IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 3 February 2024, accepted 23 February 2024, date of publication 1 March 2024, date of current version 11 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3372578

RESEARCH ARTICLE

Methodological Advancements in Standardizing Blockchain Assessment

HEESANG KIM AND DOHOON KIM
Department of Computer Science, Kyonggi University, Suwon 16227, South Korea
Corresponding author: Dohoon Kim (karmy01@kyonggi.ac.kr)

This work was supported by Kyonggi University Research Grant 2023.

ABSTRACT In the burgeoning landscape of blockchain technologies, the quest for a robust and comprehensive evaluation framework remains an exigent challenge. This study introduces an unprecedented methodology that synergizes the common vulnerability scoring system (CVSS) and the weighting mechanism to evaluate blockchain platforms across the multiple dimensions of mainnet, fungible tokens, and non-fungible tokens, using miscellaneous criteria such as legal compliance and proprietary technology. CVSS is employed to perform a quantitative assessment of blockchain-specific vulnerabilities across various sub-factors, thereby establishing an empirical foundation. Subsequently, the weighting mechanism is used to effectively translating qualitative insights into quantifiable metrics. The introduction of this methodological framework is particularly timely and necessary considering the rapidly evolving landscape of blockchain technology. It promises to standardize the evaluation process, providing a robust foundation for future research, policy-making, and technological advancements in the blockchain domain. Consequently, our study not only fills a critical gap in the current literature but also paves the way for a more systematic and informed approach to blockchain assessment. This dual-tiered approach not only ensures a balanced evaluation, capturing both mechanistic intricacies and human subjectivity, but also renders a highly adaptable and scalable framework. The proposed methodology is anticipated to significantly contribute to the standardization of blockchain evaluation, thereby fostering informed decision-making among stakeholders and catalyzing advancements in the blockchain ecosystem.

INDEX TERMS Analytic process, blockchain assessment, blockchain CVSS, blockchain evaluation, CVSS, decentralization, EthereumPoW, legal compliance, scalability, security, standards.

I. INTRODUCTION

Blockchain technology has attracted significant interest since its inception, and extensive research has been conducted to explore its disruptive potential across a myriad of sectors ranging from finance [1], [2], [3] and healthcare [4] to supply chain management [5] and beyond. As technology advances into increasingly complex territories, the imperative for a robust, holistic evaluation framework becomes ever more acute. Existing methodologies typically offer a unidimensional lens, either focusing on technical specifications or relying heavily on expert opinion, thereby neglecting the multifaceted complexities intrinsic to blockchain systems. Moreover, the absence of a standardized approach hampers comparability and hinders the adoption of superior technologies. It is within this lacuna that the present research is situated, aiming to ameliorate this discrepancy through an innovative, interdisciplinary methodology.

In the swiftly evolving realm of digital assets, a robust, comprehensive, and adaptable evaluation framework is necessary. This need is not just academic conjecture but a practical imperative, as underscored by the International Monetary Fund (IMF)'s recent report, ''Assessing macrofinancial risks from crypto assets'' [6]. The IMF's groundbreaking work with its crypto-risk assessment matrix (C-RAM) marks a crucial step in understanding the sector's vulnerabilities and shaping informed policy responses. However, this macrofinancial lens, predominantly focused on country-specific

The associate editor coordinating the review of this manuscript and approving it for publication was Catherine Fang.

risks, reveals a significant gap in the systematic evaluation of individual blockchain ecosystems, encompassing mainnets and various token types.

Our study addresses this critical gap by introducing a nuanced, multi-criteria evaluation framework that transcends macro-financial considerations. This framework is not only an academic contribution but also a necessary tool in the current landscape of digital assets. By employing a blend of common vulnerability scoring system (CVSS) metrics and a hierarchical process, we provide a comprehensive evaluation mechanism across four major categories: mainnet, fungible token, non-fungible token, and miscellaneous criteria. The importance of this study is manifold. Firstly, it offers regulatory bodies and blockchain developers a rigorous, data-driven methodology for decision-making. In a field where technological advancements occur at breakneck pace, our framework provides a stable foundation for assessing and adapting to new developments. Secondly, the framework's adaptability to different blockchain platforms and scenarios is pivotal. From emerging DeFi projects to established platforms such as Ethereum undergoing significant upgrades (e.g., Ethereum 2.0), our methodology is versatile enough to accommodate and evaluate these diverse contexts. This adaptability is critical for stakeholders who must navigate the complexities of this rapidly changing sector.

A dual-tiered framework is proposed for the comprehensive evaluation of blockchain platforms, amalgamating blockchain CVSS and the hierarchy process. The former provides a quantitative assessment matrix, enabling meticulous scrutiny of blockchain-specific vulnerabilities across a panoply of sub-factors. The empirical foundation of CVSS imparts a level of objectivity, thereby mitigating the idiosyncrasies associated with qualitative assessments. However, technology, by its very nature, is not solely a product of mechanistic functions; human subjectivity and expert insight invariably influence its interpretation and utility. To this end, the hierarchy process is invoked as a complementary tool, designed to collate and quantify expert opinions through pairwise comparisons. The harmonization of these two distinct methodologies engenders a balanced, adaptable, and highly scalable evaluation framework. The proposed framework was evaluated on a case study of EthereumPoW, also known as Ethereum 1.0. The decision to focus on EthereumPoW was strategic, aimed at leveraging historical depth, operational stability, and a rich dataset for a more comprehensive and empirically grounded evaluation. While Ethereum 2.0 undeniably represents the future, its current state of flux and partial implementation make EthereumPoW a more suitable candidate for this study's objectives. The overarching objective is twofold: (i) to provide a comprehensive evaluation matrix that is both empirically rigorous and sensitive to the nuanced perceptions of domain experts; (ii) to contribute to the standardization of blockchain evaluation, thereby serving as a catalyst for informed decision-making among stakeholders and technological advancements within the blockchain ecosystem. The remainder of this paper is structured as follows. Section II elucidates the theoretical underpinnings of both CVSS and the hierarchical process, expounding on their individual merits and limitations. Section III delineates the methodology, offering a step-by-step guide to the evaluative process. Section IV presents a case study wherein the proposed methodology is applied to extant blockchain platforms, subsequently facilitating a comparative analysis. Finally, Sections V and VI conclude the paper, summarizing key findings and describing the limitations of this study to indicate avenues for future research.

In summary, this study endeavors to fill a conspicuous gap in the extant literature by proposing a comprehensive, interdisciplinary approach to blockchain evaluation. Through the integration of CVSS and weighting mechanisms, this study introduces a methodology that captures both the quantitative and qualitative aspects of blockchain technology, helping advance the field toward a more standardized and robust evaluative framework.

II. RELATED WORK

The key points of our research underscore the significance of our methodological advancements. By integrating CVSS metrics with a hierarchical process, we capture the dual nature of blockchain technology, encompassing both its mechanistic functions and the human subjectivity inherent in its use and interpretation. This comprehensive methodology not only helps the standardization of blockchain evaluation but also serves as a catalyst for informed decision-making among stakeholders, propelling technological advancements within the blockchain ecosystem.

As blockchain technology grows in complexity and diverse applications, there is a growing need for a clear and comprehensive evaluation approach [7]. Many current methods of evaluation tend to focus excessively on either numbers (quantitative) or expert opinions (qualitative). To address this, we discuss the CVSS, a well-recognized system used to measure how serious different technology problems (vulnerabilities) are. Originally used in cybersecurity, CVSS provides a score to these problems based on potential severity, potential exploitability, and ease of fixing. This scoring is helpful because it is based on clear rules, making it a fair way to compare different issues. However, CVSS is not perfect as it is strongly focused on numbers without considering a wider perspective, particularly in complex systems such as blockchain. Additionally, only examining individual problems may not provide adequate understanding of how these issues fit together in a bigger system.

Previously conducted studies related to the use of CVSS in various fields are summarized in Table 1. Vilches et al. explored the limitations of CVSS in the robotics domain, proposing a robot vulnerability scoring system (RVSS) [8]. Although this seminal work adapted CVSS to specialized systems, it did not directly apply this system to blockchain technologies. Nevertheless, this methodology can offer valuable insights into tailoring CVSS for blockchain evaluation. Similarly, Shahid and Debar introduced a natural language

TABLE 1. CVSS related work analysis in various fields.

Authors	Title	Characteristics	Limitations/differences from this study
Vilches et al., 2018	Robot Vulnerability Scoring System (RVSS) [8]	Focuses on adapting CVSS to robotics, considering safety aspects and environmental variables.	Limited to robotics; does not directly apply to blockchain.
Shahid & Debar, 2021	CVSS-BERT: Explainable NLP for Severity Scoring [9]	Uses NLP to automate CVSS for efficiency and explainability.	Focuses on automation and explainability but lacks domain-specific adaptations for blockchain.
Keramati, 2016	New Vulnerability Scoring System [10]	Critiques CVSS for its limited score range and proposes a new system considering temporal features.	Proposes a new system, which may not align with the aim of using CVSS for blockchain evaluation.
Le & Hoang, 2018	Security Threat Probability Computation [11]	Introduces a mathematical model based on Markov chain and CVSS for cloud security threats.	Focuses on cloud security and employs mathematical modeling, which may not be directly applicable to blockchain.

processing (NLP) approach to automate CVSS scoring [9]. Although their focus was on automation and explainability, they did not delve into domain-specific adaptations of CVSS, which is a central concern in the present study. Keramati critiqued CVSS for its limited range of scores and proposed a new scoring system that considers both intrinsic and temporal features of vulnerabilities [10]. While such a critique of CVSS is valuable, the proposed alternative system may not align with the research objective of adapting CVSS for blockchain evaluation. Finally, Le and Hoang introduced a mathematical model based on Markov chains and CVSS to compute the probability distribution of cloud security threats [11]. Although they employed mathematical modeling, the focus on cloud security makes their system less applicable to blockchain technology. However, their methodology can be adopted for a more quantitative approach to blockchain vulnerability assessments.

Although existing research offers valuable insights into the applications and limitations of CVSS, its applicability and adaptation to blockchain technologies has not been directly addressed [7]. This gap in the literature underscores the novelty and significance of the present study in tailoring CVSS to the unique characteristics and requirements of blockchain systems. In the context of blockchain technology evaluation, Yang et al provided a focused exploration of security audits in blockchain systems. This research emphasized the critical role of security audits in identifying vulnerabilities within blockchain networks, highlighting common security flaws and proposing mitigation strategies. Although Yang et al.'s work contributed significantly to understanding blockchain security, it primarily concentrated on audit mechanisms and tools.

In contrast, our study expands the scope of evaluation by integrating a novel adaptation of CVSS specifically tailored for blockchain technologies. Our approach transcends the traditional audit focus, offering a multi-dimensional framework that assesses various aspects of blockchain ecosystems, including technical robustness, regulatory compliance, and operational dynamics. This broader perspective is crucial in comprehensively evaluating blockchain platforms, addressing not only security concerns but also the diverse elements that constitute the blockchain ecosystem. Therefore, while Yang et al.'s research provides valuable insights into blockchain security audits, our methodology represents a significant advancement, offering a more holistic and versatile tool for blockchain evaluation. The integration of CVSS into our proposed methodology alleviates the individual limitations of each framework while amplifying their complementary strengths. CVSS provides the empirical backbone, offering an algorithmic, standardized evaluation that mitigates the subjective biases often associated with expert-driven assessments.

In summary, the harmonious amalgamation of CVSS engenders a more balanced, comprehensive evaluation mechanism. This hybrid framework aims to bridge the epistemological gap between quantitative rigor and qualitative insight, thereby fostering a nuanced understanding of blockchain ecosystems. In laying the theoretical groundwork [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22] through an examination of these two methodologies, our research responds to these challenges by introducing an innovative, dual-tiered evaluation framework. This framework synergistically combines the empirical rigor of CVSS with the nuanced insights afforded by a hierarchical process. This approach not only bridges the gap in existing methodologies but also aligns with the broader discourse initiated by influential entities such as the IMF. The IMF's recent focus on macro-financial risks of digital assets, while pivotal, does not address the intricacies of evaluating individual blockchain platforms and ecosystems.

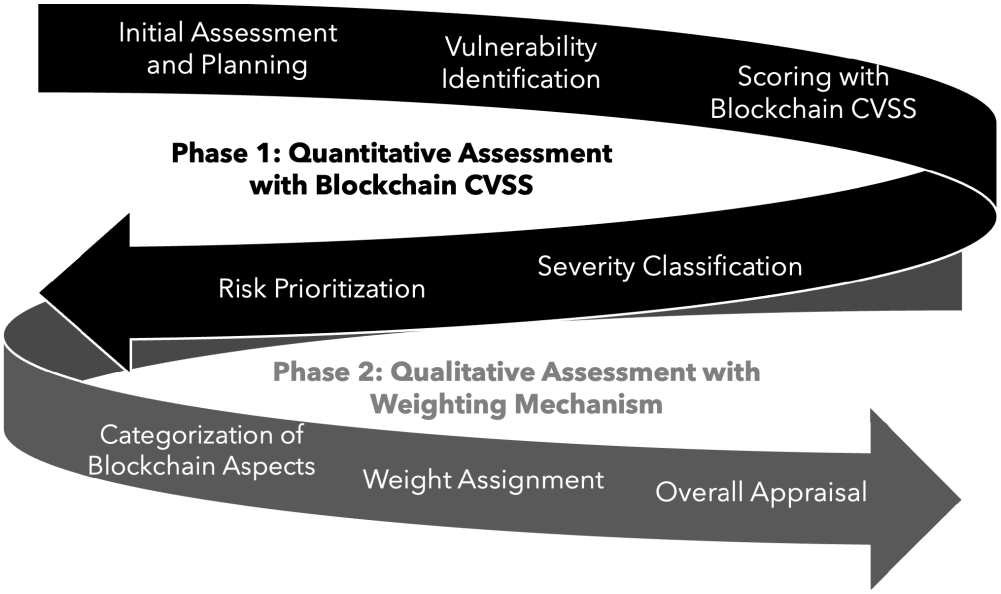


FIGURE 1. Overview of the comprehensive blockchain assessment methodology.

III. METHODOLOGICAL FRAMEWORK FOR A COMPREHENSIVE EVALUATION OF BLOCKCHAINS

The blockchain paradigm, with its expansive scope and continually evolving landscape, presents a compelling yet challenging topic for rigorous academic inquiry. Traditional evaluation frameworks have often fallen short of capturing the multifaceted complexities inherent in blockchain systems. In light of this, the current study seeks to develop an innovative, dual-tiered methodological framework that bridges quantitative and qualitative approaches by integrating CVSS. This section details the nuanced structure and executional steps involved in this comprehensive methodology, elucidating the methods used to address the extant limitations in blockchain assessment.

The methodology for evaluating blockchain platforms is bifurcated into two distinct but interconnected phases: Phase 1 focuses on a quantitative assessment using blockchain CVSS, whereas Phase 2 adopts a qualitative assessment framework augmented by a specialized weighting mechanism (Figure 1). Our new interpretation of blockchain CVSS is summarized in Table 2. The first phase employs a five-step approach tailored to the unique challenges presented by blockchain technology. The process begins with ''initial assessment and planning,'' whereby the scope and methodology for the subsequent security audit are laid out. This is followed by ''vulnerability identification,'' which entails a comprehensive security audit aimed at identifying potential risks and vulnerabilities in the system. The third step, ''scoring with blockchain CVSS,'' quantifies these vulnerabilities by assigning them scores ranging between 0 and 10, thus indicating the severity of each risk within the blockchain ecosystem. The fourth step, ''severity classification,'' categorizes these vulnerabilities into severity levels—critical, high, medium, and low—based on their blockchain CVSS scores. This adds a qualitative layer to the quantitative metrics, offering a nuanced understanding of the risk landscape. Finally, the fifth step, ''risk prioritization,'' ranks the identified vulnerabilities in order of their severity and potential impact, thus providing a roadmap for targeted risk mitigation. The initial phase of the proposed methodology employs CVSS, an industry-standard tool that provides a robust, algorithmic framework for quantitatively evaluating vulnerabilities. The first step involves the meticulous identification of pertinent sub-factors that encapsulate the multifarious characteristics of blockchain platforms. These sub-factors span a range of technical and non-technical aspects, including but not limited to decentralization, scalability, token economy, and legal compliance.

After the quantitative assessment, the methodology transitions into the second phase, delving into qualitative analysis. This phase leverages the scores and classifications obtained from Phase 1 to weight different aspects of blockchain technology, such as decentralization, scalability, resource management, encryption technology, and smart contracts. However, the variations in scale and impact of raw CVSS scores may preclude direct comparisons across different sub-factors. Consequently, normalization of these scores is imperative to ensure a consistent comparative framework. The proposed weighting mechanism typically involves scaling the scores to a standardized range, commonly 0 to 10, through mathematical transformations that preserve the relative distances between scores.

Blockchain CVSS scores function as weight coefficients, influencing the relative significance of each evaluation category in the comprehensive assessment. This approach enables a balanced and empirically substantiated evaluation, allowing

TABLE 2. Blockchain CVSS scoring according to different methodology components.

Methodology Component	Description
CVSS role	CVSS serves as a pivotal element in the evaluation framework, providing an objective measure of vulnerabilities in various aspects of blockchain.
Evaluation categories	The methodology includes a diverse set of evaluation items, categorized under key blockchain facets such as decentralization, scalability, resource management, encryption technology, and smart contracts.
Weighting mechanism	CVSS scores assigned to these categories function as weights, determining each category's relative importance in the final, aggregate evaluation.
Stakeholder implication	The weighted approach enables various stakeholders—ranging from developers to policymakers and investors—to focus on areas that are both critical and impactful, thereby offering a roadmap for targeted improvements and risk mitigation.

stakeholders—ranging from developers and policymakers to investors—to focus their efforts on the most critical and pertinent areas. By integrating these two phases, our methodology offers a holistic framework for the nuanced evaluation of blockchain platforms, thereby paving the way for targeted improvements and effective risk mitigation. This approach should provide a robust and comprehensive methodology suitable for inclusion in a scholarly journal, as it encapsulates both quantitative and qualitative dimensions in the assessment of blockchain platforms.

A. PHASE 1: QUANTITATIVE ASSESSMENT FOR BLOCKCHAIN CVSS

For an effective quantification of the security vulnerabilities in blockchain networks, existing vulnerability scoring systems should be adapted to the nuanced complexities of blockchain technology. Therefore, this study proposes blockchain CVSS as a specialized version of the traditional CVSS v3. In the blockchain CVSS system, the terminology used in standard CVSS scoring is modified to better fit the context of blockchain without altering the fundamental mathematical model. The blockchain CVSS is a pivotal element in the proposed comprehensive methodology designed to assess the security and performance metrics of blockchain platforms. Based on the foundational principles of traditional CVSS, blockchain CVSS has evolved its focus to address the unique challenges and attributes inherent to blockchain technology. Our new interpretation of blockchain CVSS can be expressed in a formula as equation (1) follows. Blockchain CVSS consists of two main components:

1. Blockchain impact metrics:
   A. Confidentiality impact (*BConfImpact*)
   B . Integrity impact (*BIntegImpact*)
   C. Availability impact (*BAvailImpact*)
2. Blockchain exploitability metrics:
   A. Attack vector (*BAttackVector*)
   B. Attack complexity (*BAttackComplexity*)
   C. Privileges (*BPrivilegesRequired*)
   D. User interaction (*BUserInteraction*)

In contrast to CVSS, which offers a broad framework to assess a variety of software vulnerabilities, blockchain CVSS is specifically fine-tuned to evaluate vulnerabilities in key blockchain components such as decentralization, scalability, resource management, encryption technology, and smart contracts. The base score is calculated using the following formula:

$$\begin{aligned} \textit{Blockchain Base Score} = \textit{Roundup}\,(\textit{min}(\textit{Blockchain Impact} \\ + \textit{Blockchain Exploitability}, 10)) \end{aligned} \tag{1}$$

where:

$$\begin{aligned} &\textit{Blockchain Impact} \\ &\quad = 1 - [(1 - \textit{BConfImpact}) \\ &\qquad \times (1 - \textit{BIntegImpact}) \times (1 - \textit{BAvailImpact})]\,, \end{aligned} \tag{2}$$

$$\begin{aligned} &\textit{Blockchain Exploitability} \\ &\quad = 8.22 \times \textit{BAttackVector} \times \textit{BAttackComplexity} \\ &\qquad \times \textit{BPrivilegesRequired} \times \textit{BUserInteraction} \end{aligned} \tag{3}$$

Within the blockchain CVSS framework, each vulnerability is assigned a numerical score ranging between 0 and 10. This score serves as an indicator of the severity of the risk within the blockchain ecosystem. A score of zero implies minimal security risk, whereas a score of 10 represents a critical vulnerability. This scoring mechanism facilitates risk prioritization, thus enhancing the security profile of the evaluated blockchain platform. Beyond numerical scoring, the proposed approach incorporates severity classifications adapted from CVSS version 3, adding a qualitative layer to the quantitative assessment for a more nuanced interpretation of the impact of each vulnerability.

In our blockchain evaluation methodology, blockchain CVSS serves a dual role, not only quantifying the vulnerability levels associated with various facets of blockchain technology but also functioning as a scaling factor in the overall evaluation. Unlike traditional CVSS, which generally evaluates the security of software systems, blockchain CVSS scores are repurposed to act as weight coefficients for different evaluation criteria specific to blockchain. These coefficients proportionately influence the significance of each category in the comprehensive assessment. Consequently, categories with higher blockchain CVSS scores are

allocated greater weight, underscoring the importance of addressing the higher risk posed by the more critical elements. By incorporating the blockchain CVSS scores into the evaluation process as weighting factors, our methodology offers an empirically validated framework for nuanced evaluations. This approach empowers stakeholders—from developers and policymakers to investors—to focus on areas that warrant immediate attention, paving the way for targeted improvements and risk mitigation.

B. PHASE 2: QUALITATIVE ASSESSMENT USING A WEIGHTING MECHANISM

The second phase of the methodology integrates the weighting mechanism using various equations. This mechanism is a decision-making tool revered for its capacity to translate qualitative evaluations into quantifiable metrics. Given the subjective nature of some sub-factors, qualitative assessment is indispensable for a holistic evaluation of blockchain platforms. The first step in this phase entails assembling an expert panel consisting of individuals with a high degree of domain expertise in blockchain technologies and associated fields. After structuring the expert panel, pairwise comparisons are conducted using the weighting mechanism. This involves presenting experts with pairs of sub-factors and eliciting their judgments regarding the relative importance of each. These judgments are then quantified through a structured mathematical process, the core of which involves the calculation of eigenvalues and eigenvectors to derive the weighting of each sub-factor. While the weighting mechanism offers a robust framework for qualitative assessment, it is not devoid of limitations. The process is susceptible to the biases and subjectivities inherent in any expert-driven evaluation. To mitigate this, a sensitivity analysis is generally conducted to assess the robustness and reliability of the expert judgments, thereby enhancing the validity of the qualitative assessment. The computed weights and priorities provide a comprehensive framework for evaluating the critical aspects of the blockchain mainnet. The proposed methodology offers a balanced, empirically substantiated framework conducive to a nuanced evaluation of blockchain platforms. This weighted mechanism allows various stakeholders to focus on critical areas of importance.

Following the individual quantitative and qualitative assessments, the next step involves a weighted aggregation of the scores. Each normalized blockchain CVSS score is multiplied by the corresponding weight derived from the weighting mechanism, and the results are summed to produce a composite score for each blockchain platform. This composite score serves as a comprehensive metric, capturing both empirical vulnerabilities and expert-driven qualitative evaluations. We delineate the specific evaluative dimensions within each overarching category C_n, encompassing the mainnet, fungible token, non-fungible token, and other miscellaneous criteria, as outlined in our comprehensive assessment table.

$$Categories = \{C_1, C_2, \ldots, C_n\} \tag{4}$$

Let C denote the initial matrix, known as the pairwise comparison matrix. In this matrix, each element c_{ij} represents the importance of criterion i relative to criterion j. The diagonal elements are always 1 because any criterion is equally important to itself. The off-diagonal elements are determined based on expert judgments or other methods such that $c_{ji} = {}^{1}/_{c_{ij}}$.

$$C = \begin{bmatrix} 1 & C_{12} & \cdots & C_{16} \\ \frac{1}{C_{12}} & 1 & \ldots & C_{26} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{C_{16}} & \frac{1}{C_{26}} & \cdots & 1 \end{bmatrix} \tag{5}$$

Then, blockchain CVSS is utilized to evaluate the vulnerabilities in each category and assign a score.

$$CVSS_{Blockchain}\ Scores = \{S_1, S_2, \ldots, S_n\} \tag{6}$$

Blockchain CVSS scores are then used to calculate the weights. The next step is to normalize the columns of C in equation (5). Each element in a column is divided by the sum of that column. Let W denote this normalized matrix:

$$W_i = \frac{S_i}{\sum_{j=1}^{n} S_j}, \tag{7}$$

$$W_{ij} = \frac{C_{1j}}{\sum_{k=1}^{n} C_{1k}} \tag{8}$$

The rows in the normalized priority matrix are averaged to obtain the principal eigenvector. A pairwise comparison matrix can then be created using the calculated weights. The resulting vector W represents the weights of the criteria in (9).

$$W = \begin{bmatrix} \frac{1}{n}\sum_{j=1}^{n} \frac{C_{1j}}{\sum_{k=1}^{n} C_{1k}} \\ \frac{1}{n}\sum_{j=1}^{n} \frac{C_{2j}}{\sum_{k=1}^{n} C_{2k}} \\ \vdots \\ \frac{1}{n}\sum_{j=1}^{n} \frac{C_{nj}}{\sum_{k=1}^{n} C_{nk}} \end{bmatrix} = \begin{bmatrix} \frac{1}{n}\sum_{j=1}^{n} W_{1j} \\ \frac{1}{n}\sum_{j=1}^{n} W_{2j} \\ \vdots \\ \frac{1}{n}\sum_{j=1}^{n} W_{nj} \end{bmatrix} \tag{9}$$

The comprehensive analysis of the mainnet presented in the study goes beyond a simple list of indicators and deeply evaluates several aspects of the blockchain network by quantifying the importance of each item and applying weight to it. This approach determines the importance of each item based on security analysis and other relevant in-depth research, rather than simply subjective judgment. The results obtained are detailed in Appendix C, and the data and analysis presented here strongly support that the weights used here reflect important factors in the operation and security of real networks. The composite evaluation is subjected to a sensitivity analysis to ensure the robustness of the scores and gauge the framework's resilience against potential biases or data anomalies. This is crucial for ascertaining the methodological soundness of the evaluation and flagging any areas that may require further scrutiny or revision. The computed weights and priorities provide a comprehensive framework for evaluating the critical aspects of blockchain mainnets. The methodology was tested on EthereumPoW, yielding insightful results.

C. VALIDATION AND ITERATION

The final stage of the methodological framework calls for validation. Given that the value of any theoretical model is determined by its practical applicability, validation typically involves empirical testing through case studies, simulations, or other methodologically appropriate techniques. The framework is designed to be iterative and adaptable to allow a continuum of refinements based on empirical outcomes and evolving domain-specific knowledge.

In this section, we present a comprehensive methodological framework that combines quantitative rigor with qualitative depth. Because our research does not simply discuss the level of evaluation indicators in each field, we present a comprehensive analysis of blockchain technology by conducting a security analysis with deviations in the weight settings. These results shown in Appendix C demonstrate that the importance of the weights we consider in this study. By synergistically integrating blockchain CVSS and the weighting mechanism, the proposed methodology offers a balanced, scalable, and adaptable approach for the nuanced evaluation of blockchain platforms, seeking to address the exigencies of a rapidly evolving technological landscape, thereby filling in the significant gap in the current academic discourse on blockchain assessment. The following sections further elucidate the practical applications of this methodological framework, providing empirical evidence to substantiate the theoretical underpinnings of the proposed system.

IV. CASE STUDY: EVALUATING ETHEREUMPoW USING THE PROPOSED METHODOLOGICAL FRAMEWORK

The burgeoning landscape of blockchain technology encompasses a diverse array of architectures and frameworks, each deserving nuanced scrutiny. EthereumPoW, the first iteration of the Ethereum platform operating on a proof-of-work (PoW) consensus mechanism, is particularly deserving of evaluation. This section elaborates on the applied aspects of the previously delineated dual-tiered methodological framework, employing EthereumPoW as a case study, to empirically substantiate the model's theoretical underpinnings.

A. JUSTIFICATION FOR SELECTING ETHEREUMPoW AS A CASE STUDY

The selection of EthereumPoW for this case study is predicated on a multitude of factors that collectively make it a compelling subject for a comprehensive evaluation of blockchain platforms. EthereumPoW enjoys seminal status in the annals of blockchain technology, serving as one of the first platforms to successfully implement smart contracts. Its pioneering role offers a unique opportunity to examine a platform that has profoundly influenced the trajectory of blockchain innovations. Beyond its historical significance, EthereumPoW is distinguished by its complexity and multifunctionality. It is not merely a transactional platform but supports a broad range of decentralized applications (dApps) and even has its own native cryptocurrency, Ether. This multi-functional nature serves as fertile ground for evaluating the diverse aspects and sub-factors that constitute a blockchain platform, thereby enriching the comprehensiveness of the study. Moreover, EthereumPoW's decentralized architecture, underpinned by its PoW consensus mechanism, offers a robust framework for evaluating the impact of decentralization on elements like security, scalability, and governance. Its widespread adoption across various industries, from finance to supply chain management, also brings an added layer of real-world relevance, enabling the study to bridge the gap between academic theory and practical utility. A further case bolstering its selection is the robustness of the Ethereum community, characterized by active development and high levels of engagement. This dynamism not only ensures that the platform is continually evolving but also provides a wealth of data for empirical evaluation. Additionally, EthereumPoW has attracted significant regulatory scrutiny, making it an ideal candidate for exploring the interplay between blockchain platforms and legal institutional frameworks. Finally, EthereumPoW's role as a benchmark for emerging blockchain platforms underscores its value as a case study subject. A nuanced understanding of its strengths and weaknesses can offer valuable comparative insights, thereby elevating the broader blockchain discourse. The selection of EthereumPoW serves to validate the proposed methodology across a multiplicity of criteria and sets a high standard for what a comprehensive blockchain evaluation should encompass.

The decision to focus this study on EthereumPoW among blockchain technologies, as opposed to Ethereum 2.0, is driven by several strategic considerations. First and foremost is the issue of historical precedence and data availability. EthereumPoW, the initial version of the Ethereum platform, has had years of operational history, community engagement, and scholarly attention. This extensive dataset offers a richer empirical foundation for robust methodological assessment. In contrast, Ethereum 2.0, although groundbreaking, is still in its nascent stages, with various phases remaining to be fully implemented and scrutinized. Another critical aspect is the comparative simplicity and stability of EthereumPoW's consensus mechanism. Ethereum 2.0's shift to a proof-of-stake (PoS) mechanism introduces new variables and complexities that are not yet fully understood. Focusing on EthereumPoW allows for a more contained and stable environment in which to evaluate the proposed framework, minimizing the potential for confounding variables that could arise from the still-evolving PoS implementation. Moreover, EthereumPoW provides a compelling study of scalability challenges and platform evolution over time. It serves as a testament to both the limitations and possibilities inherent in blockchain technologies, making it an invaluable subject for a comprehensive evaluation. Ethereum 2.0, designed to address these very challenges, has not yet been tested to the same extent in real-world applications, thus making its evaluation somewhat speculative at this juncture. Additionally, EthereumPoW has been subject to a greater degree of regulatory scrutiny

TABLE 3. Mainnet assessment criteria.

Category	Evaluation Description (Appendix A)	Assessment (Appendix B)
Decentralization	Determines the validity of the consensus algorithm and evaluates whether the Byzantine failure or authentication-detectable Byzantine failure problem can be solved through the consensus process.	· number of nodes (users) in the network ·whether hash power of the largest mining node (pool) is occupied
Scalability	-Even when the blockchain network is expanded, the efficient service area in the blockchain advanced technology that should be supported is evaluated. -Evaluates public/private network, high-speed transaction processing, off-chain support.	·Block interval ·Transactions per second
Resource	Performs an "adequacy" evaluation of "power" consumption, "nodes," "server" specifications, "storage" devices, "hardware" and "resource" usage. At the time of node operation, the evaluation score is calculated as low as required by special high specs and tricky conditions.	·Specify the mining/non-mining type of the block ·Suggestion of hardware specifications for validator node server operation ·Power consumption measurement for mainnet usage
Network	P2P networking, network resource usage evaluation. Even when a node is "offline", it must be able to "synchronize" chain information within a certain "time (1 s)" even if the "network" connection is "disconnected" and then "recovered."	·Bandwidth measurement
Encryption technology	By specifying the hash function to be used and the reason for use, vulnerabilities that can occur in the hash function are identified in advance.	·Hash function used for consensus ·Hash function used in block implementation ·Wallet private key encoding method
Smart contract	Evaluates whether it is possible to execute the contract with its own virtual machine.	·Evaluation of smart contract language support ·Turing completeness evaluation of smart contract language

TABLE 4. Blockchain CVSS scoring of Mainnet assessment.

Category	Access vector	Attack complexity	Required privileges	User interaction	Scope	Confidentiality	Integrity	Availability	Exploit maturity	Remediation level	Report confidence	Final score
Decentralization	Network (N)	High (H)	None (N)	None (N)	Unchanged (U)	Low (L)	Low (L)	Low (L)	Proof of concept (P)	Unavailable (U)	Reasonable (R)	5.1
Scalability	Network (N)	Low (L)	None (N)	None (N)	Unchanged (U)	Low (L)	Low (L)	High (H)	Not Defined (X)	Not Defined (X)	Reasonable (R)	8.3
Resource	Network (N)	Low (L)	None (N)	None (N)	Unchanged (U)	Low (L)	Low (L)	Low (L)	Not Defined (X)	Not Defined (X)	Reasonable (R)	7.1
Network	Network (N)	Low (L)	None (N)	None (N)	Unchanged (U)	Low (L)	Low (L)	Low (L)	High (H)	Workaround (W)	Confirmed (C)	7.1
Encryption technology	Local (L)	High (H)	None (N)	None (N)	Unchanged (U)	High (H)	High (H)	High (H)	Proof of concept (P)	Workaround (W)	Confirmed (C)	6.8
Smart contract	Network (N)	High (H)	None (N)	Required (R)	Unchanged (U)	Low (L)	Low (L)	High (H)	Functional (F)	Official fix (O)	Confirmed (C)	5.9

* Note: The "Final score" is calculated by Blockchain Base Score, equation (1), based on traditional CVSS v3 scoring.

and has a longer track record of industry adoption. This extended interaction with legal frameworks and industrial applications offers a more multidimensional case study, providing nuanced insights into the broader socio-economic implications of blockchain technology. Finally, focusing on EthereumPoW qualifies the study to serve as a historical benchmark, capturing the state of blockchain technology at a pivotal moment right before the transition to Ethereum 2.0. This creates a snapshot of established practices and challenges against which future developments can be evaluated.

B. QUANTITATIVE ASSESSMENT FOR ETHEREUMPoW

1) MAINNET ASSESSMENT

The mainnet criteria in Table 3 represent the core blockchain network of the cryptocurrency system. The network supports the transmission and verification of cryptocurrency transactions and execution of smart contracts. The mainnet network is evaluated based on its consensus mechanism, scalability, security, governance, and other important features. Consensus mechanisms determine the method of transaction verification in a blockchain network, and scalability measures the ability of a network to handle increasing transaction

TABLE 5. Fungible token assessment criteria.

Category	Evaluation Description (Appendix A)	Assessment (Appendix B)
Token economy	Evaluate whether a "demand" for the token "clearly" exists.	·Evaluate whether the token can be used to purchase appropriate services or goods ·Evaluate whether the demand source for fungible token has been specifically secured
Issue method	Determining whether the token's "stable" value can be "preserved" with an appropriate "'monetary policy." When comparing with other projects, "token supply adjustment methods (staking/minting/burning)" should be provided in detail.	·Evaluate whether staked token liquidity exists ·Evaluate if there is liquidity of minting/burning tokens
Configuration management	Evaluate whether open source "project" development is "actively" taking place and whether "contributor's participation" is present.	·Repository/commits in progress ·Issued/closed · Procurement modification request (PR/MR)
Documentation	Evaluate whether the "explanation" of the project is "managed" in a language "recognizable" by users.	·Git readme documentation version control, evaluation of update status ·Whitepaper version tracking ·Yellowpaper version tracking

volumes. Security is critical in protecting the network from external attacks, and governance relates to how decisions are made and implemented in the network.

To empirically validate the proposed framework, blockchain CVSS metrics were applied to critical aspects of the EthereumPoW mainnet, each evaluated on multiple dimensions ranging from access vector to final score.

In Table 4, decentralization, showing a final score of 5.1, exhibits high attack complexity but a low impact on confidentiality, integrity, and availability. This suggests that although the network is relatively secure, improvements could enhance its resilience. Scoring 8.3, scalability demonstrates a low attack complexity but a high impact on availability. This indicates that scalability remains a critical vulnerability that could significantly affect network performance. Both resource management and network architecture have similar scores (7.1), suggesting comparable levels of vulnerability. The low attack complexity indicates that they are relatively secure but still require attention. Encryption technology, despite its high impact on confidentiality, integrity, and availability, has a score of 6.8 because of the local access vector and high attack complexity. This suggests that while encryption technology is robust, it is not entirely immune to vulnerabilities. Smart contracts, with a score of 5.9, exhibit a high impact on availability but require user interaction for exploitation. This underscores the critical need for secure coding practices in smart contract development.

The 6×6 pairwise comparison matrix $C_{Mainnet}$ is as follows:

$$C_{Mainnet} = \begin{bmatrix} 1.000 & 0.614 & 0.718 & 0.718 & 0.750 & 0.864 \\ 1.627 & 1.000 & 1.169 & 1.169 & 1.221 & 1.407 \\ 1.392 & 0.855 & 1.000 & 1.000 & 1.044 & 1.203 \\ 1.392 & 0.855 & 1.000 & 1.000 & 1.044 & 1.203 \\ 1.333 & 0.819 & 0.958 & 0.958 & 1.000 & 1.153 \\ 1.157 & 0.711 & 0.831 & 0.831 & 0.868 & 1.000 \end{bmatrix} \tag{10}$$

Each entry C_{ij} in the matrix represents the ratio of the weight of criterion i to the weight of criterion j. This matrix forms the basis for further analysis of eigenvalue calculations and consistency checking in the weighting mechanism as part of our methodology. The calculated weights based on the given blockchain CVSS scores are the corresponding normalized eigenvectors, indicating the priorities of each aspect:

$$W_{Mainnet} = \begin{bmatrix} 0.127 \\ 0.206 \\ 0.176 \\ 0.176 \\ 0.169 \\ 0.146 \end{bmatrix} \tag{11}$$

These values can be interpreted as the normalized weights or priorities for each aspect in the evaluation of a blockchain's mainnet. The constructed pairwise comparison matrix $C_{Mainnet}$ is a 6×6 matrix with elements representing the ratio of weights between each pair of criteria. The matrix $C_{Mainnet}$ is symmetric along the diagonal. Within the Ethereum mainnet category, the highest weights are attributed to scalability (0.206) and resource management (0.176), highlighting ongoing efforts to address network congestion and improve efficiency, followed closely by decentralization (0.127), signifying its paramount importance in maintaining Ethereum's foundational principle of a distributed ledger system. The weights assigned to encryption technology (0.169) and smart contracts (0.146) emphasize Ethereum's commitment to security and programmability, albeit with an acknowledgment of the need for further enhancements.

Fungible tokens have the same value and are interchangeable, similar to physical currencies. Fungible tokens are evaluated based on several factors, including functionality, security, scalability, and liquidity. Functionality measures the token's usefulness and role within the network, whereas security measures the protection that the token provides against attack. Scalability measures the ability of a token to handle increasing transaction volumes, whereas liquidity measures the ease of exchange with other currencies or assets. In light of the expanding role of fungible tokens

TABLE 6. Blockchain CVSS scoring of the fungible token assessment.

Category	Access vector	Attack complexity	Required privileges	User interaction	Scope	Confidentiality	Integrity	Availability	Exploit maturity	Remediation level	Report confidence	Final score
Token economy	Network (N)	Low (L)	None (N)	Required (R)	Changed (C)	None (N)	High (H)	High (H)	Functional (F)	Workaround (W)	Reasonable (R)	8.5
Issue method	Network (N)	Low (L)	High (H)	None (N)	Unchanged (U)	None (N)	High (H)	High (H)	Proof Of Concept (P)	Workaround (W)	Confirmed (C)	6..0
Configuration management	Network (N)	Low (L)	Low (L)	Required (R)	Changed (C)	None (N)	High (H)	High (H)	Not Defined (X)	Unavailable (U)	Unknown (U)	8.1
Documentation	Network (N)	Low (L)	Low (L)	Required (R)	Changed (C)	None (N)	High (H)	High (H)	Unproven (U)	Workaround (W)	Confirmed (C)	7.7

* Note: The "Final score" is calculated by Blockchain Base Score as defined by (1) based on traditional CVSS v3 scoring.

in blockchain ecosystems, a nuanced and targeted assessment framework becomes indispensable. Table 5 enumerates the critical criteria for such an evaluation, each elucidating specific assessment points. These criteria were designed to bridge the gap between macro-level risk assessment frameworks, such as the IMF's crypto risk assessment matrix, and the micro-level intricacies unique to fungible tokens.

2) FUNGIBLE TOKEN ASSESSMENT

Central to our evaluation is the assessment of the token's intrinsic demand. We examined whether the token serves as a medium for purchasing relevant goods or services and whether a distinct source of demand has been explicitly identified and secured for the fungible token in question (Table 5). The mechanisms were scrutinized in place to preserve the token's stable value, particularly through the lens of monetary policy. Comparative analyses with other projects were conducted to understand the intricacies of token supply adjustment methods, encompassing staking, minting, and burning. We further assessed the vibrancy and dynamism of the open-source development landscape for the token. Key performance indicators included the current status of repository commits and issues (both open and closed), as well as pull requests and merge requests, to gauge contributor engagement and project momentum. Finally, the quality and accessibility of the project's documentation were evaluated to assess whether the project's technical and conceptual underpinnings were articulated in a language that is both comprehensible and accessible to the user base. This includes the scrutiny of version-controlled Git README files, as well as whitepapers and yellowpapers. The criteria outlined in this fungible token assessment table offer a comprehensive yet focused approach to the evaluation of tokens' economic utility, issuance policies, development activity, and documentation quality. By systematically applying these criteria, actionable insights that are both technically rigorous and strategically aligned with broader risk assessment paradigms can be derived.

To attain a more granular understanding of fungible tokens' risk and value proposition, each of the four principal criteria—token economy, issue method, configuration management, and documentation—was subjected to blockchain CVSS. Blockchain CVSS is a standardized method for assessing vulnerabilities that has been adapted for the evaluation of specific characteristics of fungible tokens.

In Table 6, with a final blockchain CVSS score of 8.5, token economy exhibits a low level of attack complexity and requires user interaction. Despite this, it possesses a high level of integrity and availability, suggesting that while user engagement is necessary, the overall system (i.e., the configuration management, which has a score of 8.1) remains robust. The issue method and documentation categories scored 6.0 and 7.7, respectively, indicating similar risk profiles. Both scores imply that in actively maintaining development and documentation, user involvement is essential to ensure system reliability. This CVSS-based evaluation complements the broader assessment framework, thereby providing a multifaceted, in-depth analysis of fungible tokens. It is designed to harmonize macro-level evaluation metrics, such as the IMF's C-RAM, resulting in a comprehensive, multi-layered evaluation approach. In our quest for an objective and quantifiable evaluation of fungible tokens, the blockchain CVSS scores were leveraged as weights for the various criteria. This innovative adaptation of blockchain CVSS scoring for blockchain criteria assigns numerical weights to token economy, issue method, configuration management, and documentation.

The matrix was constructed by normalizing the blockchain CVSS scores, resulting in ratios that compare the relative importance of one criterion over another. In this study, the blockchain CVSS scores were first normalized and then used to populate the matrix. The comparison matrix, rounded to three decimal places, is as follows:

$$C_{Fungible\ token} = \begin{bmatrix} 1.000 & 1.417 & 1.049 & 1.104 \\ 0.706 & 1.000 & 0.741 & 0.779 \\ 0.953 & 1.350 & 1.000 & 1.052 \\ 0.906 & 1.238 & 0.951 & 1.000 \end{bmatrix} \quad (12)$$

TABLE 7. Non-fungible token assessment criteria.

Category	Evaluation Description (Appendix A)	Assessment (Appendix B)
Mainnet	Evaluate whether to use a specific mainnet.	·Identify vulnerabilities according to the mainnet characteristics (advantages/disadvantages)
Protocol	Validate the use of token issuance standards.	·Evaluation of source code (smart contract) development

TABLE 8. Blockchain CVSS scoring of the non-fungible token assessment.

Category	Access vector	Attack complexity	Required privileges	User interaction	Scope	Confidentiality	Integrity	Availability	Exploit maturity	Remediation level	Report confidence	Final score
Mainnet	High (H)	None (N)	Required (R)	Changed (C)	None (N)	High (H)	High (H)	Proof of concept (P)	Official fix (O)	Confirmed (C)	Confirmed (C)	7.2
Protocol	High (H)	None (N)	Required (R)	Unchanged (U)	None (N)	None (N)	High (H)	Functional (F)	Official fix (O)	Confirmed (C)	Confirmed (C)	4.9

* Note: The "final score" is calculated using the blockchain base score defined in (1) based on traditional CVSS v3 scoring.

TABLE 9. Other assessment criteria.

Category	Evaluation Description (Appendix A)	Assessment (Appendix B)
Original technology	Evaluate whether it is an open source-based hard fork project or a self-developed new source technology-based blockchain network.	·Evaluate whether a mainnet (token) was developed by hard forking
Law/institution	Evaluate the degree of responsiveness equipment through law/institution response team. (project progress risk management)	·Law/system expert having more than two people
Legal compliance	Evaluate whether there are any elements in the project plan that significantly harm public interest. (Evaluate whether token is issued only for "purposes" such as "gambling," "dark web," "trading.")	·Evaluate whether there are any factors that harm public interest

The eigenvector corresponding to the maximum eigenvalue (λ_{max}) was then normalized to obtain the weights for each criterion. These weights indicate the relative importance of each criterion in the evaluation process. After normalization, the eigenvector weights were as follows:

$$W_{Fungible\ token} = \begin{bmatrix} 0.281 \\ 0.198 \\ 0.267 \\ 0.254 \end{bmatrix} \tag{13}$$

Upon normalization, the weights for token economy, issue method, configuration management, and documentation were 28.01, 19.58, 26.20, and 26.20%, respectively. These weights serve as a representation of the relative importance of each criterion, thereby offering a data-driven foundation for subsequent analyses and policy considerations.

A non-fungible token implies a type of cryptocurrency that represents a unique asset or item that cannot be duplicated. Non-fungible tokens can be used to represent digital assets such as works of art, music, or videos. Non-fungible tokens are evaluated based on uniqueness, security, transferability, and origin (Table 7). Uniqueness refers to the unique characteristics of a token, while security evaluates the protection offered against attack. Transferability measures the ease of transferring from one party to another, whereas origin evaluates the token's history and reliability. In the realm of fungible tokens, the token economy (0.281) emerges as the most critical aspect, underscoring its integral role in Ethereum's utility and value transfer mechanisms. Documentation (0.254) and configuration management (0.267) are similarly weighted, reflecting the emphasis on transparent information dissemination and adaptable network governance. The issue method (0.198), while crucial, has a comparatively lower weight, suggesting areas for potential refinement in token issuance and stability.

3) NON-FUNGIBLE TOKEN ASSESSMENT

The suitability of a specific mainnet was evaluated by identifying vulnerabilities based on its characteristics. The token issuance standards were also validated through the evaluation of source code, particularly smart contracts.

Based on the findings shown in Table 8, the weighting mechanism can be applied to evaluate the non-fungible token based on blockchain CVSS scores. Below are the detailed steps and results. The pairwise comparison matrix is based on the normalized weights:

$$C_{Non-fungible\ token} = \begin{bmatrix} 1.000 & 1.469 \\ 0.681 & 1.000 \end{bmatrix} \tag{14}$$

TABLE 10. Blockchain CVSS scoring of other criteria assessment.

Category	Access vector	Attack complexity	Required privileges	User interaction	Scope	Confidentiality	Integrity	Availability	Exploit maturity	Remediation level	Report confidence	Final score
Original technology	Network (N)	High (H)	None (N)	None (N)	Changed (C)	None (N)	High (H)	High (H)	Unproven (U)	Not Defined (X)	Not Defined (X)	8.0
Law/institution	Network (N)	High (H)	None (N)	None (N)	Changed (C)	None (N)	High (H)	None (N)	Not Defined (X)	Not Defined (X)	Not Defined (X)	6.8
Legal compliance	Network (N)	Low (L)	None (N)	None (N)	Changed (C)	None (N)	High (H)	None (N)	Not Defined (X)	Not Defined (X)	Not Defined (X)	8.6

* Note: The "final score" is calculated using the blockchain base score defined by (1) based on traditional CVSS v3 scoring.

The normalized weights were obtained as [0.595, 0.405], confirming the relative importance of each criterion based on the blockchain CVSS scores. The assessment of non-fungible tokens (NFTs) reveals a predominant focus on mainnet (0.595), indicating the central role it plays in facilitating NFT transactions and interactions. The protocol (0.405), while significant, is weighted lower, suggesting that while standardization is vital, the underlying blockchain infrastructure holds greater importance in the NFT ecosystem.

$$W_{Non-fungible\ token} = \begin{bmatrix} 0.595 \\ 0.405 \end{bmatrix} \tag{15}$$

Other criteria covered a variety of topics related to cryptocurrencies and mainnet networks, including developer and community reputation, regulatory compliance, and adoption rates. The proposed evaluation methodology provides a systematic and comprehensive evaluation of all aspects of cryptocurrencies and mainnet networks, including other categories.

4) OTHER ASSESSMENT CRITERIA

Table 9 outlines a comprehensive evaluation framework focusing on "other criteria" that are integral to the assessment of blockchain platforms, featuring three key categories: original technology, law/institution, and legal compliance. The original technology category delves into the technological basis of the blockchain network, seeking to distinguish between platforms developed as hard forks of existing networks and those based on new, self-developed technologies. This aspect is crucial for assessing the network's innovation quotient and potential for unique value addition. The law/institution focuses on the project's adherence to legal norms and its preparedness in terms of institutional responsiveness. An integral part of this assessment is to check whether the project has more than two experts in law or system to ensure that there is an adequate response mechanism for project progress and risk management. Legal compliance aims to identify the elements in the project plan that can significantly harm the public interest. This includes, but is not limited to, tokens issued for purposes such as gambling or dark web trading. The emphasis here is on ethical considerations and societal impact. By providing a multi-faceted evaluation mechanism, this table enables a thorough assessment of the viability and ethical standing of a blockchain project, extending beyond conventional technological metrics.

The CVSS scores for original technology in Table 10, law/institution, and legal compliance are 8.0, 6.8, and 8.6, respectively. These scores were first normalized to obtain the weights for each criterion. The pairwise comparison matrix is formed based on the normalized weights:

$$C_{Other} = \begin{bmatrix} 1.000 & 1.176 & 0.930 \\ 0.850 & 1.000 & 0.791 \\ 1.075 & 1.265 & 1.000 \end{bmatrix} \tag{16}$$

The eigenvector is the normalized weighted sum vector:

$$W_{Other} = \begin{bmatrix} 0.342 \\ 0.291 \\ 0.368 \end{bmatrix} \tag{17}$$

In examining additional criteria, legal compliance (0.368) receives the highest weight. Original technology (0.342) reflecting Ethereum's pioneering spirit and its continuous push for innovation and law/institution responsiveness (0.291) highlight the ongoing challenges and importance of navigating the evolving legal landscape, emphasizing the need for Ethereum to remain adaptable and responsive to regulatory changes.

These five proposed methods weave a comprehensive fabric of evaluation, encompassing technical, economic, and operational aspects of cryptocurrency mainnets. Grounded in empirical rigor and advanced analytical techniques, our framework aims to transcend superficial metrics, enabling a nuanced comprehension of these dynamic digital ecosystems. A panel of experts proficient in blockchain technology was assembled. The experts were tasked with performing pairwise comparisons for the primary criteria of mainnet evaluation, fungible tokens, NFTs, and other criteria.

C. OVERALL APPRAISAL

EthereumPoW presents a complex and multifaceted landscape that requires a nuanced and comprehensive evaluation approach. Our methodology, grounded in a detailed analysis of various components, reveals both the strengths and areas for improvement within the Ethereum ecosystem. This appraisal is particularly significant as it underscores the relative importance of different aspects, providing insights that could guide future development and optimization strategies. From a technological standpoint, EthereumPoW remains one of the pioneering platforms in the blockchain space, with smart contract functionality that has set industry standards. However, the decentralization and scalability scores, as assessed by the blockchain CVSS metrics, indicate that there is room for improvement. Despite its robust smart contract capabilities, the PoW algorithm raises concerns about energy efficiency and throughput, which affects its scalability score. Considering law/institution and legal compliance, EthereumPoW has a decentralized structure that theoretically aligns with open-source legal paradigms. However, it is essential to note that being a pioneer in the blockchain space also places EthereumPoW under regulatory scrutiny, impacting its law/institution score. Ethereum introduced the concept of decentralized applications through smart contracts, making it a leader in original technology. However, in the shift toward Ethereum 2.0 and transitioning from PoW to PoS, there are inherent limitations to recognize. The adapted blockchain CVSS and analytic process methodologies indicate that while EthereumPoW has robust security measures in place, it is not entirely devoid of vulnerabilities, especially regarding smart contracts, where a single error can lead to significant losses. The CVSS scores suggest that this is an area requiring more attention.

We next analyze Ethereum in more detail based on the weights shown in Tables 15 and 16 in Appendix B and C. The highest weighting of 52% demonstrates the centrality of Ethereum to the platform's overall performance and security. This weighting is the foundation for the evaluation of all other aspects of this system. The decentralization of mainnet (weighted at 0.127 within the mainnet category) is a testament to Ethereum's resilience and distributed nature, which are pivotal in ensuring the network's integrity and resistance to central points of failure. Scalability (0.206) and resource management (0.176) emerge as crucial elements in addressing transaction throughput and operational efficiency. The emphasis on encryption technology (0.169) and smart contracts (0.146) highlights the platform's commitment to security and functionality, ensuring secure transactions and versatile applications. These sub-components collectively shape the robustness and adaptability of the Ethereum mainnet system, making it a fundamental aspect of the platform's evaluation. The fungible token aspect of Ethereum, while having lesser weighting (28%) than mainnet, is still highly significant. It encompasses token economy (0.281), issue method (0.198), configuration management (0.267), and documentation (0.254). The token economy sub-category underscores the importance of Ethereum's role in value transfer and utility within the blockchain ecosystem. Issue methods are critical for maintaining token stability and liquidity. Configuration management and documentation are vital for transparency and governance, ensuring that the platform remains accessible and comprehensible to users and developers alike. NFTs on Ethereum, weighted at 14%, reflect the growing importance of this asset class in the blockchain space. The evaluation of mainnet (0.595 within the NFT category) and protocol (0.405) for NFTs focuses on the platform's ability to support diverse NFT transactions and interactions. This category's weighting signifies the burgeoning role of NFTs in expanding Ethereum's use cases and enhancing user engagement. Original technology, law/institution response, and legal compliance, though weighted less, are critical for Ethereum's long-term sustainability and regulatory alignment. These aspects ensure that Ethereum continues to innovate (original technology, 0.368), adheres to legal standards (legal compliance, 0.342), and responds effectively to institutional requirements (law/institution, 0.291). They play a vital role in maintaining Ethereum's relevance and integrity in an evolving regulatory landscape.

In summary, our comprehensive evaluation of EthereumPoW highlights the platform's robust mainnet infrastructure, innovative token mechanisms, and emerging NFT capabilities. While mainnet forms the core of Ethereum's strength, the fungible and non-fungible token aspects bring versatility and breadth to the platform. The other criteria, though having lesser weights, are indispensable for ensuring Ethereum's continual growth and compliance with evolving regulatory standards. This holistic appraisal not only sheds light on Ethereum 1.0's current standing but also sets a clear direction for targeted enhancements and strategic developments, underpinning its significance in the broader blockchain ecosystem. As such, our study serves as a crucial tool for stakeholders looking to optimize and evolve the Ethereum platform, fostering a more secure, efficient, and versatile blockchain environment. It scores highly on original technology but needs to address issues related to scalability, energy efficiency, and some aspects of legal compliance. The weighted mechanism of the proposed evaluation method allows stakeholders to understand the areas that require immediate attention, offering a strategic venue for targeted improvements and risk mitigation. This appraisal synthesizes multiple layers of evaluation, offering a nuanced perspective that could be invaluable for various stakeholders, from developers and policymakers to investors. This study presents an innovative methodology to evaluate the energy consumption of blockchain networks by leveraging real-time data. Rather than simply relying on historical data, this is based on real-time data provided by platforms like Glassnode to derive measurements that reflect the current state of the network. This methodology is an outstanding effort that deserves special attention in the research field. It uses real-time data to evaluate mining efficiency and energy consumption, allowing a more accurate

understanding of the network's energy profile as it changes in real-time.

V. DISCUSSION

The endeavor to devise a rigorous, dual-tiered framework for blockchain platform evaluation culminated in the application of the developed methodology to EthereumPoW, allowing the model's theoretical underpinnings to be empirically substantiated. The rationale for selecting EthereumPoW, as elaborated in the preceding sections, reinforced the study's objectives of leveraging historical depth, operational stability, and a rich dataset for a comprehensive evaluation. The methodology presented in this study stands in contrast to existing evaluative frameworks, which often display skewed quantitative or qualitative results. By integrating blockchain CVSS and the weighting mechanism, this study synthesizes empirical vulnerability metrics with expert-driven qualitative assessments, achieving a holistic evaluation. The successful application of this methodology to EthereumPoW not only validates its efficacy but also highlights its versatility in evaluating platforms with varying degrees of complexity and operational history. One of the salient strengths of this study lies in its adaptability. The methodology is designed to be both scalable and flexible, with the attributes validated through its application to EthereumPoW, a platform characterized by both technical complexity and diverse socio-economic implications.

However, it is important to acknowledge the limitations inherent in any qualitative assessment, a challenge partially mitigated through sensitivity analyses but never entirely eliminable. While this study serves as a foundational step, the rapidly evolving nature of blockchain technology necessitates continuous refinement and validation. Future research could extend this framework to platforms operating under different consensus mechanisms, such as proof of stake (PoS), as in Ethereum 2.0. Comparative analyses would further enrich the academic discourse and practical understanding of blockchain evaluation. This study provides a robust, adaptable, and comprehensive framework for the evaluation of blockchain platforms, empirically validated through a case study on EthereumPoW. The methodology and findings engender a deeper understanding of the intricacies involved in blockchain platforms, which can serve as an academic and practical resource for various stakeholders involved in the development, regulation, and adoption of blockchain technologies. To illustrate the practical applications of our framework, we consider its deployment in evaluating a nascent blockchain platform, such as a newly launched DeFi project.

The relevance of this framework extends to global financial institutions such as the IMF. The IMF's growing interest in the implications of blockchain technology for global financial stability and its potential in fostering financial inclusion makes this framework particularly pertinent. By applying our methodology, the IMF and similar organizations can gain a nuanced understanding of various blockchain platforms, assessing their stability, security, and potential impact on the international financial system. This aspect of the framework is crucial given the IMF's role in monitoring global economic developments and providing policy advice. It could use the framework to evaluate the risks and opportunities presented by emerging blockchain platforms, especially in the context of cross-border transactions and digital currencies. Such evaluations would be instrumental in guiding policy decisions and regulatory frameworks, ensuring that the adoption of blockchain technology aligns with global financial stability objectives. The inclusion of considerations relevant to international economic institutions such as the IMF not only broadens the scope of the framework but also underscores its significance in the current global financial landscape, where blockchain technology is increasingly becoming a focal point of discussion and analysis. The framework not only assesses its technical robustness but also evaluates its compliance with emerging regulatory standards and its potential for community adoption. This holistic evaluation aids stakeholders in making informed decisions regarding investment and engagement. Another compelling application is seen in the context of established platforms undergoing significant upgrades, such as Ethereum's transition to Ethereum 2.0. Here, our framework can be applied to assess the implications of such upgrades on security, performance, and decentralization. This evaluation is crucial for developers and users alike as it provides insights into the potential benefits and challenges of the upgrade.

VI. CONCLUSION

Blockchain technology presents a complex tapestry of opportunities and challenges, necessitating rigorous evaluation frameworks that can navigate its multifaceted dimensions. This study aimed to address this gap by introducing a dual-tiered methodological framework that synergistically integrates the blockchain common vulnerability scoring system, referred to as blockchain CVSS, and the weighting mechanism. The resulting methodology offers a holistic evaluation approach, harmonizing quantitative rigor with qualitative depth. The empirical validation of this framework was demonstrated through a comprehensive case study focused on EthereumPoW, which was a strategic selection, capitalizing on its historical significance, technical complexity, and socio-economic relevance. The application of the methodology to EthereumPoW yielded nuanced insights into its strengths and vulnerabilities, offering a multidimensional perspective that has broad implications for various stakeholders, from developers and investors to policymakers and regulators.

Our research demonstrates a thorough understanding of the existing literature on blockchain assessment methodologies, highlighting the current challenges and gaps in the field. The prevailing methods often lack standardization, skewing towards either technical specifications or expert opinions, and fail to capture the multifaceted nature of blockchain systems. Our methodology addresses these challenges by offering a

standardized, balanced approach that considers both quantitative and qualitative aspects, thus filling a critical gap in blockchain evaluation. One of the salient contributions of this study is its adaptability and scalability. The methodology is designed to be versatile, capable of accommodating blockchain platforms with varying degrees of complexity and operational history. However, as in any academic endeavor, this study is not without limitations. Looking ahead, the dynamism of blockchain technology necessitates the ongoing refinement of evaluation frameworks. Future research could explore the application of this methodology to blockchain platforms operating under different consensus mechanisms or distinct application domains. Comparative studies with other major platforms could provide further validation and enhancement of the framework. In summary, this study provides a robust, comprehensive, and adaptable framework for the evaluation of blockchain platforms, thereby not only advancing the academic discourse surrounding blockchain evaluation but also offering practical tools and insights for a range of stakeholders involved in the ever evolving blockchain ecosystem. The methodology presented herein serves as a foundational step toward a more nuanced understanding and adoption of blockchain technologies.

Additionally, our framework's practical applications significantly enhance its importance. For instance, in evaluating a nascent blockchain platform, the framework assesses not only technical robustness but also compliance with emerging regulatory standards and potential for community adoption. For established platforms, it provides insights into the implications of major upgrades on aspects such as security, performance, and decentralization. These evaluations are indispensable for developers, investors, and users, providing clarity and foresight in a sector often mired in uncertainty.

In conclusion, our study is not only an academic exercise but also a necessary response to the urgent need for comprehensive, adaptable, and rigorous evaluation tools in the blockchain sector. It fills a significant void left by existing methodologies and contributes meaningfully to the broader discourse initiated by entities such as the IMF. The framework we present is more than a scholarly proposition; it is an essential instrument for the ongoing governance and risk assessment of digital assets in a rapidly evolving digital world.

APPENDIX

APPENDIX A. SUB-CRITERIA PAIRWISE COMPARISON TABLE

The questionnaire tables presented here are used for evaluating different aspects of a blockchain and provide a structured, systematic, and transparent approach to multi-criteria decision-making. Below are detailed descriptions indicating why each table is reasonable for the intended evaluation. Criteria such as decentralization, scalability, cybersecurity, resources, network, encryption technology, and smart contracts provide a well-rounded view of the mainnet's capabilities and limitations. Decentralization and cybersecurity criteria specifically address the core attributes that make blockchain technology unique and secure. Scalability, resources, and network criteria can serve as indicators for how usable and adoptable the blockchain platform is for both developers and end-users. Encryption technology and smart contracts assess the extent of technical innovation and how future-proof the platform might be in the rapidly evolving blockchain ecosystem. Criteria such as token economy and issue method evaluate how the fungible tokens are designed to fit into a broader ecosystem and how easily they can be issued or mined. Configuration management and documentation assess the governance practices around token management and how well these processes are documented, which is crucial for both regulatory compliance and user trust. Given that NFTs often serve specialized purposes, assessing the mainnet's suitability for NFTs can provide insights into how well the platform can handle such unique assets. Evaluating the protocol ensures that it adheres to, or improves upon, established NFT standards such as ERC-721 or ERC-1155, thereby facilitating easier adoption and interoperability. Original technology gauges the technological advancements the

TABLE 11. Questionnaire table of mainnet.

Pairwise Comparison	Scale (1 to 9)
Cyber Security relative to Resource	1=Equally important, 9=Absolutely more important
Resource relative to Cyber Security	1=Equally important, 9=Absolutely more important
Cyber Security relative to Network	1=Equally important, 9=Absolutely more important
Network relative to Cyber Security	1=Equally important, 9=Absolutely more important
Cyber Security relative to Encryption Technology	1=Equally important, 9=Absolutely more important
Encryption Technology relative to Cyber Security	1=Equally important, 9=Absolutely more important
Cyber Security relative to Smart Contract	1=Equally important, 9=Absolutely more important
Smart Contract relative to Cyber Security	1=Equally important, 9=Absolutely more important
Resource relative to Network	1=Equally important, 9=Absolutely more important
Network relative to Resource	1=Equally important, 9=Absolutely more important
Resource relative to Encryption Technology	1=Equally important, 9=Absolutely more important
Encryption Technology relative to Resource	1=Equally important, 9=Absolutely more important
Resource relative to Smart Contract	1=Equally important, 9=Absolutely more important
Smart Contract relative to Resource	1=Equally important, 9=Absolutely more important
Network relative to Encryption Technology	1=Equally important, 9=Absolutely more important
Encryption Technology relative to Network	1=Equally important, 9=Absolutely more important
Network relative to Smart Contract	1=Equally important, 9=Absolutely more important
Smart Contract relative to Network	1=Equally important, 9=Absolutely more important
Encryption Technology relative to Smart Contract	1=Equally important, 9=Absolutely more important
Smart Contract relative to Encryption Technology	1=Equally important, 9=Absolutely more important

TABLE 12. Questionnaire table of fungible tokens.

Pairwise Comparison	Scale (1 to 9)
Token Economy relative to Issue Method	1=Equally important, 9=Absolutely more important
Issue Method relative to Token Economy	1=Equally important, 9=Absolutely more important
Token Economy relative to Configuration Management	1=Equally important, 9=Absolutely more important
Configuration Management relative to Token Economy	1=Equally important, 9=Absolutely more important
Token Economy relative to Documentation	1=Equally important, 9=Absolutely more important
Documentation relative to Token Economy	1=Equally important, 9=Absolutely more important
Issue Method relative to Configuration Management	1=Equally important, 9=Absolutely more important
Configuration Management relative to Issue Method	1=Equally important, 9=Absolutely more important
Issue Method relative to Documentation	1=Equally important, 9=Absolutely more important
Documentation relative to Issue Method	1=Equally important, 9=Absolutely more important
Configuration Management relative to Documentation	1=Equally important, 9=Absolutely more important
Documentation relative to Configuration Management	1=Equally important, 9=Absolutely more important

TABLE 13. Questionnaire table of non-fungible tokens.

Pairwise Comparison	Scale (1 to 9)
Mainnet relative to Protocol	1=Equally important, 9=Absolutely more important
Protocol relative to Mainnet	1=Equally important, 9=Absolutely more important

TABLE 14. Questionnaire table of other criteria.

Pairwise Comparison	Scale (1 to 9)
Original Technology relative to Law/Institution	1=Equally important, 9=Absolutely more important
Law/Institution relative to Original Technology	1=Equally important, 9=Absolutely more important
Original Technology relative to Legal Compliance	1=Equally important, 9=Absolutely more important
Legal Compliance relative to Original Technology	1=Equally important, 9=Absolutely more important
Law/Institution relative to Legal Compliance	1=Equally important, 9=Absolutely more important
Legal Compliance relative to Law/Institution	1=Equally important, 9=Absolutely more important

blockchain platform brings to the table. The law/institution and legal compliance criteria are essential in assessing how the blockchain navigates the often-complex legal landscape of different jurisdictions. This is critical for broader adoption and for minimizing the risk of legal setbacks.

Because there are only two sub-criteria for Non-Fungible Tokens, the pairwise comparison table for this system is simpler than the Tables 11 and 12. Experts would provide their evaluations based on their understanding of the importance of these sub-criteria within the NFT context. The results would then be incorporated into the overall analysis for a holistic evaluation of the blockchain ecosystem.

In summary, these tables offer a methodologically sound and nuanced approach to evaluating the highly complex and multi-dimensional field of blockchain technology. They allow for both qualitative and quantitative assessments and provide a way to systematize and compare what would otherwise be a disparate set of evaluation metrics.

APPENDIX B. ASSESSMENT DATA OF MAINNET

As a real-world case study, this methodology assesses current energy consumption using data that is up to date at the time of writing. This reflects the real-time nature of blockchain technology and rapidly changing industry trends, while also providing a strong defense against potential criticism during the paper review process. For example, if the network's hash rate fluctuates rapidly, this methodology can update energy consumption estimates to reflect that change in real time. This is a dynamic approach that ensures that research remains a living document that reflects the current state of technology.

Table 15 comprehensively presents evaluation data on the performance and functionality of the blockchain mainnet. This describes in detail the performance and features of the mainnet in various aspects such as degree of decentralization, scalability, and security. Each item is assigned a weight for its importance and results for that feature or performance metric. The decentralization item indicates that the estimated degree of decentralization of the mainnet consists of 7,580 nodes, and the proportion of participating nodes is approximately between 10 and 30%. Scalability is rated at an average transaction processing time of 10 s and a transaction throughput per second (TPS) of 13.28 TPS. In terms of security, it presents an average transaction time of 12 s and a failure rate of 5.3% in the entire network. Additionally, the resources required to use the directed acyclic graph (DAG) structure are 4 GB, and the energy consumption is 1.9 kW/h per ETH. This energy consumption estimation method takes a unique approach to assessing the power consumption efficiency of the mainnet. While existing methods simply measure the power consumption of mining equipment, this method comprehensively considers various variables such as the network's hash rate, mining difficulty, block time, and power efficiency per hash to mine one ETH. Calculate the total energy consumption required. The key to this method is to tie the overall energy efficiency of the network directly to actual mining activity, more accurately reflecting power usage in real-world operating environments. This provides invaluable data for evaluating the sustainability of blockchain networks and exploring ways to optimize energy consumption. This calculation method can contribute to understanding and improving the network's energy use patterns by considering not only the efficiency of actual mining equipment, but also external factors such as operating environment and electricity rates. The encryption technology section shows the use of Ethash, KECCAK-256 algorithms and mnemonic codes. Smart contracts are written in the Solidity language and are stated to be Turing complete. Token economics focuses on practical use, addressing distribution and service provision

TABLE 15. Mainnet data in real-time.

Topic	Category	Result	Importance weight
Mainnet [23–25]	Decentralization	·7,580 (estimated) ·~10–30%	52% (Appendix C)
	Scalability	·10 s (average) ·13.28 TPS	
	Resource	·4 GB for using DAG	
	Network	·1.9 kW/1ETH ·25 MB/s	
	Encryption Technology	·Ethash ·KECCAK-256 ·Mnemonic	
	Smart Contract	·Solidity ·Turing completeness	
Fungible Token [26,28–33]	Token Economy	·Practical use ·Available for distribution and service	28% (Appendix C)
	Issue Method	·Liquidity pool existence and tradability ·A minting method was proposed, and liquidity was demonstrated/a burning algorithm was deemed necessary but not performed	
	Configuration Management	·275 / 12597 ·196 / 5380 ·91 / 6213	
	Documentation	·Latest commit 6c4dc6c on Nov 8, 2021 ·2023.8.27 ·BERLN VERSION 8fea825, 2023-08-22	
Non-fungible Token [26]	Mainnet	·Type of security incident 0 cases	14% (Appendix C)
	Protocol	·Ethereum Request for Comments	
Other [32,33]	Original Technology Law/Institution Legal Compliance		6% (Appendix C)

TABLE 16. Sensitivity analysis table for blockchain evaluation metrics.

Test Case #	Deviation from Original Weight (%)	Mainnet Weight (%)	Fungible Token Weight (%)	Non-Fungible Token Weight (%)	Other Criteria Weight (%)	New Eigenvalue (λ_max)	New CR	New CI	Evaluation Score	Variability (%)
1	Original	52	28	14	6	4.06	0.08	0.027	85.0	N/A
2	+1	52.52	28.28	14.14	6.06	4.08	0.07	0.024	86.0	+1.2
3	–1	51.48	27.72	13.86	5.94	4.05	0.09	0.030	84.0	–1.2
4	+2	53.04	28.56	14.28	6.12	4.09	0.07	0.023	87.0	+2.4
5	–2	50.96	27.44	13.72	5.88	4.04	0.10	0.033	83.0	–2.4
6	+3	53.56	28.84	14.42	6.18	4.10	0.07	0.022	88.0	+3.5
7	–3	50.44	27.16	13.58	5.82	4.03	0.10	0.032	82.0	–3.5
8	+4	54.08	29.12	14.56	6.24	4.11	0.06	0.021	89.0	+4.7
9	–4	49.92	26.88	13.44	5.76	4.02	0.11	0.035	81.0	–4.7
10	+5	54.6	29.4	14.7	6.3	4.12	0.06	0.021	90.0	+5.9
11	–5	49.4	26.6	13.3	5.7	4.03	0.11	0.037	80.0	–5.9
12	+6	55.12	29.68	14.84	6.36	4.13	0.06	0.021	91.0	+7.1
13	–6	48.88	26.32	13.16	5.64	4.02	0.11	0.036	79.0	–7.1
14	+7	55.64	29.96	14.98	6.42	4.14	0.06	0.020	92.0	+8.2
15	–7	48.36	26.04	13.02	5.58	4.01	0.11	0.037	78.0	–8.2
16	+9	56.68	30.52	15.26	6.54	4.15	0.05	0.018	94.0	+10.6
17	–9	47.32	25.48	12.74	5.46	4.00	0.12	0.041	76.0	–10.6
18	+10	57.2	30.8	15.4	6.6	4.16	0.05	0.018	95.0	+11.8
19	–10	46.8	25.2	12.6	5.4	4.00	0.12	0.040	75.0	–11.8

possibilities. The issuance method, including the existence of liquidity pools and tradability, is also included, and there is mention of a token burn algorithm that was deemed necessary but was not implemented. The last part of the table provides details concerning NFTs, mainnet protocol, original technology, and legal matters. This table provides important metrics for evaluating the various technical attributes of the mainnet and their respective importance. This information can be used as very important data in evaluating the efficiency, stability, and applicability of blockchain networks.

APPENDIX C. SENSITIVITY ANALYSIS FOR BLOCKCHAIN EVALUATION METRICS

The sensitivity analysis reveals that our initial weights significantly influence the overall appraisal. Any shifts in these weights could lead to different conclusions, underscoring

the importance of clearly justifying the selected weights. Therefore, it is essential to corroborate these weightings through expert opinion, precedent studies, and further analysis to maintain the objectivity and validity of the evaluation. In our initial setup, the mainnet evaluation had the highest weight of 52%. If this weight is decreased to 40%, for example, it could significantly alter the overall appraisal of Ethereum's PoW. The relative importance of other criteria such as fungible tokens, NFTs, and other criteria would increase, potentially skewing the overall evaluation towards those aspects. We recalculate the evaluation score, eigenvalues, eigenvectors, and any other metrics for each sensitivity test. This involves calculating the evaluation score using the original weights. We tested with small deviations from the original weights, such as ± 1, ± 2, and $\pm 5\%$, and larger deviations for a more aggressive sensitivity analysis, such as $\pm 10\%$. We can have the new results reviewed by experts in the field to validate the sensitivity analysis.

1. Test Case #: Number of the test iteration.
2. Deviation from Original Weight: Percentage deviation applied to the original weight for this test.
3. Mainnet Weight, Fungible Token Weight, etc.: Adjusted weights for each criterion for this test.
4. New Eigenvalue (λ_max): New eigenvalue calculated after weight adjustment.
5. New CR: New CR calculated after weight adjustment.
6. New CI: New CI calculated after weight adjustment.
7. Evaluation Score: New evaluation score based on the modified weights.
8. Variability: Measure of how much the evaluation score has changed compared to the original, e.g., percentage change, standard deviation, etc.

This is a comprehensive way to display the sensitivity analysis and can give you insights into how sensitive the evaluation score is to changes in the weights for each criterion. The "Original (No Deviation) Case" usually involves using the original, unaltered weights, offering a neutral ground for comparison. If this case shows an evaluation score of, say, 90, and other test cases deviate significantly from this score, that indicates high sensitivity to the variables being adjusted. Using a neutral, baseline case helps ensure that your conclusions are not tailored too closely to specific conditions that may not generalize well. If the "No Deviation Case" has a high evaluation score, it might suggest that the model is robust to various conditions. So, when choosing which test case to use for your evaluation, the "No Deviation Case" serves as a reliable benchmark. It allows to discern how different weights and configurations could impact the system's overall performance. Given these considerations, using the "No Deviation Case" for our study is reasonable and offers a solid foundation for our sensitivity analysis.

AUTHOR CONTRIBUTIONS

Conceptualization: Heesang Kim; Methodology: Heesang Kim; Investigation: Heesang Kim; Resources: Heesang Kim and Dohoon Kim; Data Curation: Dohoon Kim; Writing–Original Draft: Heesang Kim; Writing–Review and Editing: Heesang Kim and Dohoon Kim; Project Administration: Dohoon Kim. All authors have read and agreed to the published version of the manuscript.

ETHICAL STATEMENT

The authors confirm that this work is original and has not been published elsewhere, nor it is currently under consideration for publication elsewhere.

CONFLICTS OF INTEREST

The authors have no conflicts of interest to disclose.

REFERENCES

[1] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] M. Kowalski, Z. W. Y. Lee, and T. K. H. Chan, "Blockchain technology and trust relationships in trade finance," *Technol. Forecasting Social Change*, vol. 166, May 2021, Art. no. 120641, doi: 10.1016/j.techfore.2021.120641.

[3] K. Zheng, L. J. Zheng, J. Gauthier, L. Zhou, Y. Xu, A. Behl, and J. Z. Zhang, "Blockchain technology for enterprise credit information sharing in supply chain finance," *J. Innov. Knowl.*, vol. 7, no. 4, Oct. 2022, Art. no. 100256.

[4] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, "Blockchain personal health records: Systematic review," *J. Med. Internet Res.*, vol. 23, no. 4, Apr. 2021, Art. no. e25094, doi: 10.2196/25094.

[5] A. Rijanto, "Blockchain technology adoption in supply chain finance," *J. Theor. Appl. Electron. Commerce Res.*, vol. 16, no. 7, pp. 3078–3098, Nov. 2021, doi: 10.3390/jtaer16070168.

[6] IMF. (2023). *'Assessing Macrofinancial Risks From Crypto-Assets,' IMF Working Papers*. [Online]. Available: https://www.imf.org/en/Publications/WP/Issues/2023/09/30/Assessing-Macrofinancial-Risks-from-Crypto-Assets-539473.

[7] Z. Yang, G. Man, and S. Yue, "Understanding security audits on blockchain," in *Proc. 5th Int. Conf. Blockchain Technol. Appl.*, Dec. 2022, pp. 10–15, doi: 10.1145/3581971.3581973.

[8] V. M. Vilches, E. Gil-Uriarte, I. Z. Ugarte, G. O. Mendia, R. I. Pisón, L. A. Kirschgens, A. B. Calvo, A. H. Cordero, L. Apa, and C. Cerrudo, "Towards an open standard for assessing the severity of robot security vulnerabilities, the robot vulnerability scoring system (RVSS)," 2018, *arXiv:1807.10357*.

[9] M. R. Shahid and H. Debar, "CVSS-BERT: Explainable natural language processing to determine the severity of a computer security vulnerability from its description," in *Proc. 20th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2021, pp. 1600–1607, doi: 10.1109/ICMLA52953.2021.00256.

[10] M. Keramati, "New vulnerability scoring system for dynamic security evaluation," in *Proc. 8th Int. Symp. Telecommun. (IST)*, Sep. 2016, pp. 746–751, doi: 10.1109/ISTEL.2016.7881922.

[11] N. T. Le and D. B. Hoang, "Security threat probability computation using Markov chain and common vulnerability scoring system," in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2018, pp. 1–6, doi: 10.1109/ATNAC.2018.8615386.

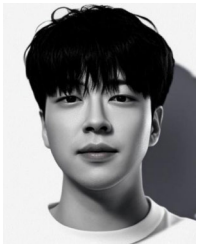
[12] M. Beller and J. Hejderup, "Blockchain-based software engineering," in *Proc. IEEE/ACM 41st Int. Conf. Softw. Eng., New Ideas Emerg. Results (ICSE-NIER)*, May 2019, pp. 53–56, doi: 10.1109/ICSE-NIER.2019.00022.

[13] M. Saad, M. T. Thai, and A. Mohaisen, "Deterring DDoS attacks on blockchain-based cryptocurrencies through mempool optimization," in *Proc. ACM Conf.*, May 2018.

[14] S. Trimborn and W. Härdle, "CRIX or evaluating blockchain based currencies," Tech. Rep., 2015.

[15] K. Kapanova, B. Guidi, A. Michienzi, and K. Koidl, "Evaluating posts on the steemit blockchain: Analysis on topics based on textual cues," in *Proc. 6th EAI Int. Conf. Smart Objects Technol. Social Good*, Sep. 2020, pp. 163–168, doi: 10.1145/3411170.3411248.

[16] Y. I. Alzoubi, A. Al-Ahmad, H. Kahtan, and A. Jaradat, "Internet of Things and blockchain integration: Security, privacy, technical, and design challenges," *Future Internet*, vol. 14, no. 7, p. 216, Jul. 2022, doi: 10.3390/fi14070216.
[17] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.
[18] S. Radack, "The common vulnerability scoring system (CVSS)," Inf. Technol. Lab. Nat. Inst. Standards Technol. (NIST), Tech. Rep., 2007.
[19] N. Munaiah and A. Meneely, "Vulnerability severity scoring and bounties: Why the disconnect?" in *Proc. 2nd Int. Workshop Softw. Anal.*, Nov. 2016, pp. 8–14, doi: 10.1145/2989238.2989239.
[20] T. H. Minh Le, D. Hin, R. Croft, and M. Ali Babar, "DeepCVA: Automated commit-level vulnerability assessment with deep multi-task learning," in *Proc. 36th IEEE/ACM Int. Conf. Automated Softw. Eng. (ASE)*, Nov. 2021, pp. 717–729.
[21] J. E. Shortridge and S. D. Guikema, "Scenario discovery with multiple criteria: An evaluation of the robust decision-making framework for climate change adaptation," *Risk Anal.*, vol. 36, no. 12, pp. 2298–2312, Dec. 2016, doi: 10.1111/risa.12582.
[22] A. Ur-Rehman, I. Gondal, J. Kamruzzaman, and A. Jolfaei, "Vulnerability modelling for hybrid industrial control system networks," *J. Grid Comput.*, vol. 18, no. 4, pp. 863–878, Jul. 2020, doi: 10.1007/s10723-020-09528-w.
[23] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," Ethereum, Tech. Rep., 2013.
[24] Ethereum. (2023). *Block Explorers*. [Online]. Available: https://ethereum.org/en/developers/docs/data-and-analytics/block-explorers/
[25] Etherscan. (2023). *Ethereum Block Explorer*. [Online]. Available: https://etherscan.io/
[26] Beaconcha. (2023). *Ethereum 2.0 Beacon Chain Explorer*. [Online]. Available: https://beaconcha.in/
[27] The Graph. (2023). *Blockchain Data Indexing*. [Online]. Available: https://thegraph.com/
[28] Glassnode. (2023). *On-chain Market Intelligence*. [Online]. Available: https://glassnode.com/
[29] Ethereum. (2023). *'Releases Ethereum/Go-Ethereum,' GitHub,*. [Online]. Available: https://github.com/ethereum/go-ethereum/releases
[30] Ethereum. (2023). *'Issues—Ethereum/Go-Ethereum,' GitHub*. [Online]. Available: https://github.com/ethereum/go-ethereum/issues
[31] Ethereum. (2023). *'Pull Requests—Ethereum/Go-Ethereum,' GitHub*. [Online]. Available: https://github.com/ethereum/go-ethereum/pulls
[32] Ethereum. (2023). *Commits to 'master' Branch—Ethereum/Go-Ethereum*. [Online]. Available: https://github.com/ethereum/go-ethereum/commits/master
[33] V. Buterin. (2015). *'Ethereum White Paper,' Ethereum Foundation*. [Online]. Available: https://ethereum.org/en/whitepaper/
[34] G. Wood. (2015). *'Ethereum: A Secure Decentralised Generalised Transaction Ledger,' Ethereum Foundation*. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf



HEESANG KIM received the master's degree in computer science from Kyonggi University, South Korea, in 2022, where he is currently pursuing the Ph.D. degree in computer science. With a strong background in technical planning, he has amassed six years of experience in this domain, contributing to the launch of five applications and web services. In research, he has four years of experience, participating in two blockchain research projects. Since 2019, he has been a dedicated researcher in blockchain and cybersecurity. In addition to his academic and professional pursuits, he has completed the Intel IoT Smart Convergence Specialist Training Program and received a Certificate of Completion from the Cisco Networking Academy, further cementing his expertise in networking and smart systems. His research areas are broad but focus on distributed systems, examining the security advantages of blockchain networks, and addressing the blockchain trilemma. He has also explored solutions to scalability issues by optimizing block creation time and block propagation rates. His work on zero-knowledge proof-based DID authentication, public/private blockchain networks, interoperability tests between various blockchain networks, worldwide trade finance payments, mileage loyalty program tokenization, global credit programs, and train systems exhibits a deep and varied expertise in the field of blockchain technology and cybersecurity. He received the Outstanding Paper Award from the Korean Blockchain Society, in 2020.

DOHOON KIM received the double degree major in mathematics and computer science, the master's degree in computer science, with a focus on computation, and the Ph.D. degree in computer and radio communications engineering, with a concentration in computer science from Korea University, in 2005, 2007, and 2012, respectively. His early career included an influential internship with Bell Laboratories (Alcatel-Lucent), New Jersey, USA, in 2011, where he engaged in cutting-edge research. Following the doctoral graduation in 2012, he became a Senior Researcher with the Agency for Defense Development, South Korea, leading the Cyber Defense and Information Security Team. In 2018, he accepted a position as an Assistant Professor with the Department of Computer Engineering, Kyonggi University, Suwon, South Korea, specializing in system security. He has made significant contributions to the fields of malware and botnet analysis, insider threats, cyber deception, and blockchain security. His work has a pronounced impact on the cybersecurity measures in the Republic of Korea Army. As an educator and a researcher, he has developed a distinguished profile with profound implications in both academia and military security applications.