# **An Assessment Framework for Identification of Enterprise-Blockchain Acceptability Challenges**

**SHEIKH MAHMUDUL HASAN SHIUMa,1, MD. MAHABUB ISLAMa,2, S.A. SAHARUKHa,3, ANAMUL HOQUE RAFIa,4 , MD. MEHEDI HASSAN ONIK\***

**a American International University-Bangladesh, Department of Computer Science, 408/1 Kuratoli, Khelkhet, Dhaka, 1209, Bangladesh.**

**Author List**

**1 Shium, Sheikh Mahmudul Hasan**

**Email:** [**19-40764-2@student.aiub.edu**](mailto:19-40764-2@student.aiub.edu)

**ORCID: 0009-0002-1301-6493** [**https://sheikhmahmudulhasanshium.github.io/**](https://sheikhmahmudulhasanshium.github.io/)

**2 Islam, Md. Mahabub**

**Email:** [**19-40826-2 @student.aiub.edu**](mailto:19-40764-2@student.aiub.edu)

**ORCID: 0009-0005-8544-4739** [**https://progmahabub21.github.io/My-Website/**](https://progmahabub21.github.io/My-Website/)

**3 Saharukh, S.A.**

**Email:** [**19-40819-2@student.aiub.edu**](mailto:19-40819-2@student.aiub.edu)

**4 Rafi, Anamul Hoque**

**Email:**[**19-40780-2@student.aiub.edu**](mailto:19-40780-2@student.aiub.edu)

**\*Corresponding-Author**

**Onik, Md. Mehedi Hassan**

**Email:** [**m.onik@deakin.edu.au**](mailto:m.onik@deakin.edu.au)

# Graphical Abstract:

**A diagram of a process flow

Description automatically generated**

# **Highlights:**

* Developed a novel framework to assess any blockchain-based product for enterprise adoption.
* Analyzed and redefined multiple trust factors from previous popular assessment frameworks to enhance understanding.
* Identified key obstacles hindering the adoption of blockchain-based products in enterprises.
* Offered valuable insights for policymakers, practitioners, and researchers in the blockchain ecosystem.

# **An Assessment Framework for Identification of Enterprise-Blockchain Acceptability Challenges**

# **ARTICLE INFO**

## **Keywords**

blockchain technology

evaluation method

protection motivation theory

technology acceptance model

unified framework

enterprise acceptability

## **ABSTRACT**

Blockchain, a revolutionary technology, has the potential to transform various sectors such as finance, logistics, management, e-voting, gaming, and healthcare. It achieves this by functioning as a decentralized digital ledger, securely and transparently recording transactions. However, despite being around for almost two decades, it has not gained widespread recognition as an alternative to current technology in the industry. To unlock its full potential, we need to identify and address any existing flaws. Currently, there is a lack of a clear and consistent framework to assess the risks of blockchain. The main objective of this research is to develop a standardized tool that can pinpoint problem areas and promote greater adoption of blockchain. The research proposes a unified assessment model based on motivation and acceptance theories. This model will provide numerical ratings to evaluate blockchain products and offer guidance on areas for improvement, ultimately increasing global acceptance.

# **Introduction**

Blockchain is a revolutionary modern architecture concept for any system that can be built and maintained globally. It protects the public and users’ most valuable information by making it immutable. Besides, blockchain eliminates the need for a trusted third party or governing body to be involved in business transactions or the provision of services due to its decentralized nature. However, blockchain has not yet attained its desired acceptance rate since it has not yet won over enough skeptics among its intended audiences, including both users and software developers. By combining protection motivation theory and technology adoption model theory, this study proposes and investigates a significant unified model for determining the trust index of adopting blockchain technology at industrial levels. “Blockchain technology (BCT)” is defined as a collection of records saved in publicly distributed ledgers that are linked as a chain, are very resistant to alteration of the original saved records, and are strongly protected by complex algorithms ([Vafadarnikjoo, Ahmadi, Liou, Botelho, and Chalvatzis (2021)](#Vafadarnikjoo2021)). Blockchain has three important characteristics: 1. distributed ledger technology (PLD); 2. in blockchain technology, the chain of blocks containing data is kept on nodes, which function as storage units; 3. smart contracts that contain logical instructions to execute [Pilkington (2016)](#Pilkington2016). While transacting at a regular bank, the bank serves as the trusted third party, which results in the user having to pay extra charges. The full-access user of blockchain can deposit and withdraw $200,000/day and unlimited monthly limits of cryptocurrency; deposit and withdraw $100,000/day or $500,000/month of flat currency, e.g., dollars, euros, and GBP, by using blockchain, which is a very large volume of transactions without kind of extra service charges ([Blockchain.com (2022)](#Blockchain2022); [Bitcoin.org (2022)](#Nakamoto2009)). Banks faced difficulties accessing the server during various events like festivals, wars, and disasters due to the centralized system. Blockchain, being decentralized and sharing a peer-to-peer network, ensures secure and unbroken service to blockchain users, preventing security breaches and overloading.

In 2004, Dr. Hal Finney introduced a system called Reusable Proof of Work (RPoW), which was able to authenticate faultlessness in real time by registering and holding the ownership of a token on a reliable server. As can be seen, the working theory of blockchain has been available for a long time, but the proper introduction of blockchain was given by an anonymous group or person named “Satoshi Nakamoto” in 2008 in a revolutionary whitepaper with a decentralized electronic money system named “Bitcoin.” By establishing a decentralized peer-to-peer system for locating and verifying transactions, Bitcoin eliminates them by putting in place a modern blockchain 1.0 [Frankenfield (2017)](#Frankenfield2017); [Sherman, Javani, Zhang, and Golaszewski (2019)](#Sherman2019). In the latter year, the first transaction involving bitcoin happened between Satoshi Nakamoto and Hal Finney, which was the first proper implementation of blockchain technology [Franken- field (2017)](#Frankenfield2017). A new cryptocurrency based on blockchain technology was introduced in 2013 by a programmer named Vitaly Dmitriyevich ([Frankenfield (2017)](#Frankenfield2017); [Aggarwal and Kumar (2021)](#Aggarwal2021)).

According to IBM analysts, the blockchain-based Distributed Ledger Technology (DLT) industry is predicted to reach $60.7 billion by 2024, illustrating the significance of the systems’ integration requirements. The adoption trend of blockchain systems is evident in virtually every digitized industry, compelling businesses to plan for the integration of blockchain technology [Frankenfield (2017)](#Frankenfield2017).Since the beginning of the blockchain era, investments in blockchain- related businesses have steadily expanded. In 2018, more than 60% of the market value of blockchain technology came from the financial industry. This makes it one of the most important drivers of blockchain integration [Gartner (2018)](#Gartner2018). In a recent survey of business leaders in Europe ([Blockchain.com (2019))](#Blockchain2019), more than half said they thought blockchain technology would soon be used in their already-established business models. About 66% of businesses around the world have shown a moderate level of  
interest in blockchain technology, and about 10% of these businesses are now either testing blockchain solutions or putting them into use [CryptoMarket (nd)](#Cryptond). In general, and Bitcoin in particular, cryptocurrencies are some of the oldest and most important uses of the well-known blockchain model. Bitcoin’s total market capitalization hit a record high of $205.4 billion U.S. dollars by the end of the third quarter of 2019 [(Alphand, Amoretti, Claeys, Dall’Asta, Duda, Ferrari, Rousseau, Tourancheau, Veltri, and Zanichelli (2018)](#Alphand2018). However, Bitcoin is usually seen as the most important and valuable cryptocurrency [De Vries (2018)](#DeVries2018). Due the pervasiveness of blockchain systems in our daily lives, the number of distributed node interactions is anticipated to increase dramatically [Nakamoto (2009)](#Nakamoto2009), putting a strain on the energy grid [CoinDesk (2018)](#Coindesk2018), infrastructure, and peer-to-peer (P2P) networks, as well as storage volumes [Mäkitalo, Ometov, Kannisto, Andreev, Koucheryavy, and Mikkonen (2017)](#Makitalo2017).

## **Problem Statement**

The Protection Motivation Theory (PMT) fails to recognize users’ trust determinants for blockchain technology adoption. Current theories lack a unified approach to assessing trust in both user and industrial contexts. Additionally, the existing blockchain development framework struggles to achieve the necessary trust, and blockchain technology lacks accepted protocols against criminal activities, resulting in explicit bans in 42 countries and complete bans in 9 countries [Bajpai, (2015)](#BajpaiP2015). The volatile value of blockchain-based cryptocurrencies, heavily dependent on user trust, raises sustainability concerns [Fauzi et al. (2020)](#MAFauzi2020); [Bloomberg (2021a)](#Bloomberg2021). Moreover, the significant energy and processing power demands pose challenges for widespread adoption, especially in developing nations ([Fauzi et al. (2020)](#MAFauzi2020); [Hayes (2017)](#HayesA2017); [Vranken (2017)](#Vranken2017)). In summary, addressing trust determinants, criminal activity protocols, and sustainability is vital for the improved adoption of blockchain technology.

## **Research Significance**

Due to its versatile potential, in 2018–2019, several tech titans, including Apple, Microsoft, Alphabet, Amazon, Facebook, Alibaba, Tencent, Samsung, and Intel, invested $1153 billion, $1105 billion, $902 billion, $887 billion, $543 billion, $486 billion, $403 billion, $382 billion, and $252 billion, respectively, in the research and development of blockchain technology for their own enterprise applications. Following in the footsteps of tech titans, modest investors are becoming interested in both investing in and applying blockchain technology to their respective companies. [Mappo (2019)](#Mappo2019) Despite its potential, has not achieved the expected global market expansion a decade after its debut. This is due to the lack of community trust required for widespread adoption. To address these issues, a sophisticated and trustworthy evaluation model is needed. Current human adoption theories, such as Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), and Analytical Hierarchical Model (AHM), are not suitable for evaluating the trust level of blockchain technology. This research aims to develop a standard evaluation system to test blockchain technology and show quantitative results for different trust factors. The blockchain's trust level can be improved by researchers by addressing specific areas that negatively impact it. If the evaluation system serves its meant purpose, blockchain could potentially replace the centralized economy with a decentralized system. However, if known and unknown problems are not addressed, users may not trust the system, leading to a market crash and the loss of half-century of research and two decades of investments.

## **Research Questions**

The research tries to answer the following questions:

**•** [How do determinants such as outdated technology, functionality, user experience, limitations, risks, positive experiences, and trust affect the adoption of new technologies, particularly in an enterprise setting?](#RQ1)

**•** [How effectively can the BCT-IATI framework assess the factors of blockchain-based technologies adoption?](#RQ2)

**•** How can the BCT be developed, maintained, and marketed efficiently?

**•** [What are the specific reasons why blockchain is not being embraced in enterprises?](#RQ3)

## **Research Novelty/Contribution**

The [table 1](#table1) ([Chenoweth, Minch, and Gattiker (2009)](#Chenoweth2009); [Degirmenci and Barros (2023)](#Degirmenci2023); [Alshammari and Rosli (2020)](#Alshammari2020)) compares PMT1 TAM2 and our unified BCT-IATI (Blockchain Technology Industrial Adoption Trust Index) model in response to the questions.

Firstly, the BCT-IATI Unified Model is more comprehensive than the PMT and TAM, as it considers a wider range of factors that influence the adoption of blockchain technology. These factors include perceived risk, trust, social norms, cognitive processing, experience, and complexity.

Table 1: Research Novelty Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **PMT****[[1]](#footnote-2)** | **TAM****[[2]](#footnote-3)** | **BCT-IATI**  **Unified Model** |
| Does the theory precisely assess the blockchain adoption factors? | × | × | ✓ |
| Can the theory assess blockchain and similar technology’s adoption factors? | × | ✓ | ✓ |
| Does the theory consider the elements of fear to be a depicted event? | ✓ | × | ✓ |
| Does the theory analyze the magnitude of a possible threat to a system? | ✓ | × | ✓ |
| Does the theory evaluate the likelihood of a threatening event’s occurrence? | ✓ | × | ✓ |
| Does the theory evaluate the efficacy of a system’s protective response? | ✓ | × | ✓ |
| Does the theory take into account the cognitive processing variable that mediates attitude change? | ✓ | × | ✓ |
| Does the theory consider the effect of all the social norms on technology adoption? | × | ✓ | ✓ |
| Does the theory take into account the targeted user’s experience when implementing similar technology as blockchain? | × | ✓ | ✓ |
| Does the theory properly measure the magnitude of blockchain system complexity? | × | × | ✓ |
| Does the theory quantify the degree to which a system is useful in day-to-day life? | × | ✓ | ✓ |
| Does the theory can estimate the effort required to learn specific blockchain-based technology? | × | ✓ | ✓ |
| Does the theory consider all the environmental forms indicating the level of trust in blockchain-based technology? | × | × | ✓ |
| Can the theory determine the better blockchain-based technology depending on certain parameters? | × | × | ✓ |

Next, the PMT and TAM focus on the perceived usefulness and ease of use of a new technology, which are important factors, but they do not consider the other factors that are unique to blockchain technology. The BCT-IATI Unified Model, designed specifically for blockchain technology, is more effective in capturing the nuances of its adoption than the PMT and TAM, which are more general theories applicable to any new technology. Additionally, the BCT-IATI Unified Model has been empirically tested for blockchain adoption. In contrast, the PMT and TAM have not been empirically tested for blockchain adoption. This means that the BCT-IATI Unified Model has a stronger empirical basis than the PMT and TAM. The BCT-IATI Unified Model is a valuable tool for businesses and organizations to determine the best Blockchain Technology (BCT) based on specific parameters. It helps identify factors influencing blockchain adoption, aiding in strategy development and informed decision-making. This model also enables organizations to compare different BCTs and select the one most likely to be adopted by users, thereby enhancing their decision-making process. Additionally, a government can use the BCT-IATI Unified Model to understand the factors that influence the adoption of BCT by citizens. This information can then be used to develop policies that promote the adoption of BCT.

In conclusion, the BCT-IATI Unified Model is a more comprehensive, specific, empirically validated, and useful model for assessing the adoption of BCT. With its consideration of diverse factors, specific focus on BCT, empirical testing, and practical applications, it proves to be a valuable tool for understanding and promoting the adoption of BCT in various contexts.

# **Research Background**

## **Blockchain Evaluation Models**

### **Protection Motivation Theory (PMT)**

Protective motivation theory (PMT) is a well-established psychological framework that provides valuable insight into how individuals respond to threats and exhibit protective behaviors. PMT ([Rogers (1975)](#Rogers1975)) believes that individuals are more likely to take protective action when they perceive the threat as serious and relevant to them and are confident in their ability to deal with it effectively. Empirical studies ([Rogers (1975)](#Rogers1975);[Witte (1992)](#Witte1992)) confirm the basic principles of PMT and its utility in understanding human responses to threatening situations.

[Figure 1](#fig1) ([Degirmenci and Barros (2023)](#Degirmenci2023)) denotes the final PMT model utilized in the development of our BCT-IATI framework is the model presented. In this, 2021 PMT [Figure 1](#fig1), each parameter has two levels of effect. HOC: higher-order construct; LOC: lower-order construct. Threat severity, threat vulnerability, and rewards are all mentioned as threat appraisal components, while response efficacy, self-efficacy, and response cost are all mentioned as coping appraisal components.

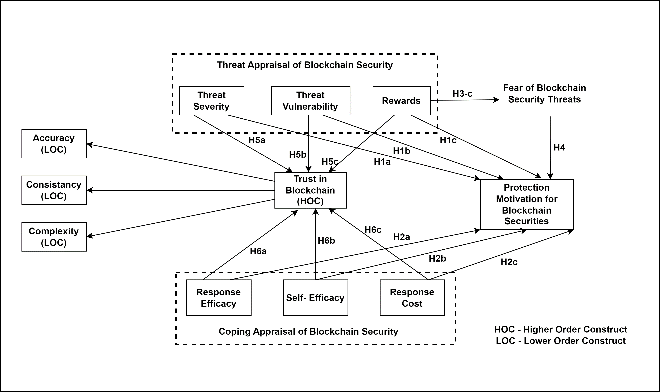


Figure 1: Adapted PMT ([Degirmenci and Barros (2023)](#Degirmenci2023))

All the mentioned parameters influence trust in blockchain, and trust influences the motivation for protection, whereas fear generated by threats also has an influence. In this model, trust affects accuracy, consistency, and complexity at a low level. This model heavily inspired the BCT-IATI framework to categorize our trust factors based on their significance and effect on trust in the blockchain.

### **Technology Adoption Model (TAM)**

The Technology Acceptance Model (TAM) is an established theory for predicting technology acceptance and usage behavior. According to TAM, people are more likely to adopt new technology when they find it [Davis (1989)](#DavisFD1989) helpful in achieving their goals and [(Venkatesh, Morris, Davis, and Davis (2003)](#Venkatesh2003) easy to use. Empirical studies provide evidence that TAMs are effective in explaining technology adoption patterns in various fields ([Taylor and Todd (1995)](#Taylor1995); [Mathieson (1991)](#Mathieson1991)).

A black background with white text

Description automatically generated

Figure 2: Unified Theory of Acceptance and use of technology model (UTAUT) ([Alshammari and Rosli (2020)](#Alshammari2020))

## **Evolution of PMT and TAM**

Rogers’s 1974 proposal for a model of PMT consisted of just three variables: (1). In the PMT version proposed by Milne et al., there are two main types of information gatherers: (1) external, through interactions and observing the world around you; and (2) internal, through considerations of one’s own personality and one’s own past experiences. Everything is fed into the cognitive mediation process, where the following four factors play crucial roles: First, one must determine the severity of the danger; second, one must evaluate available coping strategies; third, one must engage in maladaptive coping; and fourth, one must assess the threat. Threat assessment is the first variable, and it comprises several others such as perceived vulnerability, perceived severity, and dread. Perceived self-efficacy, perceived response efficacy, perceived response cost, etc., make up coping assessment, the second variable under consideration. Avoidance, denial, fatalism, pessimism, and other similarly unpleasant user responses make up maladaptive coping strategies. Protection motivation is affected in different ways by threat appraisal, coping appraisal, and maladaptive coping. Both dysfunctional coping and avoidance strategies are affected by how a threat is perceived. [Rogers (1975)](#Rogers1975)

More research into PMT in health-related areas showed that people often made predictable decisions, even if they were not always purely rational (which the model does not require) [M. A. Fauzi, N. Paiman, and Z. Othman (2020)](#MAFauzi2020).

On the other hand, Fred Davis’s seminal work, the Technology Acceptance Model (TAM), has been extensively used to examine what elements contribute to people’s being open to new forms of technology. TAM has emerged as the dominant framework for characterizing user behavior in relation to technology; it is based on the psychological theories of reasonable action (TRA) and planned behavior (TPB). Without an appreciation of the model’s limitations, it will be impossible to do thorough and methodical research on the topic. The reason for the first limitation is that the TAM was proposed this year [Vranken (2017)](#Vranken2017).

In the years after the first TAM model came out, the parsimonious TAM [Cheung, Roca, and Su (2015)](#CheungA2015) came out, which was a shorter version of the model. Several decades of research led to many changes and additions to the original model, which led to the TAM 2 model, which is the most up-to-date model [Schwartzer (2020)](#Schwartzer2020).

In 2000, Venkatesh and Davis added a new part to the Technology Acceptance Model (TAM). There are four cognitive instrumental processes that affect how useful something is thought to be: perceived ease of use, job relevance, result, demonstrability, and output quality. Subjective norms, image, and voluntariness are three social forces that affect perceived usefulness [Mappo (2019)](#Mappo2019). As human behaviors related to technology adoption are diverse and influenced by a wider range of variables the TAM provides valuable insight into technology adoption.

The [table 2](#Table2ComparisionTable) [Chenoweth et al. (2009](#Chenoweth2009)); [Degirmenci and Barros (2023)](#Degirmenci2023); [Alshammari and Rosli (2020)](#Alshammari2020) mentions the status of parameters in our BCT-IATI framework:

Table 2: Comparison table

|  |  |  |
| --- | --- | --- |
| **Assessment Model Name** | **Parameters** | **Remarks** |
| **PMT**1 | **Threat appraisal of blockchain** | Confirmed as dependent factor |
| Threat Severity (Perceived Severity) | Confirmed as independent factor |
| Threat Vulnerability (/Perceived Vulnerability) | Confirmed as independent factor |
| Rewards | It will be proposed in different way as a part of performance expectancy |
| **Coping appraisal of Blockchain security** | Confirmed as dependent factor |
| Self-Efficacy | Confirmed as independent factor |
| Response cost | Since it cannot be judged directly due to uncertainty, it can be indirectly considered as effort expectancy. |
| Response efficacy | Confirmed as independent factor |
| **Fear of blockchain** | Confirmed as dependent factor as a behavioral response of potential risks |
| **Maladaptive coping of BS** | Merging with copying appraisal to new variable |
| Technical Appraisal of BS | Will be merged with TAM |
| Complexity | Redefined and will be used as external factor |
| Accuracy | Since it has low priority in the model, it will not be considered |
| Consistency | Since it has low priority in the model, it will not be considered |
| Behavioral Intention | Confirmed as dependent factor |
| Trust in Blockchain (Trust Level in BCT) | Confirmed and will be used as output of BCT-IATI framework |
| **TAM**2 | Performance Expectancy | Confirmed as independent factor |
| Effort Expectancy | Confirmed as independent factor |
| Social Influence | Redefined and will be used as external factor |
| Gender | Since it has no visible effect, it will not be considered |
| Experience | Redefined and used as independent factor |
| Voluntariness of use | Indirectly connected to social influence, |
| Use behavior (output  of usage decision) | Similar to intention to use BCT |
| Facilitating conditions | Will not be used |
| **Perceived Usefulness** | Confirmed as dependent factor |
| Subjective Norm | Similar to Facilitating condition |
| Experience | Redefined and confirmed as independent factor |
| Voluntariness | Since it is very difficult to determine without primary data, it is merged with Behavioral intention |
| Image | Confirmed as independent factor affected by social influence |
| Job Relevance | Confirmed as independent factor |
| Output Quality | Since it has low priority, it will not be used. |
| Result Demonstrability (/Performance verifiability) | Confirmed as independent factor |
| Perceived ease of use | Same as Effort Expectancy |
| Intention to use | Same as voluntariness |
| Usage Behavior | Same as actual intention to use (Final decision result) |

# **Methodology**

Based on the Protection Motivation Theory (PMT) model in [Figure 1](#fig1) and the Technology Acceptance Model (TAM) in [Figure 2](#fig2), the [Figure 3](#fig3) represents our research model. This research model combines both theories in an improvised way.

As can be seen in [Figure 3](#fig3), there are 3 types of trust factors: 1. subcategory; 2. main category; and 3. external factors. The independent parameters or trust factors that directly influence the dependent main category and external trust factors are called “sub-categories.” For example: threat severity, threat vulnerability, response efficacy, etc. On the other hand, the dependent trust factors that directly influence the intention to use BCT are known as the “main category.” For example: threat appraisal, coping appraisal, and behavioral intention. External factors influence trust factors in the main category in addition to those in the subcategories. “External factors” that are dependent or independent but have a strong influence on the intention to use BCT, or the main category of trust factors, are the last types of trust factors. For example, social influence and system complexity. The [appendix](#appendix) section will describe and use the various types of categories in more detail. In our suggested research model, PMT and TAM were modified, and it is assumed that blockchain users in normal decision-making situations will exhibit similar protective incentives and environment-related behaviors. In other words, threat assessment, coping appraisal, fear, perceived usefulness, behavioral intention, social influence, complexity, maladaptive coping, and blockchain-based technology experience will be crucial. The details of the factors are given in the [table 10](#Table10Definitions) ([M. A. Fauzi, N. Paiman, and Z. Othman (2020)](#MAFauzi2020); [Degirmenci and Barros (2023)](#Degirmenci2023); [Popper (2021)](#Popper2021)).

A diagram of a blockchain

Description automatically generated

Figure 3: Theoretical Model for Blockchain Technology Industry Adoption Trust Index (BCT-IATI) Assessment Framework.

First, the hypothesized associations based on the suggested BCT-IATI model will be examined, followed by the role of the trust level in the blockchain. The constructed hypothesis is given below:

**H1:** Performance Verifiability, Job Relevance, and Experience affect the Perceived usefulness.

**H2:** Performance Expectancy and Effort Expectancy influence behavioral Intention.

**H3:** Images affect both social influence and perceived usefulness.

**H4:** Social influence affects Perceived Usefulness and behavioral intention.

**H5:** Response efficacy and Self Efficacy influence Coping Appraisal.

**H6:** Threat Severity and Threat Vulnerability affect Threat Appraisal.

**H7:** Coping Appraisal affects Maladaptive Coping.

**H8:** Threat Appraisal influence Fear of Blockchain.

The perceived threat of blockchain technology lowers the intention to use it, resulting in lower trust. A better coping evaluation increases the likelihood of using blockchain, boosting faith. The perceived utility of blockchain increases its usage, boosting trust. The positive impact of blockchain on society also increases its likelihood of being viewed positively and acted upon. Therefore, the more perceived threat, fear, and utility, the greater the trust in blockchain technology.

**H9:** Perceived Usefulness, Behavioral Intention, Maladaptive Coping, Fear of Blockchain, and System Complexity affect Intention to Use Blockchain.

**H10:** Intention to use blockchain highly influences the trust level of blockchain.

By considering the hypothesis, the simplified BCT-IATI model should look like the following [Figure 4](#fig4).

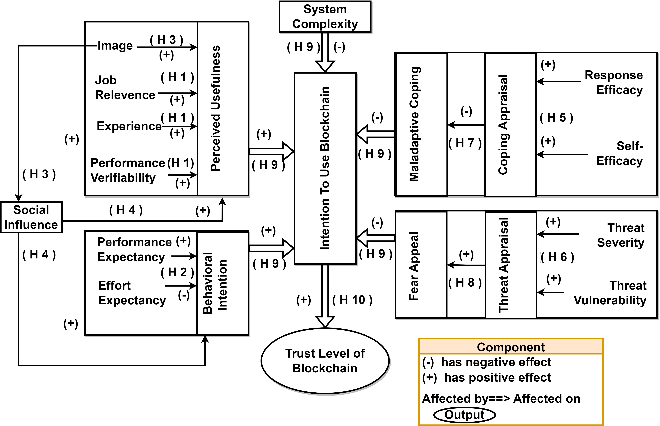


Figure 4: Hypothetically proposed model (BCT-IATI) for Blockchain Technology Industry Adoption Trust Index Assessment Framework

Here, the trust factor or parameter containing the (+) sign represents that it positively influences the pointed factor, and the (-) sign represents that it negatively affects the pointed factor.

## **Flowchart of BCT-IATI framework**

For a better understanding of the algorithm, the flowchart of the whole process of the BCT-IATI framework is given in [Figure 5](#fig5) .

A diagram of a diagram

Description automatically generated with medium confidence

Figure 5: Flowchart of BCT-IATI assessment

### **Step*-1:* *Raw text input collection with reference***

The evaluation model’s most crucial step involves selecting an input source from a text and providing the source URL. After that, if the source is a research paper, blog, or website, the user must copy and paste his selected text, and for video, the user has to mention the timestamp to evaluate it. The user can add, edit, or delete sources before and after each evaluation cycle, but it is advised not to change the input source between cycles as this could corrupt the result.

### ***Step-2: Identification of trust factor and score calculation***

The evaluation model’s most time-consuming and computationally intensive step involves three sub-tasks: converting raw text into processed “clean text” for comparison with trust factors. Then, comparing the sentiment of clean text with independent and external trust factors mentioned earlier in [Section 3.1](#sec31) and assigning a score to each trust factor based on the input text’s portion A detailed explanation is given below:

1. **Text analysis process:**The diagram given in [Figure 6](#fig6) represents the first part of Step 2 by doing the text analysis process*:*

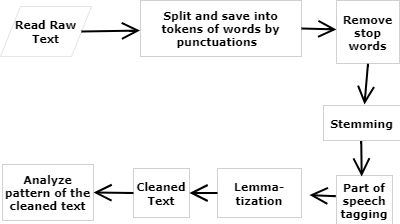
**

Figure 6: Text analysis process (NLP) flowchart of BCT-IATI framework

As it can be seen in the [figure 6](#fig6) diagram, the text analysis process in the BCT-IATI framework involves splitting and saving raw text by punctuation using the “word\_tokenize()” function. The base/root word of all token words is taken by the “stem()” function, reducing processing time. The stemmas are tagged into parts of speech using the “pos\_tag()” function. The “lemmatize()” function identifies the base word for different tenses, genders, and moods. The NLP algorithm then attempts to understand the meaning of a named entity to better understand the sentiment of the input sentence. Therefore, it is capable of identifying impact of the trust factors, with the actual availability score by using the code given in the GitHub repository link: <https://github.com/ProgMahabub21/Text-Analysis>. The text analysis process is created using NLTK in the Python programming language. [IBM (n.d.)](#IBMnd)

1. **Identification of trust factor pattern and comparison of sentiment :**The majority of the processing time of BCT-IATI framework is spent on the second part of Step 2: calculating different trust factors by identifying patterns that affect other trust factors. For a better understanding of each categorized factor, they are demonstrated as blocks. The flowchart in [Figure 7](#fig7) represents the data flow of trust factor blocks influencing the trust factors.

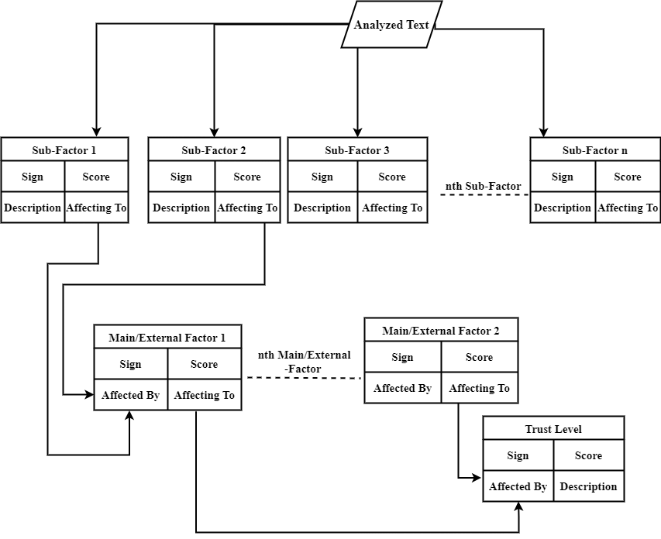


Figure 7: The data flow of trust factors affecting trust level

The blockchain’s trust level is directly influenced by various external and major factors, which are identified and updated based on the name, sign, score, and description of each sub-factor block, ensuring a comprehensive evaluation of the blockchain’s effectiveness.

1. **Score Calculation Process:**After comparing the sentiment of the text with the trust factor by using the following code or pseudocode, the score is added to the related trust factors. It is the last portion of Step 2.

The scale of the BCT-IATI framework ranges from 0 up to 10. As mentioned earlier in [Figure 7](#fig7), all the factors contain their name, signed score, reference to the factor(s) they are affected by, and the reference to the factor(s) they are going to affect too. There can be two possible routes each factor can take.

Table 3: Positive Score Ranges

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Availability Status** | **Not Available** | **Very Low** | **Low** | **Medium** | **High** | **Very High** |
| **Score Range** | 0 | 0<score<2 | 2≤score<4 | 4≤score<6 | 6≤score<8 | 8≤score ≤10 |

Table 4: Negative to positive conversion table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Negative Score Range** | 0 | -10 ≤ score≤ -8 | -8 < score≤ -6 | -6 < score≤ -4 | -4 < score≤ -2 | -2 < score<0 |
| **Negative Availability** | **Not Available** | **Very High** | **High** | **Medium** | **Low** | **Very Low** |
| **Equivalent Positive Status** | **Not Available** | **Very Low** | **Low** | **Medium** | **High** | **Very High** |
| **Equivalent Positive Score** | 0 | 0 < score <2 | 2 ≤ score <4 | 4 ≤ score <6 | 6 ≤ score <8 | 8 ≤ score≤ 10 |
|

If the score value of the following factor has a positive impact on the next factor (has a positive score), the scale will follow [table 3](#table3positivescore) .

If the score value of the following factor has a negative impact on the next factor (has a negative score), the score will be converted to its equivalent positive score. For a negative score, the scale will follow [table 4](#table4NegtoPos) .

***Code/Pseudocode* :** Pseudocodes have been developed for systematic analysis of the sentiment of clean text in the three mentioned distinct categories of trust factors, as well as the central scale system utilized within the BCT-IATI framework. Here are pseudocodes from every listed category; a sample is given below, and the rest can be found at the following link: <https://github.com/sheikhmahmudulhasanshium/PsudoCode.git>.

**Code/Pseudocode for Scale:**

The scale is implemented by combining [Table 3](#table3positivescore) and [Table 4](#table4negTopos) The snippet of the Code/Pseudocode for the scale is given [Snippet 1](#Snippet1Scale) .

|  |
| --- |
| def scale(factor\_name, score):  “““  Scales the score of a factor to a value between 0 and 10.  Args:  factor\_name: The name of the factor.  score: The score of the factor.  Returns:  The scaled score.  “““  if score >= 0:  if score > 0 and score < 2:  return score / 2  elif score <= 2 and score < 4:  return score / 3  elif score <= 4 and score < 6:  return score / 4  elif score <= 6 and score < 8:  return score / 5  elif score <= 8 and score < 10:  return score / 6  else:  return score / 7  else:  return (10 + score) / 11 |

Snippet 1 Scale

**Code/Pseudocode for Sub-factors:**

The Code/Pseudocode is developed by identifying different subcategories from the definition given in [appendix](#appendix) section and depending on the sentiment of the input sentence identified by the text analysis process mentioned in [Section 3.1.2.1](#sec3121), the availability score of each sub-factor is calculated. The sample Code/Pseudocode of the sub-factor is given in [Snippet 2](#Snippet2ThreatSeverity).

|  |
| --- |
| def score\_ts(para):  TS = 0  for sentence in para:  if sentence does not have a problem that another technology has:  TS = 1  elif sentence has a problem that can be overlooked:  TS = 3  elif sentence has a solution to the problem but it is not matured or optimized enough:  TS = 5  elif sentence has evidence of an unsolved problem that is less likely to happen again:  TS = 7  elif sentence has evidence of an unsolved problem that reduced trust level significantly enough to switch to other technology:  TS = 9  return TS  for para in document:  TS = score\_ts(para) |

Snippet 2: Threat Severity

**Code/Pseudocode for Main-factors:**

The Code/Pseudocode is developed by measuring the average of the evaluated subcategories, and the negative values are converted by using the conversion algorithm in [Snippet 3](#Snippet3).

|  |
| --- |
| def calculate\_factors():  TA = round((TS + TV) / 2)  FA = -TA  CA = round((RE + SE) / 2)  MC = -CA  BI = round((PE + EE + SI) / 3)  PU = round((Im + PV + JR + Ex + SI) / 5)  IB = round((FA + MC + SC + BI + PU) / 5)  TL = IB \* 10  return TA, FA, CA, MC, BI, PU, IB, TL  def main():  TA, FA, CA, MC, BI, PU, IB, TL = calculate\_factors()    if \_\_name\_\_ == “\_\_main\_\_”:  main() |

Snippet 3 : Main Factor

**Code/Pseudocode for External factors:**

The Code/Pseudocode is developed by identifying different external factors from the definition given in [Section 3.1](#sec31) and depending on the sentiment of the input sentence identified by the text analysis process mentioned in [Section 3.2.2.1](#sec3121), the availability score of each external factor is calculated. The sample Code/Pseudocode of the sub-factor is given in [Snippet 4](#Snippet4).

|  |
| --- |
| def score\_sc(para):  SC = 0  for sentence in para:  if sentence mentions that BCT is very easy to understand for the user and the system is very easy to implement:  SC = 1  elif sentence mentions that BCT is relatively easy to understand because of reliable solutions and well-defined support, and the system is still difficult to maintain and implement when problems occur:  SC = 3  elif sentence mentions that BCT is sometimes difficult to understand because of its partially reliable solution and undefined support and is still difficult to maintain and implement when a problem occurs:  SC = 5  elif sentence mentions that BCT is most of the time difficult to understand because it has no existing solution and no reliable support and is very difficult to maintain and implement when a problem occurs:  SC = 7  elif sentence mentions that BCT has unsolved challenges of using BCT due to system complexity or the user is losing interest in using blockchain due to the high effort required to find and understand the solution of BCT:  SC = 9  return SC  for para in document:  SC = score\_sc(para) |

Snippet 4: System Complexity

### ***Step-3: Rounding and Value of Sign Adjustment***

This step contains two major sub-tasks: the fraction and odd values are rounded for further evaluation in the score rounding section, and trust factors with negative affect are converted to equivalent positive scores by using the scale given in [Section 3.1.2.3.](#sec3123) For example, for low system complexity (4), the equivalent positive value will be high (8) since it has a negative effect on the next factor, trust level. The flowchart of the generalized calculation process is given in [figure 8](#fig8).

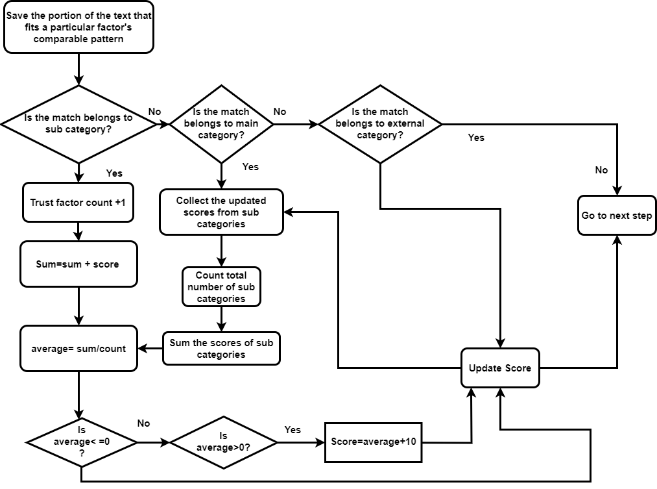


Figure 8: The calculation flowchart of the score of trust factors of the evaluation framework

### ***Step-4: Trust Level Description with Summary***

After all the calculations, the trust level is stated with a description. The description contains the score of all three types of previous factors affecting the trust level. If a user manually readjusts a score, he or she can also review the trust factor scoring and remarks in the correction log in the next evaluation cycle.

### ***Step-5: Manual Readjustment***

This is an optional step to solve an issue with the scoring due to rounding, when the evaluation criteria do not match the sentiment of the input text, or for any other reason, which leads the user to believe the evaluation is unfair. The user can select or trace back the problem by reading the trust level description and updating the score. The [formula](#Equation) mentioned here will be used by the framework to assess its accuracy:

*This is how the framework should evaluate blockchain-based technologies based on input from various sources.*

# **Results**

On a scale of 0–10 given in [Section 3.1.2.3](#sec3123); the trust factors were evaluated. A thorough study is conducted to evaluate blockchain-based technologies, for example, Bitcoin, Ethereum, Social NFT, etc., from multiple reliable sources. After evaluation, the score was averaged for a fair score. Finally, the behavioral intention and the trust level of blockchain technology are based on the relationship between trust factors and parameters described in [appendix](#appendix) section.

## **Case Study 1: Ethereum**

Ethereum, a decentralized open-source blockchain system introduced by Vitalik Buterin in 2013 and operational since 2015, boasts its native cryptocurrency, Ether (ETH), which serves as payment for transactions and services on the network. A prominent aspect of Ethereum is its smart contracts, transparent and immutable self-executing contracts residing on the blockchain, capable of automating various functions like financial transactions, voting, and property ownership. This feature holds tremendous potential to revolutionize numerous industries, offering opportunities for creating a more efficient and transparent financial system and establishing novel forms of decentralized governance [Buterin et al. (2014)](#Buterin2014). As Ethereum continues to evolve, its impact on various sectors could be substantial and far-reaching, presenting exciting possibilities for the future.

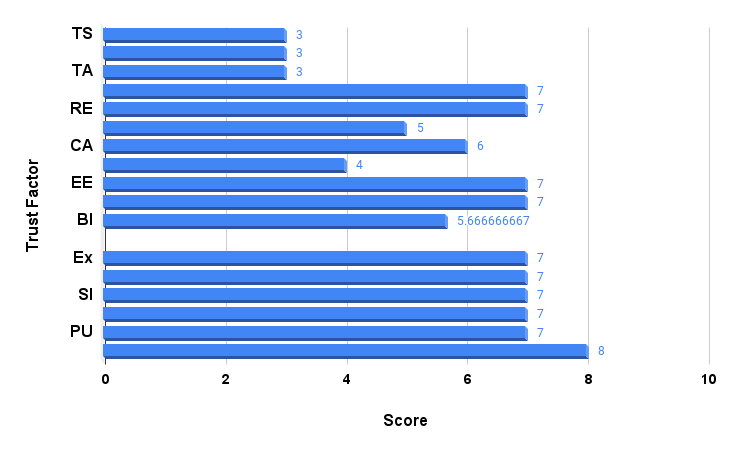


Figure 9: Trust Score of Ethereum

The detailed evaluation of each trust factor is given in section A.1 (which can be accessed by the link: <https://aiubedu60714-my.sharepoint.com/:w:/g/personal/19-40764-2_student_aiub_edu/EScFUoJjo9RNuWhpCDo2vyMB6sMVpfgFfQZMHAOReJH-xA?e=5xg4g4>). The chart of [Ethereum](#fig9) demonstrates the calculated trust factors from the review of Ethereum from multiple sources given in the table.

## **Case Study 2: Bitcoin**

Bitcoin was the first decentralized cryptocurrency, and it was released as open-source software in 2009. As of March 2022, there were over 9,000 different cryptocurrencies [Szabo (1998)](#Szabo1998) on the market, with over 70 having a market capitalization greater than $1 billion. [Kish, Srinivasan,Wortzel, Sharma Charge D’affaires, Chung, Jain, Lichtman, French, Watts, Lee, and Smith (nd))](#KishMnd)

A graph with numbers and a bar

Description automatically generated

Figure 10: Trust Score of Bitcoin

The detailed evaluation of each trust factor is given in Section A.2 (which can be accessed by thelink:<https://aiubedu60714-my.sharepoint.com/:w:/g/personal/19-40764-2_student_aiub_edu/EScFUoJjo9RNuWhpCDo2vyMB6sMVpfgFfQZMHAOReJH-xA?e=5xg4g4>). The chart of [Bitcoin](#fig10) demonstrates the calculated trust factors from the review of Bitcoin from multiple sources given in the table.

## **Case Study 3: Solana**

Solana is an open-source project implementing a new, high-performance, permissionless blockchain. Finding a way to share a time when nodes cannot rely on one another Solana uses a far more granular verifiable delay function, a SHA-256 hash chain, to coordinate consensus. So, it is one of the blockchain’s protocols, whose objectives are to run programs using the platforms.

A graph with numbers and a bar

Description automatically generated

Figure 11: Trust Score of Solana

The detailed evaluation of each trust factor is given in Section A.3 (which can be accessed by the link: <https://aiubedu60714-my.sharepoint.com/:w:/g/personal/19-40764-2_student_aiub_edu/EScFUoJjo9RNuWhpCDo2vyMB6sMVpfgFfQZMHAOReJH-xA?e=5xg4g4>). The chart of [Solana](#fig11) demonstrates the calculated trust factors from the review of Solana from multiple sources given in the table.

## **Case Study 4: Dogecoin**

In the cryptocurrency ecosystem, Dogecoin (DOGE) has truly taken off. One of the most well-known cryptocurrencies ever is what began as a parody cryptocurrency. Even more impressive is the fact that Dogecoin’s popularity does not appear to be declining; rather, it appears to be increasing with each passing day. Doge is a humorous meme; however, the way Dogecoin impacts our planet’s environment is not at all humorous. The fact that DOGE is technologically based on the obsolete and ineffective Proof of Work algorithm, a sort of blockchain infrastructure, is the source of the issue. [Hayes (2017)](#HayesA2017) As per supply statistics as of August 17, 2022, there was 132.6 billion DOGE in supply, where the market capitalization was $10.9 billion with a 484.91 TH/sec hash rate [Bajpai (2015)](#BajpaiP2015).

A graph with numbers and a bar

Description automatically generated

Figure 12: Trust Score of Dogecoin

The detailed evaluation of each trust factor is given in Section A.4 (which can be accessed by the link: <https://aiubedu60714-my.sharepoint.com/:w:/g/personal/19-40764-2_student_aiub_edu/EScFUoJjo9RNuWhpCDo2vyMB6sMVpfgFfQZMHAOReJH-xA?e=5xg4g4>). The chart of [Dogecoin](#fig12) demonstrates the calculated trust factors from the review of Dogecoin from multiple sources given in the table.

## **Case Study 5: Social NFT Marketplace**

A social NFT marketplace is an online marketplace where users can purchase, sell, and trade non-fungible tokens (NFTs). It offers a safe, secure, and user-friendly platform for users to showcase their digital assets and interact with the community. It also lets users communicate with one another through chat, comments, and ratings. In addition, users can monitor their portfolios, connect with other users, and discuss NFT market trends.

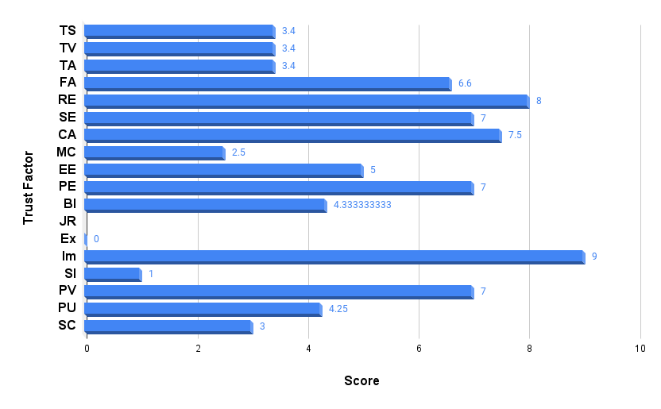


Figure 13: Trust Score of Social NFT

The detailed evaluation of each trust factor is given in Section A.6 (which can be accessed by the link: <https://aiubedu60714-my.sharepoint.com/:w:/g/personal/19-40764-2_student_aiub_edu/EScFUoJjo9RNuWhpCDo2vyMB6sMVpfgFfQZMHAOReJH-xA?e=5xg4g4>). The chart of [Social NFT](#fig13) Marketplace demonstrates the calculated trust factors from the review of Bitcoin from multiple sources given in the table.

## **Case Study 6: Axie Infinity**

Axie Infinity is a blockchain-based game that combines the greatest elements of collection and warfare games with the chance to acquire tokens. Axies are digital creatures that players can keep, reproduce, fight, and trade. Axies can be mated with different body parts, accessories, and classes to produce unique axes. Axies can then be utilized to engage in combat with other players for rewards. Additionally, players can earn tokens by engaging in a variety of in-game activities. Axie Infinity also features a marketplace for purchasing and selling in-game items, as well as a decentralized platform for creating and playing user-generated content.

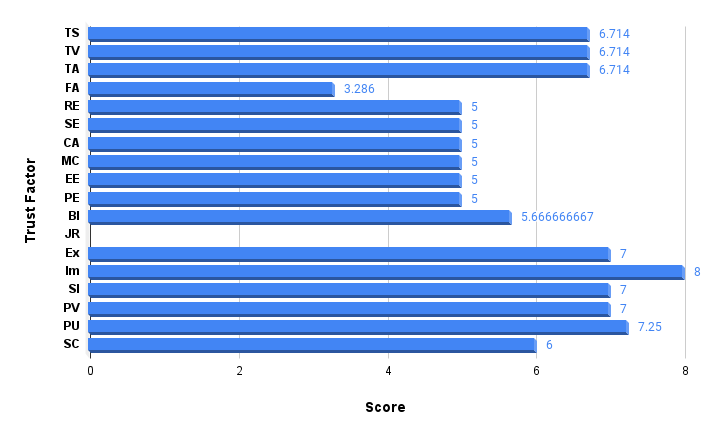


Figure 14: Trust Score of Axie Infinity

The detailed evaluation of each trust factor is given in Section A.5 (which can be accessed by the link: <https://aiubedu60714-my.sharepoint.com/:w:/g/personal/19-40764-2_student_aiub_edu/EScFUoJjo9RNuWhpCDo2vyMB6sMVpfgFfQZMHAOReJH-xA?e=5xg4g4>). The chart of [Axie Infinity](#fig14) demonstrates the calculated trust factors from the review of Bitcoin from multiple sources given in the table.

# **Discussion**

The study aimed to understand the reasons behind public and industry resistance to BCT adoption by examining two popular human recruitment theories: PMT and TAM. These models contain different trust factors and priority levels, making them confusing. To address this, both theories were combined and realigned to redefine the relationship between trust coefficients influencing BCT trust. A unified framework was developed, assessing BCT trust factor through sentiment and text analysis from authoritative sources. The independent variables collected from the mentioned PMT and TAM frameworks are given in the [table 5](#table5), [Chenoweth et al. (2009)](#Chenoweth2009); [Degirmenci and Barros (2023)](#Degirmenci2023); [Alshammari and Rosli (2020)](#Alshammari2020) :

Table 5: Independent Variables of PMT & TAM

|  |  |
| --- | --- |
| **Theories** | **Independent Variables** |
| **Protection Motivation Model**  **(PMT)** | threat severity, threat vulnerability, response efficacy, self-efficacy |
| **Technology Acceptance Model (TAM)** | image, performance verifiability, job relevance, experience, performance expectancy, effort expectancy |

The dependent variables are given in the [table 6](#table6) [Chenoweth et al. (2009)](#Chenoweth2009); [Degirmenci and Barros (2023)](#Degirmenci2023); [Alshammari and Rosli (2020)](#Alshammari2020)

Table 6: Dependent Variables of PMT & TAM

|  |  |
| --- | --- |
| **Theories** | **Dependent Variables** |
| **Protection Motivation Model**  **(PMT)** | threat appraisal, fear appeal, coping appraisal, maladaptive coping |
| **Technology Acceptance Model (TAM)** | behavioral intention, perceived usefulness, |

The external factors are given in the [table 7](#table7) [(Chenoweth et al. (2009)](#Chenoweth2009); [Degirmenci and Barros (2023)](#Degirmenci2023); [Alshammari and Rosli (2020)](#Alshammari2020))

Table 7: External Variables of PMT & TAM

|  |  |
| --- | --- |
| **Theories** | **Dependent Variables** |
| **Protection Motivation Model** **(PMT)** | System complexity |
| **Technology Acceptance Model (TAM)** | Social Influence |

The definition of each factor of our unified BCT-IATI model is mentioned in the Appendix section, in the [table 10](#Table10Definitions) [Chenoweth et al. (2009)](#Chenoweth2009); [Degirmenci and Barros (2023)](#Degirmenci2023); [Alshammari and Rosli (2020)](#Alshammari2020) in detail.

## **How do determinants such as outdated technology, functionality, user experience, limitations, risks, positive experiences, and trust affect the adoption of new technologies, particularly in an enterprise setting?**

When making a choice to adopt a new technology, individuals and organizations consider several factors that influence their decision. One such factor is the existence of outdated technology with its limitations, risks, or other problems that the new technology aims to address. If the new technology offers better functionality and is expected to perform more effectively, it becomes more appealing for adoption. For instance, in 2012, Google introduced the Circles feature on its social media platform, Google+, allowing users to share activities from external websites with their Google+ friends. However, later revelations revealed that Google+ had secretly tracked users’ activities on these external sites, even when they were not logged into the platform. This tracking was done using “invisible 1x1 pixels” embedded on other websites without obtaining users’ informed consent or providing an opt-out option. As a result, a privacy backlash emerged in early 2011, leading notable users like Robert Scoble to leave the Google+ platform. Despite Google’s subsequent attempt to address the issue by changing the Circles feature to an opt-in setting, the negative impact had already been felt. The incident generated significant anger, disappointment, and distrust among users regarding Google+’s practices, resulting in widespread rejection of the platform within the user community. Consequently, Google+ faced challenges in regaining its former standing, and the Circles feature remained relatively unpopular in the history of social media. This event serves as a strong reminder of the utmost importance of user trust and privacy considerations, with far-reaching implications for both individual platforms and the broader social media industry [Imran and Zimmer (2017))](#ImranM2017).

Ease of use is another significant factor. If the new technology is user-friendly and intuitive, it increases the likelihood of attracting new users. Positive past experiences with similar types of technology can also play a role. If users have previously utilized similar technologies and had positive outcomes, they are more inclined to adopt the new technology. An illustration of this phenomenon can be observed in the realm of photo editing software, particularly Adobe Photoshop, a widely-used tool employed by both professionals and hobbyists. Despite its popularity, some users find the software challenging to comprehend, particularly those with limited familiarity with photo editing processes. In recent times, there has been a noticeable trend where users are transitioning towards interactive photo editing software alternatives such as GIMP and Paint.NET. These emerging solutions are intentionally designed to be more user-friendly and interactive, catering to a broader spectrum of users. Their emphasis on simplicity and ease of understanding has led to an increasing number of users adopting these new platforms, reflecting the significance of user-friendliness in technology adoption decisions [Drake (2018)](#DrakeRR2018).

Additionally, the level of trust in the new technology is crucial. Users evaluate whether the technology has any limitations or evidence of threats. For instance, if the new technology demonstrates effective incident prevention or the involvement of the organization in taking appropriate action, it instills trust and creates a positive image of the product. This can motivate existing users to continue using the technology and encourage new users to adopt it.

In an enterprise setting, trust-level determinants play a vital role in adoption decisions. The BCT Trust Index framework suggests that factors like system complexity, social impact, performance verifiability, job relevance, experience, performance expectations, and effort expectations directly influence the trust level of accepting BCT-based (Blockchain Technology) products. These determinants affect the likelihood of adoption, both for general users and industry professionals.

In summary, when considering the adoption of new technology, users and enterprises assess various factors such as outdated technology, functionality, user experience, limitations, risks, positive experiences, and trust. These factors collectively shape the decision-making process and influence the adoption of new technologies.

## **How effectively can the BCT-IATI framework assess the factors of blockchain-based technology adoption?**

Our research paper highlights the BCT-IATI Unified Model as a novel and comprehensive approach for evaluating the factors influencing the adoption of blockchain-based technology (BCT) within enterprises. By incorporating trust factors from the Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM), this framework goes beyond mere reliance on market hype, aiming to provide a deeper and more robust evaluation process. Unlike approaches that focus on specific industries such as healthcare, supply chain, or logistics, our framework seeks to standardize BCT products in a general context. Moreover, it is designed to be versatile and adaptable across various countries, drawing information from diverse sources like articles, journals, websites, blogs, and other reviews worldwide. [Balasubramanian, Shukla, Sethi, Islam, and Saloum (2021)](#Balasubramanian2021)

An important strength of the BCT-IATI Unified Model lies in its ability to offer a holistic perspective on BCT adoption by considering a wide range of factors. These encompass technological, psychological, and motivational dimensions, enabling a thorough understanding of the determinants that drive or inhibit BCT adoption in the enterprise setting. By analyzing multiple parameters related to the reliability, sustainability, and overall feasibility of BCT, this framework ensures that all relevant aspects are considered and contributes to a comprehensive assessment.

Moreover, the model’s streamlined criteria, achieved by combining similar parameters and eliminating low-priority factors, enhance its efficiency and focus without compromising accuracy. This approach facilitates a more effective assessment of BCT adoption factors, empowering enterprises to make well-informed decisions based on the model’s insights.

The BCT-IATI Unified Model also benefits from insights derived from the correlation matrix, which provides valuable information on the interrelationships between factors. By identifying key influential factors and potential risks, the model’s predictive capabilities are strengthened, allowing for a more informed assessment of BCT adoption potential.

Another significant advantage of the BCT-IATI Unified Model is its practical applicability to diverse BCT implementations and specific enterprise contexts. Its adaptability to real-world scenarios ensures that enterprises can use the framework to guide adoption decisions that align with their unique needs and goals.

However, while acknowledging these strengths, it is crucial to recognize that the effectiveness of the BCT-IATI Unified Model can be further enhanced with more extensive data and feedback from actual BCT users in an enterprise setting. Gathering real-world data and user experiences will provide valuable insights to validate and refine the model, making it even more robust and accurate in assessing BCT adoption factors.

Furthermore, considering the dynamic nature of technology and the rapid advancements in the blockchain domain, continuous updates, and refinements to the BCT-IATI Unified Model will be essential to keeping pace with evolving market trends and user preferences.

In conclusion, the BCT-IATI Unified Model is a powerful tool for evaluating factors influencing blockchain adoption in enterprises. It incorporates PMT and TAM trust factors, correlation matrices, and optimized criteria. However, ongoing data collection and user feedback are crucial for refining the model. Collaborative efforts between researchers, industry practitioners, and technology users will lead to a more precise and actionable model for enterprises adopting blockchain technologies.

## **What are the specific reasons why blockchain is not being universally embraced?**

The reason for the limited universal adoption of blockchain technology can be attributed to various specific factors, as evident from the outcomes obtained through our BCT-IATI Unified Model, displayed in [Table 8](#table8).

Table 8: Summery result of the BCT products' trust index assessment using the proposed framework

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **BCT**  **Product**  **Trust Factor** | **Bitcoin** | **Ethereum** | **Solana** | **Dogecoin** | **Axie Infinity** | **Social NFT Marketplace** |
| **TS** | 4.3158 | 3 | 3 | 6.6 | 6.714 | 3.4 |
| **TV** | 4.3158 | 3 | 3 | 6.6 | 6.714 | 3.4 |
| **TA** | 4.3158 | 3 | 3 | 6.6 | 6.714 | 3.4 |
| **FA** | 5.6842 | 7 | 7 | 3.4 | 3.286 | 6.6 |
| **RE** | 4.9474 | 7 | 5.25 | 1 | 5 | 8 |
| **SE** | 5.3158 | 5 | 5.5 | 1 | 5 | 7 |
| **CA** | 5.1316 | 6 | 5.5 | 1 | 5 | 7.5 |
| **MC** | 4.8684 | 4 | 4.5 | 9 | 5 | 2.5 |
| **EE** | 5.3529 | 7 | 1.2857 | 6.3333 | 5 | 5 |
| **PE** | 5.6316 | 7 | 6.55 | 5.6667 | 5 | 7 |
| **BI** | 4.8429 | 5.6667 | 7.0881 | 5.2222 | 5.6667 | 4.3333 |
| **JR** | \_ | \_ | \_ | \_ | \_ | \_ |
| **Ex** | 3 | 7 | 3 | 6.3333 | 7 | 0 |
| **Im** | 4.5455 | 7 | 6.77 | 5 | 8 | 9 |
| **SI** | 4.25 | 7 | 6 | 6.3333 | 7 | 1 |
| **PV** | 7.4 | 7 | 7 | 3 | 7 | 7 |
| **PU** | 4.7989 | 7 | 5.6925 | 5.1667 | 7.25 | 4.25 |
| **SC** | 7 | 8 | 1 | 2 | 6 | 3 |
| **TL (%)** | **46.9151** | **55.333** | **68.5612** | **45.5778** | **50.4053** | **59.3667** |

From the trust level scores expressed as a percentage, it is clear that the intentions to adopt these BCT products differ. Bitcoin and Ethereum have a Trust Index score of 46.92% and 53.33%, respectively, indicating a moderate level of trust and adoption intent. On the other hand, Solana, Social NFT Market-Place, and Axie Infinity showed higher relative trust index scores of 68.56%, 59.37%, and 50.41%, respectively, indicating a better outlook for acceptance. However, Dogecoin lags behind with a Trust Index of 45.58%, indicating a relatively low level of trust and intention to adopt.

The specific reasons for the different levels of acceptance can be explored in more detail by analyzing the performance of each BCT product on specific trust determinants. Here is an overview of the weak or poor performance areas for each product based on specific trust factors [table 9](#table9).

Table 9: Overview of weak/poor performed BCT products on particular trust determinants

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Trust Factor** | **Bitcoin** | **Ethereum** | **Dogecoin** | **Solana** | **Social NFT** | **Axie Infinity** |
| **Threat Severity** |  |  | ✓ |  |  | ✓ |
| **Threat Vulnerability** |  |  | ✓ |  |  | ✓ |
| **Response Efficacy** | ✓ |  | ✓ |  |  |  |
| **Self-Efficacy** |  | ✓ | ✓ |  |  |  |
| **Effort Expectancy** |  | ✓ | ✓ |  |  |  |
| **Performance Expectancy** |  |  |  |  |  | ✓ |
| **System Complexity** | ✓ | ✓ |  |  |  | ✓ |
| **Experience** | ✓ |  |  | ✓ | ✓ |  |
| **Image** | ✓ |  | ✓ |  |  |  |
| **Social Influence** | ✓ |  |  |  | ✓ |  |
| **Performance Verifiability** |  |  | ✓ |  |  |  |

Dogecoin, for instance, underperforms on seven independent variables, exhibiting the lowest trust score. On the other hand, Bitcoin shows good performance on five different parameters, as supported by its trust level score. Ethereum ranks fourth, performing poorly on three independent trust factors. These observations highlight that the higher the number of poorly performing instances, the lower the trust and adoption intentions for a given BCT product.

The areas of poor performance identified in the assessment suggest that developers need to address specific weaknesses in their BCT products to improve their overall adoption potential. Eliminating or significantly reducing trust factor weaknesses is crucial for increasing the likelihood of widespread acceptance and adoption of blockchain technology. For instance, blockchain technology is primarily used in cryptocurrency, with a small group of individuals significantly influencing the market and its social image. [Bloomberg (2021a)](#Bloomberg2021). As a result, their single comment about a cryptocurrency can cause a sudden price fluctuation for that product [Bloomberg (2021b)](#BloombergEG2021). Failure to avoid conflict of interest among the small group of individuals could harm the company and investors, which, in turn, would tarnish the reputation of BCT, despite having no technical faults. As a real-world illustration, the price-to-post ratio of Elon Musk’s tweets is given in the [figure 15](#fig15) [Molla (2021)](#Molla2021).

A graph with text and numbers

Description automatically generated with medium confidence

Figure 15: Elon Musk Effect on Bitcoin Market

This high volatility and susceptibility to sudden changes in BCT need to be solved to gain universal trust and be widely used as a substitute for fiat money like the US dollar. In addition, BCT’s anonymity is a challenge for criminals, leading to activities like money laundering, gambling, ransomware attacks, and fraud. Lastly, popular BCT-based cryptocurrencies like Bitcoin, Dogecoin, and others use proof-of-work (PoW) as a trustless and decentralized validation process. It requires high validation times, processing power, and high-end configurations for mining Bitcoin [Gonzalez (2022)](#Gonzalez2022). However, recent technologies have introduced proof-of-stake (PoS) to solve the mentioned issues. Despite these advantages, PoS-based BCT products have faced criticism due to less security and decentralization compared to PoW-based ones [Daugherty (2022)](#Daugherty2022).

In conclusion, the lack of a universal embrace of blockchain can be attributed to varying levels of trust and adoption intention among different BCT products. By using our BCT-IATI Unified Model, specific areas of poor performance have been identified, providing valuable insights for developers to enhance their products and improve adoption prospects. Addressing these weaknesses will play a vital role in increasing the overall adoption and success of blockchain technology in various industries and applications.

## **Statistical Analysis**

[Table 8](#table8) represents the summary of our assessment of each blockchain-based technology (BCT). The table shows that Bitcoin holds a huge user base among the entire blockchain user base. Since bitcoin is relatively older than any other BCT, it has faced a lot of ups and downs. It gained huge popularity for its huge potential but lost significant trust over the years due to several hacking attacks, data loss threats, etc. The current trust level of Bitcoin is 46.915% (about 50%) according to our measurement, and the slow increase in the userbase validates the trust level of Bitcoin. The second BCT, Ethereum, is relatively newer than Bitcoin, but it gathered more trust by introducing a proof-of-stake model as well as smart contracts, which are less power-consuming and more efficient, which attracted its user base. On the other hand, with evidence of hacking attacks and proof-of-stake being a centralized system, Ethereum gained some criticism. That is why the trust level of Ethereum is higher than average (55%). Solana, which launched two years ago in 2020, is one of the most recent BCTs, with a 20 million-strong active user base. A feature known as ‘‘proof-of-history, ‘which uses hashed timestamps to verify when transactions occur, improves Solana`s proof-of-stake (PoS) blockchain. That is why the trust level in Solana is high (68%). It was the first blockchain based on a popular meme with a very short transaction period. But things got out of control when the fraudster took advantage of the hype and fooled innocent new users into investing in their fraud scheme. When users realized that the Dogecoin hype was caused by a misinterpretation of Elon Musk’s joke on Saturday Night Live and that fraudsters took advantage of it, the number of users dropped dramatically. So now the trust level of Dogecoin is less than average (45%). The second-last user base, according to our assessment, is Axie Infinity, which is a game based on blockchain technology. Players can use blockchain-based cryptocurrency to collect and sell various fantasy creatures (NFTs). In a nutshell, Axie Infinity gained high trust among the gamer and investor user bases, which is also reflected in our evaluation with a trust level of 50%. Unlike Axie Infinity, Social NFT does not have any gamers as users. That is why the actual user base is much lower than all the products mentioned by BCT. Since the technology is still new, the number of discovered threats is also very low. That is why the score is 59.37%, which is more than average. The final score vs. BCT product graph is given in [figure 16](#fig16) :

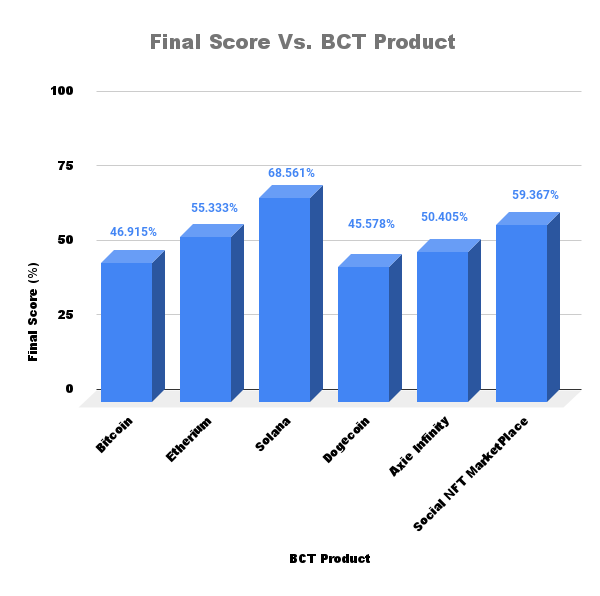


Figure 16: Final Score of BCT Products

By considering all the trust factors in the BCT-IATI framework, a correlation diagram is developed to indicate the relationship between two trust factors. The strength of the relationship among the factors is represented within the -1 to +1 range. The correlation value of 0 represents the neutral relationship between two trust factors, whereas the positive values up to +1 indicate a positive effect, and the negative values up to -1 indicate a negative effect. The correlation value ±0.5 up to ±1 represents a strong relationship between the two parameters and 0 up to ±0.4 represents a weak relationship.

A screenshot of a graph

Description automatically generated

Figure 17: Correlation between factors

## **Recommendations**

The following steps can be taken to reduce the risks of BCT products:

* To address the effect of a group of small individuals mentioned in [section 5.3](#elonmuskeffect), a protocol could be implemented to prevent the manipulation of the entire BCT-based cryptocurrency market, similar to the “Dodd-Frank Act” for the stock market [Hayes (2010)](#HayesA2010). It will ensure both product stability and overall improvement while tackling potential controversies. Another way to handle individual influence on crypto market is by maintaining a balanced professional relationship, avoiding conflicts of interest, and effectively managing demand.
* To ensure reliability and user anonymity, a protocol approved by governments worldwide should be developed to eliminate these criminal activities mentioned in [section 5.3](#crimes).
* The blockchain market is not self-sustaining, leading to price fluctuations in BCT products. Investors should seek professional advice before investing. BCT prices are heavily influenced by social influencer feedback and promotions, creating market hype. Users should evaluate the quality of these promotions. As BCT products gain popularity, fraudulent schemes may attempt to exploit hype, so users should exercise common sense or seek professional advice.
* BCT product developers should provide comprehensive, user-friendly news, offers, risks, and updates to prevent third-party scams and ensure consumer safety and security by addressing potential risks in product features.
* Social influencers play a crucial role in the BCT market, adhering to principles like understanding concepts, features, risks, and ethical implications, and providing genuine feedback based on personal experience.
* Lastly, achieving a balance among security, cost, and power consumption is crucial for BCT to realize its full potential on a global scale.

## **Limitations And Future Works**

Due to a lack of time, only two popular adoption theories were analyzed: ‘‘Protection Motivation Theory” (PMT**1**) and “Technology Acceptance Model” (TAM2) to develop a framework where PMT focuses on the threat and security of a technology while TAM focuses on the user perspective of a technology. While assessing the BCT, it was realized that one of our trust factors, job relevance, could not be properly determined without the primary data from the user community of people using the BCT in their personal day-to-day lives. That is why the effect of the factor trust level was omitted, which was in our primary evaluation model. Besides, there were some more factors (reward, response cost, accuracy, consistency from PMT, gender, and output quality from TAM) that were not added due to lack of time and their effect on our new framework.

It should be noted that while the BCT-IATI framework can provide the reason for a specific trust level and show the developer which features should be fixed, added, or updated to make a BCT ideal, the practical implementation must be done by the developer and approved by the majority of BCT users. Research question 2 was not answered completely due to a lack of real data on framework effectiveness. As originally planned, after implementation, the framework will be tested by industry experts to assess the correctness of the research model. However, due to time constraints, the evaluation cannot be performed at this time. Some BCT investors and users were interviewed, but due to communication gaps and the very low number of volunteers, the volunteers were not qualified to justify themselves as professionals, and the feedback was not effective at all. To provide long-term general trends rather than accurate short-term price forecasts, the BCT-IATI model attempts to estimate trust levels based on the most recent reviews of specific BCT products. For similar reasons, research question 3 was not answered, even though it was partially answered in the recommendation portion. Finally, for a given technology, BCT-IATI frameworks rely directly on the sentiment of inputs from different text sources, each input having a unique impact on different levels of trust.

# **Conclusion**

The study started with some main questions to be answered, including the factors that play key roles in people`s decisions about a new technology when it’s available to use, finding a proper framework that can accurately and successfully judge a blockchain technology-based product, and finding out whether it is expected to be accepted or rejected in the enterprises.

That will lead to the possible conclusion of finding out those factors that are causing negative impacts in the growth of blockchain-based technology products, which are believed to have a potential impact on society in the near future. While finding out the answers to the first main question, this study integrated various versions of the TAM and PMT models to develop a unified model that can assess the level of trust in any blockchain-based product. The study also found some other existing theorems that discuss and figure out some other factors that influence potential users to make decisions when they are about to accept or reject a new technology in some other respects. The results of this study demonstrate factors that play an important role in determining whether a blockchain-based product will be accepted by its target audience. Also, some suggestions have been made to neutralize the negative impact of these factors, which are believed to have a positive impact on the adoption rate of blockchain-based products. Since one of the main parts of our research is to provide a suitable framework for evaluating blockchain-based products, we will examine these for specific blockchain products, as briefly described in the [methodology](#methodology) section. This helps us evaluate these product-related factors more accurately in order to get the right output from the BCT-IATI framework.

# **Appendix**

Table 10: Definitions and examples of all parameters

|  |  |  |
| --- | --- | --- |
| **Trust Factor** | **Definition** | **Example** |
| **Threat Severity (TS)** | The measure of how acute the threat’s consequences are known as threat severity. In other words, a threat can potentially cause harm to the user while using the technology. The level at which the threat originated from that technology is affecting the user negatively will be called threat severity. | A San Francisco programmer named Stefan Thomas has 7,002 Bitcoins worth over $300 million that he cannot access because he lost the password to his digital wallet [Degirmenci and Barros (2023)](#Degirmenci2023). Here, by using blockchain, a user has the vulnerability of losing their data and money, which is a risk. The $300 million dollar loss of bitcoins is called thread severity. |
| **Threat Vulnerability (TV)** | The probability of the success of a threat is called threat vulnerability. | Approximately 20% of all Bitcoins currently in existence appear to be in stranded or lost wallets [Popper (2021)](#Popper2021). Here, the threat of data loss is able to affect 20% of the total standard wallets. The 20% loss of total bitcoin is a threat vulnerability. |
| **Threat Appraisal (TA)** | Threat severity and threat vulnerability are called threat appraisal together. It is a measure of the threat of a particular system by analyzing its intensity and the likelihood of successful occurrence of that threat. |  |
| **Fear Appeal (FA)** | Threat appraisal plays a major role in defining the trust level in blockchain technology. Performing security behaviors is also ascribed to fear appeals because while assessing threat vulnerability and severity, individuals often feel afraid and discomfort, which causes them to become nervous, anxious, and uncomfortable. These cognitive processes of threat create fear of blockchain that reduces the intention to use blockchain, thus reducing the trust level of blockchain. |  |
| **Response Efficacy (RE)** | It is described as the user’s or client’s beliefs or trust as to whether the system’s preferred protective actions/measures are effective against possible threats or unexpected situations. | Approximately 20% of all Bitcoins currently in existence appear to be in stranded or lost wallets. The blockchain infrastructure was originally utilized by Bitcoin, the first digital currency ever created. It is produced in a transaction log with networked computer participation [Böhme, Christin, Edelman, and Moore (2015)](#Bohme2015). By prohibiting fraudsters from using the currency more than once, this blockchain offers one of the greatest security mechanisms [M. A. Fauzi, N. Paiman, and Z. Othman (2020)](#MAFauzi2020). The built-in security mechanisms are called response efficacy since that ensures protection against fraudsters and the risk of data loss. |
| **Self-Efficacy (SE)** | It is described as the user’s or client’s beliefs to have his own ability to perform that preferred action effectively to overcome threats or unexpected situations. | The Bitcoin platform has greatly facilitated and increased the independence of bitcoin trading and transaction while protecting user privacy. Some claim that using this manner of payment gives them the freedom and anonymity to transact [M. A. Fauzi, N. Paiman, and Z. Othman (2020)](#MAFauzi2020). |
| **Coping Appraisal (CA)** | Response efficacy and self-efficacy are collectively known as coping appraisal. While using a system, there are some protective actions/measures provided with the system to effectively against the threat. Now the trust in how effectively the threat can be eliminated by preferred protective measures and how effectively the user can have protective measures is called coping appraisal. | A user who is confident in the security features of a blockchain system and their own ability to use those features effectively will have a high coping appraisal. |
| **Maladaptive Coping (MC)** | When the user has uncertainty about the effectiveness of protective measures and their own ability against the threat, the user tends to reduce the intention to adapt to the new technology. This is called maladaptive coping. | A user who is unsure of how to use the security features of a blockchain system or is concerned about their ability to protect themselves from cyberattacks may have maladaptive coping. |
| **System Complexity (SC)** | System complexity is a measure that defines the degree of complexity required to implement and maintain the system during changes. It directly affects the intention to use blockchain. A sophisticated system should have an optimal amount of complexity, otherwise, the system will not be feasible for the developer or user. | Even for experts in the blockchain field, the Bitcoin system can be complex and challenging to understand. This complexity can make it difficult for users to trust and use the system. [Fry (2016)](#FryJ2016); [Fauzi et al. (2020)](#MAFauzi2020) |
| **Perceived Usefulness (PU)** | It assesses the degree of usefulness perceived by the user before and after utilizing technology in their daily lives. Perceived usefulness is determined by measuring performance verifiability, job relevance, social influence, image, and experience. Perceived usefulness influences the intention to use blockchain. |  |
| **Coping Appraisal (CA)** | Response efficacy and self-efficacy are collectively known as coping appraisal. While using a system, there are some protective actions/measures provided with the system to effectively against the threat. Now the trust in how effectively the threat can be eliminated by preferred protective measures and how effectively the user can have protective measures is called coping appraisal. | A user who is confident in the security features of a blockchain system and their own ability to use those features effectively will have a high coping appraisal. For example, a user who understands how to use multi-signature wallets and two-factor authentication will have a higher coping appraisal than a user who does not. |
| **Maladaptive Coping (MC)** | When the user has uncertainty about the effectiveness of protective measures and their own ability against the threat, the user tends to reduce the intention to adapt to the new technology. This is called maladaptive coping. | A user who is unsure of how to use the security features of a blockchain system or is concerned about their ability to protect themselves from cyberattacks may have maladaptive coping. For example, a user who has heard stories of people losing their bitcoins due to hacks may be hesitant to use blockchain technology. |
| **System Complexity (SC)** | System complexity is a measure that defines the degree of complexity required to implement and maintain the system during changes. It directly affects the intention to use blockchain. A sophisticated system should have an optimal amount of complexity, otherwise, the system will not be feasible for the developer or user. | Even for experts in the blockchain field, the Bitcoin system can be complex and challenging to understand. This complexity can make it difficult for users to trust and use the system. For example, a user who does not understand how blockchain works may be less likely to use it than a user who has a better understanding of the technology. |
| **Perceived Usefulness (PU)** | It assesses the degree of usefulness perceived by the user before and after utilizing technology in their daily lives. Perceived usefulness is determined by measuring performance verifiability, job relevance, social influence, image, and experience. Perceived usefulness influences the intention to use blockchain. | A user who believes that blockchain technology can be useful to them in their daily lives is more likely to trust and use it. For example, a user who wants to make secure and anonymous payments may find blockchain technology to be useful. |
| **Performance Verifiability (PV)** | It measures the degree of precision with which the performance of technology can be evaluated and justified. It affects the perceived usefulness. | Blockchain transactions are verifiable because the user can track their origin. This verifiability can increase the perceived usefulness of blockchain technology for users. For example, a user can be confident that their blockchain transactions will be processed and recorded accurately. |
| **Job Relevance (JR)** | It defines how appropriate the system is for the user according to the user’s job. It influences the perceived usefulness. | A user who works in a field where blockchain technology is commonly used, such as finance or technology, may find blockchain technology to be more relevant to their job. This increased relevance can increase the perceived usefulness of blockchain technology for users. For example, a software developer who is working on a blockchain-based application may find blockchain technology to be very relevant to their job. |
| **Social Influence (SI)** | It defines how popular the technology is among the users and social influencers. It can be both positive and negative. | The popularity of blockchain technology among other users and social influencers can have a positive impact on the perceived usefulness of blockchain technology. For example, if a user sees that their friends and colleagues are using blockchain technology without any problems, they may be more likely to trust and use it themselves. |
| **Behavioral Intention (BI)** | The perceived usefulness and performance expectancy of the user will create a specific attitude toward using the piece of technology. That attitude could be a positive attitude or a negative attitude, which will be significantly affected by social influence. The behavioral intention will also affect the intention to use blockchain. | A user who perceives blockchain technology to be useful and easy to use is more likely to have a positive attitude towards it and have a higher behavioral intention to use it. For example, a user who wants to make fast and secure international payments may find blockchain technology to be useful and easy to use, and therefore have a higher behavioral intention to use it. |
| **Image (Im)** | It reflects a user’s mind for the application of technology before they use it. The image is created by analyzing a review of existing users of the technology. The image can affect both perceived usefulness and social influence. When a user wants to use a new technology, firstly he will search on reliable sources to see the expert opinion about the specific technology. Even the user can take information from the blog site. After that, the user will summarize all the information and decide about the particular technology and whether he will use it or not. | Last year, a burglar used the bridge to steal almost $610 million from Poly Network. And barely two months ago, the $325 million bridge of the decentralized finance (DeFi) platform Wormhole was compromised. In the case of Axie/Ronin, the network's owner did not even become aware of the breach for approximately a week. Or, if it did, it chose to wait before making an official announcement: Six full days after the assailant stole the money, on March 29, a blog entry detailing the losses was published [Gottsegen (2022)](#Gottsegen2022). The lack of accountability on the part of Axie infinity's creator gives the user base a bad **image**. |
| **Experience (Ex)** | After using technology, a user develops a perception of it, which is known as experience. Experience can be positive or negative. A user having a positive experience tends to use similar technology throughout their life cycle without exception. | Hashcash, a digital currency created in the middle of the 1990s and used before bitcoin, was among the most popular. Hashcash was created to stop DDoS assaults and reduce email spam, among other things ([Blockchain.com, Full-Access Account Limits for Depositing and Withdrawing, 2022)](#Blockchain2022). The features of Hashcash created a positive **experience**, which will ultimately encourage the experienced user to use similar types of technologies like bitcoin. |
| **Effort Expectancy (EE)** | It defines how much effort is going to be needed to use the technology to get benefit from that technology. | Besides the initial investment in hardware, the most significant expense a miner incurs is the cost of energy ([Hayes A. S. (2017)](#HayesA2017); [O'Dwyer & Malone (2014)](#ODwyer2014)). It has been discovered that mining digital money consumes more electricity than the prices offered for solving a block. Cryptocurrency mining has consumed an enormous amount of electricity. The mining cost is dependent on the performance of the hardware. According to studies, the electricity created by cryptocurrency mining ranges from 10 to 100 MW (equal to a small power plant) to 3 to 6 GW (the estimated amount of energy utilized by small to medium-sized nations such as Bangladesh and Denmark) ([Vranken (2017)](#Vranken2017); [M. A. Fauzi, N. Paiman, and Z. Othman, (2020)](#MAFauzi2020)). The required investment for bitcoin is called **effort expectancy**. |
| **Intention to Use Blockchain Technology (IB)** | Perceived usefulness, maladaptive coping, fear and behavioral intention, social influence and system complexity all influence the intention to use BCT and it directly influence the trust level of BCT. | A user who perceives blockchain technology to be useful, has low maladaptive coping, low fear, high behavioral intention, is influenced by positive social influence, and finds the system to be of optimal complexity is more likely to have a high intention to use blockchain technology. For example, a user who is confident in their ability to use blockchain technology, has seen their friends and colleagues using blockchain technology successfully, and finds the system to be easy to understand is more likely to have a high intention to use blockchain technology. |
| **Trust Level of Blockchain Technology (TL)** | It is the final parameter that indicates the percentage of trust level depending on the intention to use BCT. | A user with a high intention to use blockchain technology is more likely to have a high trust level in blockchain technology. For example, a user who is actively using blockchain technology to make payments and store their assets is more likely to have a high trust level in blockchain technology. |

# **References**

Aggarwal, S., & Kumar, N. (2021). Blockchain 2.0: Smart contracts. In S. Aggarwal, N. Kumar, & P. Raj (Eds.), *Advances in Computers* (Vol. 121, pp. 301–322). Elsevier.

Alphand, O., Amoretti, M., Claeys, T., Dall'Asta, S., Duda, A., Ferrari, G., Zanichelli, F. (2018). IoTChain: A blockchain security architecture for the Internet of Things. *2018 IEEE wireless communications and networking conference (WCNC)*, (pp. 1–6).

Alshammari, S. H., & Rosli, M. S. (2020). A review of technology acceptance models and theories. *Innovative Teaching and Learning Journal (ITLJ), 4*, 12–22. Retrieved from https://www.researchgate.net/publication/347439493\_A\_Review\_of\_Technology\_Acceptance\_Models\_and\_Theories

Bajpai, P. (2015). Countries where Bitcoin is legal and illegal. *Countries where Bitcoin is legal and illegal*. Investopedia. Retrieved from https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp

Balasubramanian, S., Shukla, V., Sethi, J. S., Islam, N., & Saloum, R. (2021). A readiness assessment framework for Blockchain adoption: A healthcare case study. *Technological Forecasting and Social Change, 165*, 120536.

Bitcoin.org. (2022). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

Blockchain.com. (2019). Blockchain Market Cap. *Blockchain Market Cap*. Retrieved from https://www.blockchain.com/charts/market-cap

Blockchain.com. (2022). Full-Access Account Limits for Depositing and Withdrawing. *Full-Access Account Limits for Depositing and Withdrawing*. Retrieved from https://support.blockchain.com/hc/en-us/articles/360040015091-Full-Access-Account-Limits-for-Depositing-and-Withdrawing

Bloomberg. (2021). Bitcoin declines after Tesla CEO Elon Musk hints that prices are excessive. *Bitcoin declines after Tesla CEO Elon Musk hints that prices are excessive*. Business Standard. Retrieved from https://www.business-standard.com/article/international/bitcoin-declines-after-tesla-ceo-elon-musk-hints-that-prices-are-excessive-121022300083\_1.html

Bloomberg, E. G. (2021, October). Bitcoin is still concentrated in a few hands, study finds. *Time*.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives, 29*, 213–238.

Buterin, V., & others. (2014). A next-generation smart contract and decentralized application platform. *white paper, 3*, 2–1.

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies. *Hawaii International Conference on System Sciences*, (pp. 1-10). doi:10.1109/HICSS.2009.74

Cheung, A., Roca, E., & Su, J.-J. (2015). Crypto-currency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices. *Applied Economics, 47*, 2348–2358.

CoinDesk. (2018). ICO Tracker. *ICO Tracker*. Retrieved from https://www.coindesk.com/ico-tracker/

Crypto market cap and DeFi market cap charts —. (n.d). *Crypto market cap and DeFi market cap charts —*.

Daugherty, B. (2022, September). Proof-of-stake is proof of misunderstanding - CoinGeek. *Proof-of-stake is proof of misunderstanding - CoinGeek*. CoinGeek. Retrieved from https://coingeek.com/proof-of-stake-is-proof-of-misunderstanding/

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319–340.

De Vries, A. (2018). Bitcoin's Growing Energy Problem. Joule, 2 (5), 801-805. *URL: https://www. sciencedirect. com/science/article/pii S*.

Degirmenci, K., & Barros, A. (2023). How secure is blockchain? Extending the protection motivation theory with trust. *How secure is blockchain? Extending the protection motivation theory with trust*. ResearchGate. Retrieved from https://www.researchgate.net/publication/353947141\_How\_Secure\_Is\_Blockchain\_Extending\_the\_Protection\_Motivation\_Theory\_with\_Trust

Drake, R. R. (2018). *Site Occupancy Analysis of the Sagebrush Lizard (Sceloporus graciosus) in the Disappearing Desert-Scrub of the Columbia Basin.* Ph.D. dissertation, Western Washington University.

Frankenfield, J. (2017). Merkle Tree. *Merkle Tree*. Retrieved from https://www.investopedia.com/terms/m/merkle-tree.asp

Fry, J., & Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis, 47*, 343–352.

Gartner. (2018). Organizations' Blockchain Plans. *Organizations' Blockchain Plans*. Retrieved from https://www.gartner.com/newsroom/id/3873790

Gonzalez, O. (2022, July). Bitcoin mining: How much electricity it takes and why people are worried. *Bitcoin mining: How much electricity it takes and why people are worried*.

Gottsegen, W. (2022, April 04). *Coindesk*. Retrieved from Nasdaq: https://www.nasdaq.com/articles/the-bigger-problem-with-axie-infinity#:~:text=On%20March%2023%2C%20%24620%20million,your%20standard%20in%2Dgame%20currency/

Hayes, A. (2010, July). Dodd-Frank act: What it does, major components, and criticisms. *Dodd-Frank act: What it does, major components, and criticisms*.

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics, 34*, 1308-1321. doi:https://doi.org/10.1016/j.tele.2016.05.005

IBM(n.d.). “What is Natural Language Processing?,” Ibm.com. [Online]. Available: https://www.ibm.com/topics/natural-language-processing. [Accessed: 19-Oct-2023].

Imran, M., & Zimmer, M. (2017). Privacy backlash on Google+: The Circles controversy and its implications for user trust in social media. *Computers & Society, 47*, 258–272.

Kish, M., Srinivasan, A., Wortzel, L., Sharma Charge D'affaires, A., Chung, K., Jain, R., . . . Smith, M. M. (n.d.). UN Commission on Science and Technology for Development. *UN Commission on Science and Technology for Development*.

M. A. Fauzi, N. Paiman, and Z. Othman. (2020). Bitcoin and Cryptocurrency: Challenges, Opportunities and Future Works. *J. Asian Finance Econ. Bus., 7*, 695–704.

Mäkitalo, N., Ometov, A., Kannisto, J., Andreev, S., Koucheryavy, Y., & Mikkonen, T. (2017). Safe, secure executions at the network edge: coordinating cloud, edge, and fog computing. *IEEE Software, 35*, 30–37.

Mappo. (2019, December). Top 10 Tech Giants are Diving into Blockchain - aelf - Medium. *Top 10 Tech Giants are Diving into Blockchain - aelf - Medium*.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research, 2*, 173–191.

Molla, R. (2021, May). Chart: How bitcoin prices move with Elon Musk's tweets. *Chart: How bitcoin prices move with Elon Musk's tweets*.

Nakamoto, S. (2009). Nakamoto, S, Bitcoin: A peer-to-peer electronic cash system. *Nakamoto, S, Bitcoin: A peer-to-peer electronic cash system*.

O'Dwyer, K. J., & Malone, D. (2014). Bitcoin Mining and its Energy Footprint. *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014)*. doi:10.1049/cp.2014.0699

Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research Handbook on Digital Transformations* (pp. 225–253). Edward Elgar Publishing.

Popper, N. (2021, January). Lost passwords lock millionaires out of their bitcoin fortunes. *NY Times*.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology, 91*, 93–114.

Salha, R. A., El-Hallaq, M. A., & Alastal, A. I. (2019). Blockchain in smart cities: Exploring possibilities in terms of opportunities and challenges. *Journal of Data Analysis and Information Processing, 7*, 118–139.

Schwartzer, L. A. (2020, April). The $40 trillion problem. *The $40 trillion problem*.

Sharma, T. K. (2018). How Is Blockchain Verifiable By Public And Yet Anonymous? *Blockchain Council, 10*.

Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the origins and variations of blockchain technologies. *IEEE Secur. Priv., 17*, 72–77.

Szabo, N. (1998). Secure property titles with owner authority. *Online at http://szabo. best. vwh. net/securetitle. html*, 1.

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information systems research, 6*, 144–176.

Vafadarnikjoo, A., Ahmadi, H., Liou, J. J., Botelho, T., & Chalvatzis, K. (2021, April). Analyzing blockchain adoption barriers in manufacturing supply chains by the neutrosophic analytic hierarchy process. *Annals of Operations Research*. doi:10.1007/s10479-021-04048-6

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425–478.

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability, 28*, 1–9. doi:10.1016/j.cosust.2017.04.011

Wang, N. (2022, October). Tesla made no changes to its bitcoin holdings in third quarter. *Tesla made no changes to its bitcoin holdings in third quarter*.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*, 329–349.

1. PMT (Milne et al., 2000), Adapted PMT ([Tim Chenoweth et al., 2009](#Chenoweth2009)), Adapted PMT ([Kenan Degirmenci et al., 2021](#Degirmenci2023)) [↑](#footnote-ref-2)
2. TAM ([Fred Davis](#DavisFD1989)), TAM2 ([Venkatesh and Davis, 2003)](#Venkatesh2003), UATUT ([Venkatesh et al, 2003](#Venkatesh2003)) [↑](#footnote-ref-3)