International Journal of Computers and Informatics (IJCI)

Vol. (2), No. (6)

المجلة الدولية للحاسبات والمعلوماتية

الإصدار (2)، العدد (6)

October 2023

"Blockchain Technology Applications and Cybersecurity Techniques: A Literature Review"

Jawad Wazna Ali
Assistant Professor of Information Security, King Abdulaziz University, Kingdom of Saudi Arabia
Jawadwazna77@yahoo.com

Nabil Qassem
Lecturer of Computers, Université de Tunis, Tunisia
qassemabou@utunis.rnu.tn

Abstract:

Blockchain is a relatively novice technology rapidly increasing as a next-generation solution for maintaining digital transactions and record-keeping issues. Blockchain technology can be used in financial services, healthcare facilities, social services, the governmental sector, the Internet of Things (IoT), etc. Regularly any new technologies have some challenges like security risks (threats and vulnerabilities). Among these blockchain challenges is managing the large-scale digital transactional system, which is potentially exposed to a multitude of threats. Thus, this paper introduces the categories of blockchain technologies' cybersecurity vulnerabilities and some aspects of cybersecurity risk assessment.

Keywords: Blockchain Technology, Blockchain Applications, Cybersecurity.

1- Introduction

Incremental dependency on IT in many business domains leads to an increase in IT solutions' importance as a significant factor in business success and sustainability.

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk

E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

IT solutions must have the proper functionality, availability, usability, and security. Most IT solutions give the security factor little weight. So many researchers highlight a security issue and the associated risks as an important concern. From this point, the researchers should evaluate and assess the risks and threats associated with any solutions.

Risk is a universal term, and it has a direct relation to day-to-day tasks 'The term risk is used in a variety of contexts and domains' A risk assessment is the examination of a business's assets, the threats to those assets and the adequacy of the controls in place to protect them from misuse or compromise.

Risk assessments are the foundation of every security best practice and are the first step in the formulation of an effective risk management program (Turstwave Resource Library,2017). However, the researcher can predict, prevent, and reduce its consequences by applying analysis techniques and rational decision-making methods.

Risk analysis includes processes such as identification of activity, threat analysis, vulnerability analysis, and guarantees. Risk analysis is one of the completed phases in the information security risk assessment process. It required to do strategies as a part of Information Security Risk Management (ISRM) (as shown in Fig.1) requires wellsprings of exact information, measurable quantities of unforeseen occasions, and so forth to assess and acquire precise outcomes.

Moreover, chances evaluation is a multifaceted activity requiring numerous parameters, and many of those are hard to measure. The risk assessment process consists of gathering relevant information, risk analysis, and evaluating, to obtain the best possible decision basis regarding planned activities.

E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

International Journal of Computers and Informatics (IJCI)

Vol. (2), No. (6)

المجلة الدولية للحاسبات والمعلوماتية

الإصدار (2)، العدد (6)

October 2023

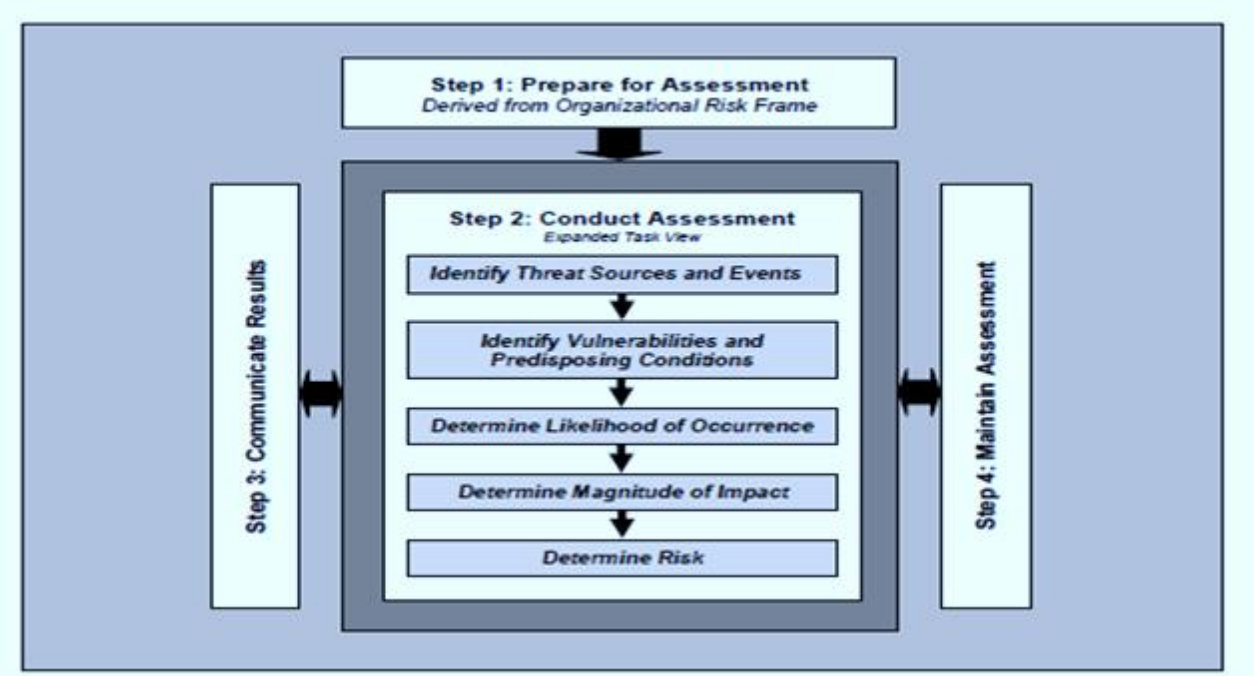

Figure 1: NIST Publication 800-30 Risk Assessment Process (Rebecca and Patrick, 2012)

One of the latest IT solutions that requires information security risk management (ISRM) and is considered not only as an innovative technology but as a potential revolution for the world of business is Blockchain. The term "Blockchain" is especially used when talking about cryptocurrencies, of which bitcoin, the one which pioneered this technology, is certainly the most known.

Nowadays, however, the Blockchain has already become one of the most interesting areas of research in academics, companies, and investors not only operating in the finance area, but also in many other domains: e.g., scientific, social, humanitarian, medical, and so on. However, with the increasing use of Blockchain, the number and

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk

E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

severity of security accidents will go hand in hand (Legal News & Analysis, Asia Pacific, Banking & Finance, 2018).

To give an idea of the seriousness of the damage, the analysis published estimates that, only in 2017, consumers in Blockchain sector lost nearly 490 million dollars. The cause of the incidents was multiple, from wallet theft to software vulnerabilities. Similarly, Blockchain Graveyard1, which is a list of all massive security breaches or thefts involving Blockchain, calculated from publicly available data that since 2011 there have been 58 incidents (Giacomo et al., 2018).

2- Background

In this section, we introduce the basic Blockchain technological aspects constituting the required background. The successful adoption and operation of any new technology are dependent on the appropriate management of the risks associated with that technology (Deloitte, 2018). Distributed ledger technologies (DLT) have the potential to be the backbone of many core platforms soon.

Blockchains or distributed ledger technologies (DLT), were primarily designed to facilitate distributed transactions by removing central management. As a result, blockchains for example could help in addressing the challenges faced by decentralized energy systems. (Merlinda et al. ,2019).

Blockchain/DLT technology has many attractive features, such as decentralization, persistency, anonymity, and auditing. Consequently, these features make Blockchain/DLT a promising solution for many application problems (cryptocurrency and IoT) (Claudio, 2018). Any transfer of value between two parties and the associated debits and credits are captured in the Blockchain ledger for all parties to see. The cryptographic consensus protocol ensures the immutability and irreversibility of all transactions posted on the ledger.

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

3- Quantitative and Qualitative Risk Assessment Methods

Any organization can use quantitative and /or qualitative analysis methods as fundamental methods in risk analysis. But there are some Advantages and disadvantages of both information risk assessment methods (as shown in Table 1), (Stroie, 2011).

Quantitative, where estimation of chance esteem relates to the application of numerical measures – esteem of resources is characterized in sums, the recurrence of threat occurrence within the number of cases, and helplessness by the esteem of likelihood of its loss, those strategies present results within the shape of markers.

Qualitative description of assets' value, determination of qualitative scales for the frequency of threat occurrence and susceptibility for a given threat, or description of so-called threat scenarios by prediction of the main risk factors.

Table 1. Advantages and disadvantages of quantitative and qualitative methods (Stroie, 2011)

Quantitative Methods	
Advantages	• It allows for the definition of the consequences of incidents occurrence in quantitative way. • The realizations of costs and benefits analysis during the selection of protections. • It obtains more accurate image of risks
Disadvantages	• Quantitative measures must depending on the scope and accuracy of defines measurement scale. • Analysis's results may not precise and event confusing • It must be enriched in qualitative description • Analysis conducted with the application of those methods is generality more expensive, demanding greater experience
Qualitative Methods	
Advantages	• It allows for the determination of areas of greater risk in short time and without bigger expenditures • Analysis is relatively easy and cheap.
Disadvantages	• It does not allow for the determination of probabilities and results using numerical measures • Costs benefits analysis is more difficult during the selection of protections

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

The researcher will explore information security risk assessment methods and pickup one or more (NIST, MCDA, Attack defense tree, ALE/SLE, CORAS, CIRA,,.), and these methods can be used with quantitative, qualitative or both situations. (Table 2) will describe the previous methods.

4- Multi-Criteria Decision Analysis/ Making (MCDA/MCDM)

MCDM and MCDA are often used interchangeably, set forth seven guidelines for selecting a MCDM methodology (Guitouni & Martel, 1998). Multi-Criteria Decision Analysis has had a lot of amounts of use over the last several decades. It is a role in different application areas has increased significantly. MCDA methods are concerned with the task of ranking a finite number of alternatives.

Applying MCDA techniques in information security includes the following Advantages:

- It can be used in the Information security domain of risk-based decision-making, risk metrics associated with a triplet of threat, vulnerability, and consequences (TVCs) (Alexander et al.,2017). TVC are quantified in their natural units or on a constructed scale and integrated based on values associated with the importance of these metrics to specific goals.
- It has the capability to characterize risk in highly complex and uncertain situations to move from the use of traditional risk assessment to risk-based decision-making that utilizes multi-criteria decision analysis (MCDA).
- Easier to compare alternatives whose overall scores are expressed as single numbers (Linkov et al. 2006).

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

International Journal of Computers and Informatics (IJCI)

Vol. (2), No. (6)

المجلة الدولية للحاسبات والمعلوماتية

الإصدار (2)، العدد (6)

October 2023

Table 2 overview of a set of existing methods with categorization and description (Alireza et al, 2016)

Method	Main Category	Procedure	Description
Attack Trees	Model-based Risk Analysis	Qualitative or Quantitative	The Attack Tree method is constructed from a specific malicious scenario (root node), and allows the analyst to model several actions (leaf nodes) the attacker(s) can perform in order to realize the scenario. The method builds on Boolean logic with "and" "or" gates, and Node values. The method allows for modeling of attacker capabilities and motivation. Applicable in the design phase, or in analysis of major changes to existing systems.
Attack-Defense Trees [	Model-based Risk Analysis	Qualitative or Quantitative	The Attack-Defense tree is an extension upon the Schneierås attack trees, and allows the analyst to add defense nodes into the attack tree.
Annual and Single Loss Expectancy (ALE/SLE)	Standard Risk Analysis (Can be model based)	Primarily Quantitative	ALE/SLE are prevalent quantitative methods for ISRA. The SLE is calculated using asset value (A times exposure factor (EF). The annual rate of occurrence (ARO). The ALE is calculated using SLE times the ARO. ALE/SLE are beneficial in the terms that the results can be used in cost/benefit analysis. Applicable in risk estimation of single and annual losses from security breaches.
Conflicting Incentives Risk Analysis (CIRA)	Standard Risk Risk Analysis	Qualitative	In CIRA, risks are modelled in terms of conflicting incentives between stakeholders and focuses is according to CIRA, when a Risk Analysis stakeholder is in the position to trigger the action an the risk taker would be in disagreement as in the action. The method is built on economic theori (similar to Game Theory). Applicable in scenario analysis of human interactions and incentives. Proposed as an extension of the stakeholder analysis in early phases of the SDLC.
CORAS [53]	Model-Based Risk Analysis	Qualitative or Quantitative	CORAS is a seven-step method for ISRA. It uses its own Risk Modeling language based on UML, both for modeling and communication. CORAS is based on modeling threat scenarios to assets. The models are similar to trees, with an attacker/threat, vulnerabilities, risks, unwanted incidents and impacts to asset. The risk estimation uses qualitative values, but there is room for quantificat
CRA [170]	Simplified Risk Analysis	Qualitative	The CCTA Risk Analysis and Management Method (CRAMM v.5) is a qualitative ISRA method [: CRAMM is sequentially built, first identifying and evaluating assets. Second, assessing threats and vulnerabilities, before combining the risk estimation and evaluation activities into a joint analysis process. Lastly, CRAMM proposes a risk management process. CRAMM is dependent on the software to utilize its full potential.
TAVE Allegro	Standard Risk Analysis	Qualitative	OCTAVE Allegro centers on threat profiling assets. Organizational drivers provide the basis for developing risk measurement criteria. In coarse terms, the method is as follows: identify and profile assets within their containers, identify threats to assets, identify and mitigate risks based on threat information. The method uses threat trees as a part of the process.
FAIR	Model-based Risk Analysis	Primarily Quantitative	FAIR is a method that is the predecessor of the risk taxonomy by The Open Group contains four well-defined factors for each of the loss and probability calculate on. Including ways to measure the different factors and to derive quantitative analysis results.
NSMROS [113]	Standard Risk Analysis	Qualitative or Quantitative	The NSMROS (Norwegian Security Authority Risk and Vulnerability Assessment) approach is a Norwegian approach for asset and object security. The goal of the method is to help organizations conduct risk and vulnerability assessments, and improve their capability to handle risk.
ISO/IEC 27005 [15]	Standard Risk Analysis	Qualitative or Quantitative	ISO/IEC 27005 is the current ISRM standard and details the complete process of ISRM/RA, with activities, inputs, and outputs of each task. The approach is sequential with an extensive appendi which supports the user in scoping, and asset, threat, and vulnerability assessment. It centers on assets, threats, controls, vulnerabilities, consequences, and likelihood.
NIST SP 800-30 rev.1 [37]	Standard Risk Analysis	Qualitative or Quantitative	NIST SP 800-30 is a sequential method and a threat-centric method, which suggests a threat-based approach to risk, instead of asset-based approach. SP 800-30 actively makes use of the risk framin components from NIST 800-39 [103]. It supports both types of probability estimations or hybrid. The method allows for different risk models, and the components of the estimation output are dependent on the chosen model.
MCDA	Model-based	Quantitative	Multi-Criteria Decision Analysis, or *MCDA*, is a valuable tool that we can apply to many complex decisions. It is most applicable to solving problems that are characterized as a choice among alternatives Risk Analysis

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk

E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

- Choice of an alternative can be transparent if the highest scoring alternative is chosen (Linkov et al. 2006)
- Does not require the reduction of all criteria to a single unit.

5- Related Work

The content of this section consists of several works that suggest the framework for comparing information security risk analysis methodologies while assessing the way risks are valued and prioritized.

In (JIN-HEE CHO et al. 2016), this survey particularly focuses on how a system security state can evolve as an outcome of cyber-attack-defense interactions. This survey concerns how to measure system-level security by proposing a security metrics framework based on the following four sub-metrics: (1) metrics of system vulnerabilities, (2) metrics of defense power, (3) metrics of attack or threat severity, and (4) metrics of situations. To investigate the relationships among these four sub-metrics, we propose a hierarchical ontology with four sub-ontologies corresponding to the four sub-metrics and discuss how they are related to each other.

In (Alexander A. Ganin et al. 2017), this paper introduces a decision-analysis-based methodology that measures risk, threat, vulnerability, and outcomes through a lot of criteria intended to survey the general utility of cyber security the executives yet there is a requirement for practical, contextual investigation representing the way toward assessing and positioning five cyber security improvement systems options. The proposed system conquers any hindrance between risk assessment and risk management, enabling an investigator to guarantee an organized and straightforward procedure of risk management alternatives.

In (Hamido Fujita et al. 2018), this paper exhibits a technique dependent on granular processing to help leaders in investigating and support decision-makers in analyzing

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

and protecting large-scale infrastructures, or urban areas from external attacks by identifying a suitable partition of the infrastructure or the area under analysis The technique takes a shot at a very constrained arrangement of data identifying with the vulnerabilities of segments, and likelihood data in regards to how vulnerabilities can affect the significant segments and probability information regarding how vulnerabilities can impact the meaningful partitions.

In (Zeinab Amin. 2019), this paper introduces a handy guide for surveying digital dangers, a guide that underlines the significance of building up an organization and culture-explicit risk and resilience model. The analyst built up a structure for a Bayesian system to demonstrate the financial loss as a function of the key drivers of risk and resilience. The researcher used qualitative scorecard assessment to determine the level of cyber risk exposure and evaluate the effectiveness of resilience efforts in the organization. The researcher highlights the importance of capitalizing on the knowledge of experts within the organization and discusses methods for aggregating multiple assessments.

In (Thomas Llansó et al.2019), this paper looks at an approach to employ a set of weighted criteria, where the security engineer design sets the weights based on the organizational needs and constraints. The approach is based on a capability-based representation of cyber security mitigations. The paper talks about a gathering of artifacts that compose the approach through the focal point of Plan Science, inquire about and reports execution comes about of an instantiation artifact. The doesn't investigate ways to join instability and affectability examination into the approach.

In (Marco Rocchetto et al. 2019), this research proposes the appropriation of an asset-driven viewpoint and a model-based approach to SECRA, we distinguish current holes. In specific, we examine (i) CPS (security) modeling languages and methodologies, (ii) vulnerability cost models and the network of public repositories

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

of vulnerabilities, (iii) attacker models and profiles, and (iv) complex cyber-physical attack chains.

In (Ángel J. Varela-Vaca et al 2019), this research proposes a risk assessment method to enable the analysis and evaluation of a set of activities combined in a business process model to ascertain whether the model conforms to the security-risk objectives. To achieve this objective, we use a business process extension with security-risk information to 1) define an algorithm to verify the level of risk of process models; 2) design an algorithm to diagnose the risk of the activities that fail to conform to the level of risk established in security-risk objectives; and 3) the implementation of a tool that supports the described proposal.

In (Justin Fanelli et al 2019), this paper proposes a strategy for deciding and prioritizing the foremost fitting security controls or domestic computing. Using Multi-Criteria Decision Making (MCDM) and subject matter expertise, we recognize, analyze and prioritize security controls utilized by the government and industry to decide which controls can substantively make strides in domestic computing security. We apply our strategy utilizing cases to illustrate its benefits.

In (Tanweer Alam 2019), this research talks about a part of Blockchain (BC) within the Internet of Things (IoT) that could be a novel innovation that acts with decentralized, dispersed, free, and real-time record to store exchanges among IoT hubs. The IoT hubs are distinctive kinds of physical, but keen gadgets with inserted sensors, actuators, and programs and able to communicate with other IoT hubs. The part of BC in IoT is to supply a method to handle secured records of information through IoT hubs.

In (HONGFANG LU et. 2019), the researchers talk about a part of Blockchain innovation that has been created more than ten a long time and has gotten to be a

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

drift in different businesses. As the oil and gas industry is steadily moving toward insights and digitalization, numerous expansive oil and gas companies were working on Blockchain innovation within the past two long time since it can altogether make strides in the administration level, effectiveness, and information security of the oil and gas industry. This paper does a precise audit to talk about the application prospects of Blockchain innovation within the oil and gas Industry.

In (Giacomo Morganti 2019), this research explores the number of threats to Blockchains which may concretely lead to a significant risk of adverse impact (thus Moderate or higher) is 76.47%. Fortunately, for some of the attacks, possible mitigations already exist. Nevertheless, for all the threats, and especially for the remaining 23.53%, it is imperative to examine continuously better approaches of relief and, where conceivable, anticipation. The paper does not examine the countermeasures of those vulnerabilities.

6- Blockchain cyber security attacks

In this section, we address threat events in Blockchain technology (BT) that exploit weaknesses in their communication protocols, design, or implementation. Activities associated with BT are classified into three categories from the viewpoint of the organization and accessibility: (a) the first-generation public Blockchain (Blockchain 1.0), (b) the second-generation public Blockchain (Blockchain 2.0), (c) the third-generation private Blockchain (Blockchain 3.0) the BT vulnerabilities classified as shown in figure 3 (Huru et al. 2019).

The following is a classification of Blockchain risks:

- Blockchain 1.0 And 2.0 General Risks
    a) Double spending.
    b) The 51% attack or Goldfinger.

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

c) Wallet security (private key security).
d) Specific flaw in PoS.
e) Network-level attack.
f) Malleability attack.
g) Real DOS attack against the Ethereum network
h) Specific flaw in DPoS
i) Block producers collude
j) Exploit law voter turnout
k) Attacks at scale

- BLOCKCHAIN 2.0 VULNERABILITIES
  a) Re-entrance vulnerability (DAO attack)
  b) Parity multisig wallet
  c) King of the ether throne
  d) GovernMental
- BLOCKCHAIN 3.0 VULNERABILITIES
  a) Attack against Hyper ledger Fabric
  b) Generals risk on private Blockchain implementation

7- Conclusion

This paper is trying to highlight the impact of a Blockchain security function as well as other functions that may lead to threats. This paper explores the real attacks on blockchain systems. Also, it is crucial to understand the scope and impact of security and privacy challenges in Blockchain to predict the possible damage. Future Blockchain research still promising in different applications. One of the important research topics is Bitcoin because it's used on a daily base in cryptocurrency transactions. Consequently, it will attract industry and academia to conduct more research. But there other domains we can use Blockchain Technology like (IoT, Healthcare, Voting mechanism) still has a remaining challenges and open research

IJCI, VSRP Publishing, UK
https://ijci.vsrp.co.uk
E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

issues needed to be solved .The suggested Blochian Technology future researches is : Healthcare , public sector ,Blockchain as a Service (BaaS),IoT, Energy-aware, large-scale applications, Smart Contracts, Consensus mechanisms.

References

- Turstwave Resource Library (2017). Information Security Risk Assessment -Industry Best Practices to Keep Your Data Secure. Retrieved from https://www.trustwave.com/en-us/resources/library/documents/evaluating-your-it-risk-assessment-process-does-it-stand-up-to-current-best-practices/
- Legal News & Analysis, Asia Pacific, Banking & Finance (2018). Break Through With Blockchain - How Can Financial Institutions Leverage A Powerful Technology? . Retrieved from https://conventuslaw.com/report/break-through-with-blockchain-how-can-financial/
- Giacomo,M ; Enrico,S ; Andrea,B(2018,October). Risk Assessment of Blockchain Technology. In 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), 87 - 96.
- Rebecca M. B.&Patrick D.G. (2012, September). NIST Publication 800-30- Risk Assessment Process, Guide for Conducting Risk Assessments. National Institute of Standards and Technology; U.S. Department of Commerce, Gaithersburg: MD20899-8930 (September2012).
- Deloitte (2018). Risks posed by blockchain-based business models is your organization prepared? Retrieve from https://www2.deloitte.com/us/en/pages/risk/articles/blockchain-security-risks.html .
- Merlinda A., Valentin R., David F., Simone A., Dale G., David J., Peter M.& Andrew (2019). Blockchain technology in the energy sector: A systematic review of challenges Renewable and Sustainable Energy Reviews, and opportunities – Elsevier, 100, 143–174.
- Claudio L., (2018, November). Developing Open and Interoperable DLT/Blockchain Standards. Blockchain Engineering Council; IEEE Blockchain Standards Working Group, 106 - 111.
- Stroie E. R. (2011 December). Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches. Chinese Business Review, Vol. 10, No. 12, 1106-1110.

E-ISSN 2976-9361
https://doi.org/10.59992/IJCI.2023.v2n6p2

- Alireza S.S., Rouzbeh A. b., Mohamed C. (2016). Taxonomy of Information Security Risk Assessment (ISRA) . Elsevier ,Computers & Security Vol 57, 14-30.
- Alexander A. G.,Phuoc Q., Mahesh P., Zachary A. C,.Jeffrey M. K., Dayton M., & Igor L.(2017 Multicriteria Decision Framework for Cyber security Risk Assessment and Management. Wiley Online Library, DOI: 10.1111/risa.12891.
- Linkov I, Satterstrom FK, Kiker G, Seager TP, Bridges T, Gardner KH, Rogers SH, Belluck DA & Meyer A.(2006, March) .Multicriteria Decision Analysis: A Comprehensive Decision Approach for Management of Contaminated Sediments . Cambridge Environmental Inc 26(1):61-78.
- Linkov I, Satterstrom FK, Kiker G, Bridges T, Ferguson E. (2006, December). From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications. Environment International, Elsevier,Vol 32, Issue 8, 1072-1093
- Huru H., Ui-jun B., Mu-gon S., Kyunghee C., Myung-Sup K., (2019, junary). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. The International Journal of Network Management, Vol29, Issue2.1-36.