study by [46], [56] which successfully validated the acceptance of data mining among public university student in Malaysia as it is suitable to be implemented in this study.

Therefore, an overview of the proposed model with respective constructs from TAM 3 and TRI 2 is presented as in Fig. 2.

The established model can be used in investigating an individual's acceptance and readiness for the implementation of blockchain in the intelligence community. Based on the constructed model, a set of hypotheses is developed.

TABLE II. SELECTED CONSTRUCT

| Variables | Factors | Determinants |
|---|---|---|
| System Characteristic | Job Relevance | PU |
| Individual Difference | Computer Self-Efficacy,<br>Computer Anxiety | PEoU |
| Facilitating Conditions | Perception of External Control | |

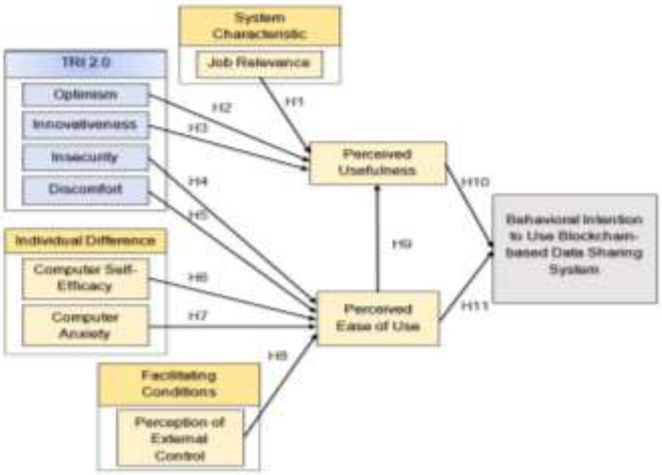

Fig. 2. Overview of the Proposed Conceptual Model with Respective Constructs from TAM 3 and TRI 2.

### B. Hypothesis Development

This study suggests the following hypothesis in exploring the influence of the variable to blockchain-based data sharing acceptance and readiness in the intelligence community. Hence, this study hypothesises that:

H1: Job relevance has a positive influence on the perceived usefulness of the blockchain-based data-sharing system.

H2: Optimism has a positive influence on the perceived usefulness of the blockchain-based data-sharing system.

H3: Innovativeness has a positive influence on the perceived usefulness of the blockchain-based data-sharing system.

H4: Insecurity has a negative influence on the perceived ease of use of the blockchain-based data-sharing system.

H5: Discomfort has a negative influence on the perceived ease of use of the blockchain-based data-sharing system.

H6: Computer self-efficacy has a positive influence on the perceived ease of use of the blockchain-based data-sharing system.

H7: Computer anxiety has a negative influence on the perceived ease of use of the blockchain-based data-sharing system.

H8: Perception of external control has a positive influence on the perceived ease of use of the blockchain-based data-sharing system.

H9: Perceived ease of use has a positive influence on the perceived usefulness of the blockchain-based data-sharing system.

H10: Perceived usefulness has a positive influence on the behavioural intention to use the blockchain-based data-sharing system.

H11: Perceived ease of use has a positive influence on the behavioural intention to use the blockchain-based data-sharing system.

## VI. Methodology

### A. Instrument Development

This study adopts a quantitative deductive approach of primary data collection using the survey questionnaire. The previous study by [35] [43] [46] and [56] was adapted and tailored accordingly to suit this study. The survey instrument that was developed consisted of 56 questions and divided by two sections include first section; Demographic Information, Authentication and Blockchain Knowledge, and second section; Technology Acceptance Model and Technology Readiness Index. Demographic information comprises the relevant information of the respondents including age, gender, level of education, work experience in the intelligence community, knowledge in authentication system and knowledge on the blockchain application. The questionnaire is measure by 7-points Likert scale in which (1) Strongly Disagree, (2) Quite Disagree, (3) Slightly Disagree, (4) Neutral, (5) Slightly Agree, (6) Quite Agree and (7) Strongly Agree. The questionnaire was validated through a pre-test conducted with 3 respondents from the intelligence community, 2 experts in the blockchain industry and 2 experts in academics to validate the accuracy of the items.

### B. Selection of Respondent

This pilot study applies purposive sampling among intelligence personnel from the intelligence community in Malaysia. For the sampling, we used purposive sampling that also referred to as judgement sampling. Participants were selected based on the qualities that the participant holds according to the pre-determined specific criteria [57]. Purposive sampling is commonly used in study using TAM as found in [49] [58] to meet specific criteria of the respondent that is vital in meeting the objectives of the study. Furthermore, the purposive sampling used in a under researched area such as in intelligence community mainly because of the closeness and confidentiality of intelligence practices which made the target population normally reluctant to participate and the sample was chosen exhibit must possess knowledge and experience in intelligence and information sharing, as well as awareness on latest intelligence structures and communication networks [59]. In this study, the sample must work in an intelligence organisation and experienced in the data-sharing system. Targeted respondent is selected and interviewed using a questionnaire where knowledge on authentication and blockchain application is surveyed in the earlier section of the questionnaire. About 35 survey questionnaires were distributed during the interview, and 30 data which meet the criteria were used in the analysis.

## VII. Result and Findings

### A. Demographic Profile

In total, 30 respondents of this study consist of 23 (76.67%) males and 7 (23.33%) are females. Age distribution of respondent with the majority of 21-30 years old with the sum of 18 (60.00%) respondents, followed by 31-40 years old with 8 respondents (26.67%), 41-50 years old 3 (10.00%) respondents and 51-60 years old 1 (3.33%) respondent. Majority of respondent qualified with bachelor’s degree level of education 19 (63.33%) followed by master’s degree and secondary school qualification of Sijil Pelajaran Malaysia with both 4 (13.33%) respondents, meanwhile for diploma 2 (6.67%) and Doctor of Philosophy (PhD) with 1 (3.33%) respondent. 9 (30%) respondents had 3-5 years working experience in the intelligence community, 7 (23.33%) respondents had less than 3 years working experience in the intelligence community, 7 (23.33%) respondents had 6 to 10 years working experience, meanwhile 4 (13.33%) respondents with more than 16 years’ experience and 3 (10%) respondents with 11-15 years’ experience respectively. To gauge respondent’s knowledge on the authentication system, result from related question shows 23 (76.67%) had knowledge in authentication meanwhile 7 (23.33%) possess no knowledge on authentication system. Data distribution of knowledge on blockchain application shows that 16 (53.33%) had knowledge of blockchain applications; meanwhile, 14 (46.67%) respondents had no knowledge of blockchain application. The indication of high percentage in knowledge about blockchain and authentication system provides credibility of the respondent in answering the questionnaire of this study. The overall demographic information of the respondent is shown in Table III.

### *B. Reliability and Validity Test*

To analyse the reliability and normality, partial least squares structural equation modelling (PLS-SEM) analysis was done by applying Smart PLS 3 software. Based on the model and reference from previous literature, this model is designed and evaluated using a reflective measurement model. The measurement model is assessed by evaluating Internal consistency that includes Cronbach's alpha and composite reliability, Convergent validity that includes indicator reliability and average variance extracted. Also, this research includes the discriminant validity as proposed by [60]. In ensuring the consistency of a measuring instrument, reliability and normality testing is required. Satisfactory level of validity and reliability is required before a significant relationship in the structural model is evaluated [61].

TABLE III. DEMOGRAPHIC INFORMATION (N = 30)

| **Demographic Criteria** | **Frequency** | **Percentage** |
|---|---|---|
| **Gender** | | |
| Male | 23 | 76.67 |
| Female | 7 | 23.33 |
| **Age** | | |
| 21-30 | 18 | 60.00 |
| 31-40 | 8 | 26.67 |
| 41-50 | 3 | 10.00 |
| 51-60 | 1 | 3.33 |
| **Level of education** | | |
| SPM | 4 | 13.33 |
| Diploma | 2 | 6.67 |
| Bachelor's degree | 19 | 63.33 |
| Master's Degree | 4 | 13.33 |
| PhD | 1 | 3.33 |
| **Work experience in intelligence community:** | | |
| < 3 years | 7 | 23.33 |
| 3 – 5 years | 9 | 30.00 |
| 6 – 10 years | 7 | 23.33 |
| 11 – 15 years | 3 | 10.00 |
| 16 years > | 4 | 13.33 |
| **Knowledge on Authentication System** | | |
| Yes | 23 | 76.67 |
| No | 7 | 23.33 |
| **Knowledge on Blockchain Applications** | | |
| Yes | 16 | 53.33 |
| No | 14 | 46.67 |

The assessment of the measurement model that was proposed in this research, Cronbach's Alpha for all construct are analysed. Previous studies recommended that the value for Cronbach's Alpha that greater than 0.7 [61] [60] determined as reliable. Table IV shows all Cronbach's Alpha values is above the acceptable level of 0.7, where the lowest value is Perceived Usefulness (0.722), and the highest value is Job Relevance (0.946). For indicator reliability in exploratory research, values between 0.60 and 0.70 are acceptable; meanwhile, reliability value between 0.70 and 0.95 considered satisfactory to good reliability levels [60]. Hence, 20 indicators with values below 0.6 are eliminated from the original 60 indicators in this study.

After insignificant indicators were eliminated for the model, the composite reliability is evaluated to determine internal consistency. for the composite reliability, the expected minimum level is above 0.70 [60]. As per Table IV, the value of the composite reliability ranged from 0.82 to 0.971. These values are above the recommended acceptable value above 0.70, demonstrating reliability. To assess the convergent validity, the AVE value is evaluated. Convergent validity refers to the theory that indicators for a specific construct are at least moderately correlated between the indicators of constructs [61]. As per Table IV, the AVE value recorded is above 0.5, demonstrate that all the AVE value is satisfactory and reflect that the constructs explain more than half of the indicator's variance [61]. Next, the assessment is done on the discriminant validity. Discriminant validity refers to the extent to which a particular construct varies from others [61]. In this study, as per Table V the discriminant validity is assessed by using the Heterotrait-Monotrait Ratio (HTMT). The author in [61] suggested that HTMT value below 0.8 indicates conceptually different construct. Table V indicates that all the HTMT value is below 0.8 indicates discriminant validity in this study.

TABLE IV. RELIABILITY AND NORMALITY TEST

| **Variable** | **Cronbach's Alpha** | **Composite Reliability** | **AVE** |
|---|---|---|---|
| Behavioural Intention to Use (BIU) | 0.836 | 0.871 | 0.631 |
| Computer Anxiety (CANX) | 0.941 | 0.971 | 0.944 |
| Computer Self-Efficacy (CSE) | 0.856 | 0.901 | 0.696 |
| Discomfort (DISC) | 0.807 | 0.851 | 0.538 |
| Innovativeness (INN) | 0.861 | 0.877 | 0.549 |
| Insecurity (INS) | 0.787 | 0.844 | 0.576 |
| Optimism (OPT) | 0.812 | 0.869 | 0.575 |
| Perception of External Control (PEC) | 0.756 | 0.820 | 0.540 |
| Perceived Ease of Use (PEoU) | 0.834 | 0.884 | 0.658 |
| Perceived Usefulness (PU) | 0.722 | 0.828 | 0.546 |
| Job relevance (REL) | 0.946 | 0.961 | 0.860 |

TABLE V. HETEROTRAIT-MONOTRAIT RATIO (HTMT)

| | BIU | CANX | CSE | DISC | INN | INS | OPT | PEC | PEoU | PU | REL |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **BIU** | | | | | | | | | | | |
| **CANX** | 0.094 | | | | | | | | | | |
| **CSE** | 0.299 | 0.275 | | | | | | | | | |
| **DISC** | 0.277 | 0.430 | 0.646 | | | | | | | | |
| **INN** | 0.364 | 0.467 | 0.668 | 0.475 | | | | | | | |
| **INS** | 0.384 | 0.450 | 0.318 | 0.796 | 0.587 | | | | | | |
| **OPT** | 0.164 | 0.195 | 0.212 | 0.312 | 0.378 | 0.249 | | | | | |
| **PEC** | 0.345 | 0.231 | 0.757 | 0.602 | 0.632 | 0.406 | 0.354 | | | | |
| **PEoU** | 0.237 | 0.138 | 0.297 | 0.291 | 0.307 | 0.371 | 0.215 | 0.401 | | | |
| **PU** | 0.300 | 0.270 | 0.253 | 0.353 | 0.288 | 0.269 | 0.788 | 0.288 | 0.255 | | |
| **REL** | 0.139 | 0.346 | 0.137 | 0.264 | 0.276 | 0.291 | 0.244 | 0.335 | 0.104 | 0.714 | |

### C. Structural Model Analysis

Bootstrapping procedure is used in this study to evaluate the significance level of the partial least square estimation [62]. As recommended in reference [60], this study use bootstrapping procedure using 5000 subsamples. Fig. 3 and Table VI shows the values of the path coefficients and R-squared of the structural model.

As per our finding that shown in the structural model result in Fig. 3 and Table VI, consistent with H1, job relevance has a positive influence on the perceived usefulness of blockchain-based data-sharing system with a path coefficient of 0.453. As hypothesised in H2, optimism has a positive influence on the perceived usefulness of blockchain-based data-sharing system with a path coefficient of 0.561. As in H3, the hypothesis is not significant as innovativeness has a negative influence on the perceived usefulness of blockchain-based data-sharing system with a path coefficient of -0.238. For H4, the hypothesis is significant as insecurity has a negative influence on the perceived ease of use of the blockchain-based data-sharing system with a path coefficient value of -0.428.

As in H5, the hypothesis is not significant as the discomfort has a positive influence on the perceived ease of use of the blockchain-based data-sharing system with a path coefficient of 0.018. As hypothesised in H9, perceived ease of use has a positive influence on the perceived usefulness of blockchain-based data-sharing system with a path coefficient of 0.051. The rest of hypothesis is not significant as the result shows a contrast value compared to an early hypothesis in H6, computer self-efficacy has a negative influence on the perceived ease of use of the blockchain-based data-sharing system with a path coefficient of -0.162, in H7, computer anxiety has a positive influence on the perceived ease of use of the blockchain-based data-sharing system with a path coefficient of 0.295. In H8, perception of external control has a negative influence on the perceived ease of use of the blockchain-based data-sharing system with a path coefficient of -0.165, in H10, perceived usefulness has a negative influence on the behavioural intention to use blockchain-based data sharing system with a path coefficient of -0.193 and in H11, perceived ease of use has a negative influence on the behavioural intention to use blockchain-based data sharing system with a path coefficient of -0.011.In order to support the hypothesized paths, as per reference [60], the t values need to be significant at 1.65 (significance level = 0.05), or 2.33 (significance level = 0.01). Based on the result, H1, H2, and H4 are supported meanwhile H3, H5, H6, H7, H8, H9, H10 and H11 are not supported.

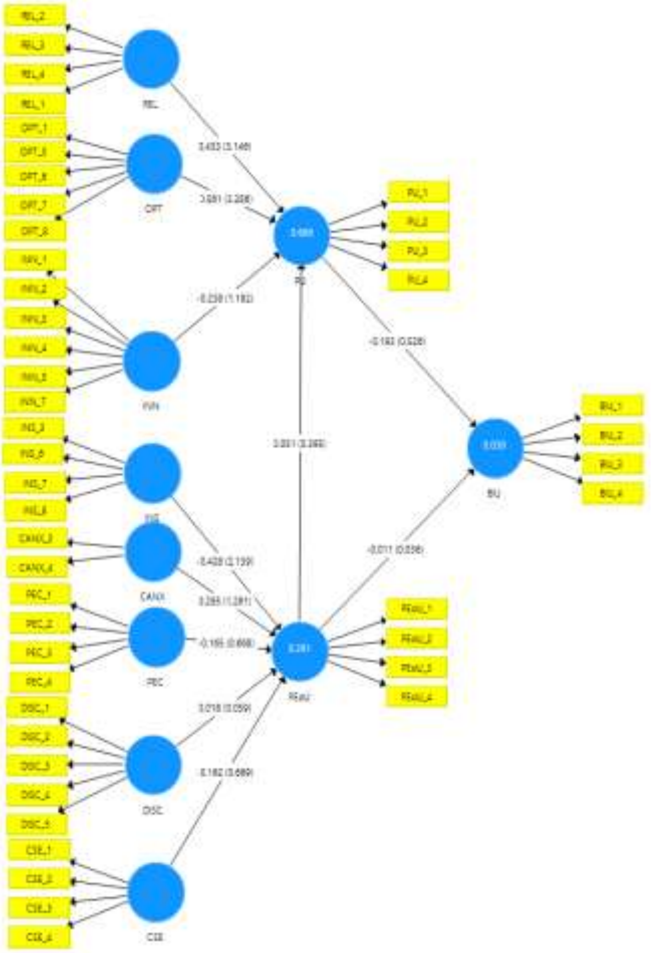

Fig. 3. Structural Model Results.

TABLE VI. RESULT OF STRUCTURAL MODEL TESTING

| | Path | Path coefficient | *p*-value | *t*-value | Findings |
|---|---|---|---|---|---|
| H1 | REL → PU | 0.453 | 0.000* | 3.355 | Supported |
| H2 | OPT → PU | 0.561 | 0.000* | 3.392 | Supported |
| H3 | INN → PU | -0.238 | 0.096 | 1.305 | Not supported |
| H4 | INS → PEoU | -0.428 | 0.028* | 1.917 | Supported |
| H5 | DISC → PEoU | 0.018 | 0.477 | 0.057 | Not supported |
| H6 | CSE → PEoU | -0.162 | 0.257 | 0.654 | Not supported |
| H7 | CANX → PEoU | 0.295 | 0.110 | 1.225 | Not supported |
| H8 | PEC → PEoU | -0.165 | 0.263 | 0.636 | Not supported |
| H9 | PEoU → PU | 0.051 | 0.351 | 0.382 | Not supported |
| H10 | PU → BIU | -0.193 | 0.305 | 0.509 | Not supported |
| H11 | PEoU → BIU | -0.011 | 0.486 | 0.036 | Not supported |

*Significant at the 0.05 Level.

Next, the determination of coefficient or $R^2$ value is carried out. The $R^2$ value shows the amount of variance in endogenous constructs which the exogenous constructs may describe [63]. The $R^2$ ranges are from 0 to 1, with higher levels show higher predictive accuracy [60]. In [64], the authors stated $\mathrm{R}^2$ values for endogenous latent variables in the structural model of 0.75 is substantial, 0.50 as moderate and or 0.25 as weak. Fig. 3 shows that the accuracy of the endogenous constructs PU predicted at (68.6 %) and PEOU at (29.1 %), which meant their associated independent variables could explain both dependent variables. The $R^2$ for BIU is at (3.8 %) indicating weak predictive accuracy.

## VIII.DISCUSSION

This study proposed a conceptual model of acceptance and readiness on the blockchain-based data-sharing system for the intelligence community based on constructs in Technology Acceptance Model 3 (TAM 3) and Technology Readiness Level 2 (TRI 2). We achieved our objective of this study to integrate constructs from TAM 3 and TRI 2 in the proposed model of Blockchain-Based Data-sharing Acceptance Model to explore behavioural intention to use the blockchain-based data-sharing system.

This study validates the reliability and validity of the proposed acceptance model using a pilot study conducted among the respondents. Prior to that, a pre-test was conducted to validate the questionnaire survey used in this study with validation from representatives from the respondent group and subject matter expert feedback. From the initial 60 indicators, 20 indicators were removed from the pilot questionnaire due to unsatisfactory level of below 0.6, resulting in the remaining 40 indicators used in further analysis. The reliability and validity of the model are satisfactory and suitable based on the Cronbach's Alpha, Composite Reliability, and Average Variance Extracted (AVE) and discriminant validity based on heterotrait-monotrait ratio (HTMT).

However, the analysis of structural model testing is limited due to the small sample size used in this pilot study. This limitation is similar to other study using a small sample size in investigating acceptance and intention to use blockchain and cryptocurrency as in [50], [51]. According to [60], by using the rule of thumb, the minimum sample size must be 10 times the maximum number of arrowheads in the model. In this model, PEoU has the maximum number of arrowheads pointing to the variable with 5 arrowheads. Hence, at least 45 observations are needed to achieve a statistical power of 80% for at least 0.25 $\mathrm{R}^2$ values detected with a 5% probability of error [60]. In this study, three hypotheses are supported including on job relevance has a positive influence on the perceived usefulness of the blockchain-based data-sharing system, optimism has a positive influence on the perceived usefulness of blockchain-based data-sharing system and insecurity has a negative influence on the perceived ease of use of the blockchain-based data-sharing system.

## IX. CONCLUSION AND FUTURE WORK

This paper elaborated and discussed regarding blockchain technology acceptance in intelligence community using the case of the proposed blockchain-based data-sharing system in the intelligence community. As known, the intelligence community relies on accurate and precise information for country security purposes. Thus, blockchain technology is proposed to be integrated into the intelligence community data sharing system due to its capability in managing access control and authentication automatically. Blockchain is also proven to be a brilliant solution in ensuring data integrity that is vital for the intelligence community-related data. However, since that blockchain technology is still new, the readiness and acceptance level of the intelligence community upon blockchain technology implementation is yet to be discovered. Thus, this paper survey about blockchain technology and proposes a pilot study by integrating a reliable model in investigating the intelligence community readiness and acceptance upon blockchain technology usage. The model is established based on constructs from TAM 3 and TRI 2. The establishment of the integrated model derived by the effectiveness that was proven by other researchers in their previous work that we obtained from literature reviews. This study is an ongoing work of implementing TAM 3 and TRI 2 for blockchain technology readiness and acceptance in the intelligence community of Malaysia.

This study concludes that the acceptance model can be used in investigating behavioural intention to use the blockchain-based data-sharing system in the intelligence community. The awareness and knowledge in blockchain technology among the respondent shall be enriched via training and education to increase the level of acceptance and readiness of such technology. Future work may include full-scale survey based on the recommended sample size and involvement of different agencies from the intelligence community context. This will provide reliable data that could serve as a source of reference for the development of government policy for blockchain implementation, especially in the intelligence community environment.

## ACKNOWLEDGMENTS

This research is fully supported by National Defence University of Malaysia (UPNM) under Short Grant UPNM/2020/GPJP/ICT/6 and Center of Research and Innovation Management. The authors fully acknowledged the Malaysia Ministry of Higher Education (MOHE) and UPNM for the approved fund, which makes this important research viable and effective.

## REFERENCES

[1] W. N. Wan Muhamad et al., “Enhance multi-factor authentication model for intelligence community access to critical surveillance data,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, vol. 11870 LNCS, pp. 560–569, doi: 10.1007/978-3-030-34032-2_49.

[2] J. Schmid, “Technology and the Intelligence Community,” in Advanced Sciences and Technologies for Security Applications, 2018, pp. 39–53.

[3] W. J. Lahneman, “Knowledge-sharing in the intelligence community after 9/11,” Int. J. Intell. CounterIntelligence, vol. 17, no. 4, pp. 614–633, 2004, doi: 10.1080/08850600490496425.

[4] S. N. Q. S. Mohamed and M. Yaacob, “Understanding the Intelligence Failure and Information Sharing in Handling Terrorism among Intelligence Community,” Int. J. Acad. Res. Bus. Soc. Sci., vol. 9, no. 9, pp. 1201–1213, 2019, doi: 10.6007/ijarbss/v9-i9/6414.

[5] J. W. Crampton, “Collect it all: national security, Big Data and governance,” GeoJournal, vol. 80, no. 4, pp. 519–531, 2015, doi: 10.1007/s10708-014-9598-y.

[6] S. S. De Matas and B. P. Keegan, “An exploration of research information security data affecting organizational compliance,” Data Br., vol. 21, pp. 1864–1871, 2018, doi: 10.1016/j.dib.2018.11.002.

[7] C. Lin, D. He, X. Huang, K. R. Choo, and A. V Vasilakos, “BSeIn : A blockchain-based secure mutual authentication with fi ne-grained access control system for industry 4 . 0 ☆,” J. Netw. Comput. Appl., vol. 116, no. March, pp. 42–52, 2018, doi: 10.1016/j.jnca.2018.05.005.

[8] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, “Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things,” J. Cyber Secur. Mobil., vol. 1, pp. 309–348, 2013.

[9] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “FairAccess : a new Blockchain-based access control framework for the Internet of Things,” no. February, pp. 5943–5964, 2017, doi: 10.1002/sec.1748.

[10] X. Xu et al., “A Taxonomy of Blockchain-Based Systems for Architecture Design,” 2017 IEEE Int. Conf. Softw. Archit., pp. 243–252, 2017, doi: 10.1109/ICSA.2017.33.

[11] N. Larasati, “Technology Readiness and Technology Acceptance Model in New Technology Implementation Process in Low Technology SMEs,” Int. J. Innov. Manag. Technol., vol. 8, no. 2, pp. 113–117, 2017, doi: 10.18178/ijimt.2017.8.2.713.

[12] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” IEEE Internet Things J., vol. 5, no. 2, pp. 1184–1195, 2018, doi: 10.1109/JIOT.2018.2812239.

[13] T. Tuan, A. Dinh, R. Liu, M. Zhang, and G. Chen, “Untangling Blockchain : A Data Processing View of Blockchain Systems,” IEEE Trans. Knowl. Data Eng., vol. 30, no. 7, pp. 1366–1385, 2018, doi: 10.1109/TKDE.2017.2781227.

[14] C. Tankard, “Big data security,” Netw. Secur., vol. 2012, no. 7, pp. 5–8, 2012, doi: 10.1016/S1353-4858(12)70063-6.

[15] N. Kshetri, “Big data׳s impact on privacy, security and consumer welfare,” Telecomm. Policy, vol. 38, no. 11, pp. 1134–1145, Dec. 2014, doi: 10.1016/j.telpol.2014.10.002.

[16] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “Blockchain-based database to ensure data integrity in cloud computing environments,” in CEUR Workshop Proceedings, 2017, vol. 1816, pp. 146–155.

[17] O. Alphand et al., “IoTChain : A Blockchain Security Architecture for the Internet of Things,” 2018 IEEE Wirel. Commun. Netw. Conf., pp. 1–6, 2018.

[18] W. Zhang et al., “Blockchain-Based Distributed Compliance in Multinational Corporations’ Cross-Border Intercompany Transactions,” in Future of Information and Communication Conference (FICC), 2019, no. July, pp. 304–320, doi: 10.1007/978-3-030-03405-4_20.

[19] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, “Blockchain – The Gateway to Trust-free Cyrptographic Transactions,” Twenty-Fourth Eur. Conf. Inf. Syst. (ECIS), İstanbul,Turkey, vol. 6, no. May, pp. 4013–4027, 2016.

[20] J. P. Es-Samaali, H., Outchakoucht, A., & Leroy, “A Blockchain-based Access Control for Big Data,” J. Comput. Networks Commun. Secur. Internet Things J., vol. 5, no. 7, p. 137, 2017, doi: 10.1109/JIOT.2018.2812239.

[21] M. Milutinovic, W. He, H. Wu, and M. Kanwal, “Proof of Luck: An efficient blockchain consensus protocol,” in SysTEX 2016 - 1st Workshop on System Software for Trusted Execution, colocated with ACM/IFIP/USENIX Middleware 2016, 2016, pp. 2–7, doi: 10.1145/3007788.3007790.

[22] . Karamitsos, M. Papadaki, and N. B. Al Barghuthi, “Design of the Blockchain Smart Contract: A Use Case for Real Estate,” J. Inf. Secur., vol. 09, no. 03, pp. 177–190, 2018, doi: 10.4236/jis.2018.93013.

[23] X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, and A. V. Vasilakos, “Designing blockchain-based applications a case study for imported product traceability,” Futur. Gener. Comput. Syst., vol. 92, pp. 399–406, 2019, doi: 10.1016/j.future.2018.10.010.

[24] P. Novotny et al., “Permissioned blockchain technologies for academic publishing,” Inf. Serv. Use, vol. 38, no. 3, pp. 159–171, 2018, doi: 10.3233/ISU-180020.

[25] X. Cheng and F. Chen, “Design of a Secure Medical Data Sharing Scheme Based on Blockchain,” J. Med. Syst., vol. 44, no. 2, pp. 1–11, 2020.

[26] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare Data Gateways : Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control,” J. Med. Syst., 2016, doi: 10.1007/s10916-016-0574-6.

[27] C. Service and P. Via, “MeDShare : Trust-less Medical Data Sharing Among,” IEEE Access, vol. 5, pp. 1–10, 2017, doi: 10.1109/ACCESS.2017.2730843.

[28] R. Xu, Y. Chen, E. Blasch, and G. Chen, “BlendCAC : A BLockchain-ENabled Decentralized Capability-based Access Control for IoTs,” 2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, pp. 1027–1034, 2018, doi: 10.1109/Cybermatics.

[29] K. Naerland, C. Müller-Bloch, R. Beck, and S. Palmund, “Bill of Lading on Blockchain Blockchain to Rule the Waves - Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized Environments,” Proc. Int. Conf. Inf. Syst., pp. 1–16, 2017.

[30] A. Tarhini, N. A. G. Arachchilage, R. Masa’deh, and M. S. Abbasi, “A Critical Review of Theories and Models of Technology Adoption and Acceptance in Information System Research,” Int. J. Technol. Diffus., vol. 6, no. 4, pp. 58–77, 2015, doi: 10.4018/ijtd.2015100104.

[31] C. E. Porter and N. Donthu, “Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics,” J. Bus. Res., vol. 59, no. 9, pp. 999–1007, 2006, doi: 10.1016/j.jbusres.2006.06.003.

[32] A. Indrati et al., “Validity of the technology acceptance model (tam): a sensemaking perspective,” Ijms, vol. 6, no. 1, pp. 99–120, 2012, doi: 10.5897/AJBM10.1398.

[33] Q. L. Chen and Z. H. Zhou, “Unusual formations of superoxo heptaoxomolybdates from peroxo molybdates,” Inorg. Chem. Commun., vol. 67, no. 3, pp. 95–98, 2016, doi: 10.1016/j.inoche.2016.03.015.

[34] V. Venkatesh and F. D. Davis, “Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies,” Manage. Sci., vol. 46, no. 2, pp. 186–204, 2000, doi: 10.1287/mnsc.46.2.186.11926.

[35] V. Venkatesh and H. Bala, “Technology Acceptance Model 3 and a Research Agenda on Interventions,” Decis. Sci., vol. 39, no. 2, pp. 273–315, 2008.

[36] D. J. McFarland and D. Hamilton, “Adding contextual specificity to the technology acceptance model,” Comput. Human Behav., vol. 22, no. 3, pp. 427–447, May 2006, doi: 10.1016/j.chb.2004.09.009.

[37] P. Lai, “The Literature Review Of Technology Adoption Models And Theories For The Novelty Technology,” J. Inf. Syst. Technol. Manag., vol. 14, no. 1, pp. 21–38, Apr. 2017, doi: 10.4301/S1807-17752017000100002.

[38] K. M. Kuo, C. F. Liu, and C. C. Ma, “An investigation of the effect of nurses’ technology readiness on the acceptance of mobile electronic medical record systems,” BMC Med. Inform. Decis. Mak., vol. 13, no. 1, pp. 1–14, 2013, doi: 10.1186/1472-6947-13-88.

[39] A. Caison, D. Bulman, S. Pai, and D. Neville, “Exploring the technology readiness of nursing and medical students at a Canadian University,” J. Interprof. Care, vol. 22, no. 3, pp. 283–294, 2008, doi: 10.1080/13561820802061809.

[40] A. Parasuraman and Charles L. Colby, Techno-Ready Marketing: How and Why Your Customers Adopt Technology. NY, USA: The Free Press New York, 2007.

[41] J. S. C. Lin and P. L. Hsieh, “Refinement of the technology readiness index scale: A replication and cross-validation in the self-service technology context,” J. Serv. Manag., vol. 23, no. 1, pp. 34–53, 2012, doi: 10.1108/09564231211208961.

[42] S. Shin and W. J. Lee, “The effects of technology readiness and technology acceptance on NFC mobile payment services in Korea,” J. Appl. Bus. Res., vol. 30, no. 6, pp. 1615–1626, 2014.

[43] A. Parasuraman and C. L. Colby, “An Updated and Streamlined Technology Readiness Index: TRI 2.0,” J. Serv. Res., vol. 18, no. 1, pp. 59–74, 2015, doi: 10.1177/1094670514539730.

[44] A. Parasuraman, “Technology Readiness Index (TRI): A Multipleitem Scale To Measure Readiness To Embrace New Technologies,” J. Serv. Res., vol. 2:307, no. May, 2000.

[45] C.-H. Lin, H.-Y. Shih, and P. J. Sher, “Integrating technology readiness into technology acceptance: The TRAM model,” Psychol. Mark., vol. 24, no. 7, pp. 641–657, Jul. 2007, doi: 10.1002/mar.20177.

[46] M. Wook, Z. M. Yusof, and M. Zakree Ahmad Nazri, “The Acceptance of Educational Data Mining Technology among Students in Public Institutions of Higher Learning in Malaysia,” Int. J. Futur. Comput. Commun., vol. 4, no. 2, pp. 112–117, 2015, doi: 10.7763/ijfcc.2015.v4.367.

[47] J. S. C. Lin and H. C. Chang, “The role of technology readiness in self-service technology acceptance,” Manag. Serv. Qual., vol. 21, no. 4, pp. 424–444, 2011, doi: 10.1108/09604521111146289.

[48] Y. Yi, L. L. Tung, and Z. Wu, “Incorporating Technology Readiness ( TR ) Into TAM : Are Individual Traits Important to Understand Technology Acceptance ?,” Digit 2003 Proc., pp. 1–27, 2003.

[49] H. Yusof et al., “Behavioral Intention to Adopt Blockchain Technology: Viewpoint of the Banking Institutions in Malaysia,” Int. J. Adv. Sci. Res. Manag., vol. 3, no. 10, pp. 1–6, 2018, [Online]. Available: www.ijasrm.com.

[50] Y. C. Yeong, K. S. Kalid, and S. K. Sugathan, “Cryptocurrency acceptance: A case of Malaysia,” Int. J. Eng. Adv. Technol., vol. 8, no. 5, pp. 28–38, 2019, doi: 10.35940/ijeat.E1004.0585C19.

[51] A. K. Shrestha and J. Vassileva, “User acceptance of usable blockchain-based research data sharing system: An extended TAM-based study,” Proc. - 1st IEEE Int. Conf. Trust. Priv. Secur. Intell. Syst. Appl. TPS-ISA 2019, pp. 203–208, 2019, doi: 10.1109/TPS-ISA48467.2019.00033.

[52] L. Wanitcharakkhakul and S. Rotchanakitumnuai, “Blockchain technology acceptance in electronic medical record system,” Proc. Int. Conf. Electron. Bus., vol. 2017-Decem, pp. 53–58, 2017.

[53] C. C. Lee, J. C. Kriscenski, and H. S. Lim, “An Empirical Study Of Behavioral Intention To Use Blockchain Technology.: Sistema de descoberta para FCCN,” J. Int. Bus. Discip., vol. 14, no. 1, pp. 1–21, 2019, [Online]. Available: https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=4&sid=c4c41200-8ffa-4706-9562-33088ffd69aa%40pdc-v-sessmgr02.

[54] S. Supranee, S. Rotchanakitumnuai, and R. Siriluck, “The Acceptance of the Application of Blockchain Technology in the Supply Chain Process of the Thai Automotive Industry,” 2017, [Online]. Available: http://aisel.aisnet.org/iceb2017http://aisel.aisnet.org/iceb2017/30.

[55] I. Roussou, E. Stiakakis, and A. Sifaleras, “An empirical study on the commercial adoption of digital currencies,” Inf. Syst. E-bus. Manag., vol. 17, no. 2–4, pp. 223–259, 2019, doi: 10.1007/s10257-019-00426-7.

[56] M. Wook, S. Ismail, N. M. M. Yusop, S. R. Ahmad, and A. Ahmad, “Identifying priority antecedents of educational data mining acceptance using importance-performance matrix analysis,” Educ. Inf. Technol., vol. 24, no. 2, pp. 1741–1752, 2019, doi: 10.1007/s10639-018-09853-4.

[57] I. Etikan, “Comparison of Convenience Sampling and Purposive Sampling,” Am. J. Theor. Appl. Stat., vol. 5, no. 1, p. 1, 2016, doi: 10.11648/j.ajtas.20160501.11.

[58] Y. Malhotra and D. F. Galletta, “Extending the Technology Acceptance Model to account for social influence: Theoretical bases and empirical validation,” Proc. Hawaii Int. Conf. Syst. Sci., vol. 00, no. c, p. 5, 1999, doi: 10.1109/hicss.1999.772658.

[59] J. Carter, “Inter-organizational relationships and law enforcement information sharing,” no. May, 2015, doi: 10.1080/0735648X.2014.927786.

[60] Hair, G. T. Hult, C. Ringle, and M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) - Joseph F. Hair, Jr., G. Tomas M. Hult, Christian Ringle, Marko Sarstedt. Los Angeles: SAGE Publications, Inc. Printed, 2017.

[61] A. Leguina, “A primer on partial least squares structural equation modeling (PLS-SEM),” Int. J. Res. Method Educ., vol. 38, no. 2, pp. 220–221, 2015, doi: 10.1080/1743727x.2015.1005806.

[62] W. W. Chin, Handbook of Partial Least Squares. 2010.

[63] M. Sarstedt, C. M. Ringle, and J. F. Hair, Handbook of Market Research, no. September. 2017.

[64] J. F. Hair, C. M. Ringle, and M. Sarstedt, “PLS-SEM: Indeed a silver bullet,” J. Mark. Theory Pract., vol. 19, no. 2, pp. 139–152, 2011, doi: 10.2753/MTP1069-6679190202.