An ISO/IEC 25010-based quality assessment model for distributed ledger technology platforms*

Serhii Zhebka[1,†], Viktoriia Zhebka[1,*,†], Kateryna Nesterenko[1,†], Ganna Grynkevych[2,†], and Oleksii Cherevyk[2,†]

[1] State University of Information and Communication Technologies, 7 Solomenskaya str., 03110 Kyiv, Ukraine
[2] Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

Abstract
In this paper, the selection of a DLT platform is presented as part of the design decision for an information system based on a distributed ledger. In financial services, IoT solutions, digital platforms and enterprise systems, the requirements for such a ledger differ, so a single assessment is not suitable for all cases. Blockchain platforms differ in their architecture, consensus algorithms, trust model and level of decentralization. Because of this, their comparison cannot be reduced to a list of advantages. A framework is required in which security, performance, scalability and cross-network interaction are considered in relation to one another. The review of the literature has shown that most approaches operate with individual metrics, whereas a consistent multicriteria assessment of DLT platforms still requires refinement. The paper substantiates an adapted quality assessment model for DLT platforms based on ISO/IEC 25010 and oriented towards the properties of the distributed ledger environment. The DLT-QM model considers traditional software quality engineering characteristics together with parameters of the blockchain environment, including decentralization, consensus reliability, transaction finality, auditability, interoperability and the features of on-chain/off-chain architecture. For the practical application of the model, an algorithm for the integral assessment and ranking of blockchain platforms by application scenarios is proposed. The model was tested on six platforms: Ethereum, Hyperledger Fabric, Polygon, Avalanche, Solana and Corda. This set was chosen deliberately, as it combines public networks, permissioned solutions, enterprise platforms and systems with different approaches to scaling. The comparison made it possible to trace how the balance between decentralization, security, performance and interoperability changes within each class. The sensitivity of the results to the criteria weights was examined separately, since it is the weights that change the order of the platforms in a given scenario.

Keywords
distributed ledger, blockchain, DLT platform, blockchain system, decentralization, software quality, software engineering, multicriteria analysis, systems architecture, consensus, information security, information technology.

1. Introduction

Distributed ledger technologies are now used much more widely than in the financial sector alone. They are applied in logistics, digital platforms, IoT environments, e-government and enterprise data exchange. In such systems, what matters is not only the records in the distributed network themselves, but also the ability to verify their immutability, trace transactions and reduce dependence on a single central intermediary.

The difficulty of the choice lies in the fact that DLT platforms have different design logics. Some solutions emphasize open participation and decentralization, others — controlled access, managed trust or higher throughput. The type of consensus, the way transactions are confirmed, the support for on-chain/off-chain interaction and interoperability also differ. Therefore, the technical profile of a platform must be considered together with the application scenario.

* CPITS 2026: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2026, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
s.zhebka@stud.duikt.edu.ua (S. Zhebka), v.zhebka@duikt.edu.ua (V. Zhebka); k.nesterenko@duikt.edu.ua (K. Nesterenko); g.grynkevych@kubg.edu.ua (G. Grynkevych); o.cherevyk@kubg.edu.ua (O. Cherevyk)
0009-0007-4620-9888 (S. Zhebka); 0000-0003-4051-1190 (V. Zhebka); 0000-0001-7672-7386 (K. Nesterenko); 0000-0003-1922-5165 (G. Grynkevych); 0009-0006-0347-7607 (O. Cherevyk)

The literature usually analyses throughput, latency, energy efficiency or the resilience of consensus to attacks and failures separately. For an engineering choice this is not enough, because a platform is assessed by a combination of properties. ISO/IEC 25010 can be used as an initial framework; however, the standard contains no direct criteria for transaction finality, decentralized governance, cross-network interaction and hybrid DLT platforms. Therefore, the ISO characteristics need to be supplemented with parameters of distributed ledger systems.

In this regard, there is a need to develop an adapted quality assessment model for DLT platforms that would make it possible to perform a multicriteria analysis of blockchain systems within a single mathematical framework, ensure the integration of ISO characteristics with DLT-specific parameters, and support decision-making on the selection of the optimal platform depending on the application scenario.

In works devoted to distributed ledger systems and blockchain technologies, DLT platforms are regarded as the basis of financial services, e-government systems, IoT networks, logistics platforms and enterprise information systems [1-5]. Their operation relies on distributed data storage, decentralized consensus and cryptographic confirmation of transactions, which ensure the transparency, integrity and immutability of data [1, 2, 4]. Considerable attention in research is paid to blockchain governance, interoperability, consensus algorithms and the security of distributed ledger systems [3, 5, 7, 10]. At the same time, the differences between platforms in architecture, consensus, degree of decentralization and trust models complicate their comparison on a single scale [1, 3, 6, 8].

Existing approaches to the analysis of blockchain systems are mostly focused on individual aspects of the operation of distributed ledger platforms: studies of consensus algorithms aim to ensure the resilience and consistency of the distributed environment [7, 10], interoperability approaches aim to support the cross-network interaction of blockchain systems [3], and works in the field of blockchain governance and trust models aim to form mechanisms of decentralized management [5]. Individual studies address the problems of blockchain security, scalability and smart contract ecosystems [2, 4, 8, 9]. However, there are no comprehensive models that would ensure the integration of classical software quality engineering characteristics with the specific parameters of the DLT environment within a single mathematical framework for the multicriteria assessment of blockchain platforms [1, 5, 6].

The analysis of the literature revealed a scientific gap consisting in the absence of adapted quality assessment models for DLT platforms capable of simultaneously taking into account decentralization, consensus reliability, transaction finality, auditability, the trust model, cross-network interoperability and the features of on-chain/off-chain architectures [3, 5, 7, 10]. This determines the relevance of further research aimed at developing integrated models for the multicriteria assessment of blockchain systems based on combining the characteristics of ISO/IEC 25010 with DLT-specific parameters, with the aim of supporting decision-making on the selection of the optimal distributed ledger platform depending on the application scenario [1, 2, 6].

Within this paper, the aim of the study is to build an adapted quality assessment model for DLT platforms based on ISO/IEC 25010. Such a model should be suitable for a formalized multicriteria analysis of blockchain systems and, at the same time, take into account the properties of the distributed ledger environment. To achieve this aim, the following objectives have been defined:

- to analyse existing approaches to the assessment of DLT platforms and to determine the limitations of applying the ISO/IEC 25010 standard to blockchain systems;
- to form a set of DLT-specific characteristics and to build a mathematical model that combines ISO and DLT criteria in a common assessment space;
- to develop an algorithm for the integral assessment and ranking of DLT platforms depending on the application scenario;
- to carry out an experimental validation of the model and to determine its suitability for supporting decision-making in the selection of blockchain platforms.

2. Research Results

The proposed quality assessment model for DLT platforms implements a full cycle of multicriteria analysis of distributed ledger platforms — from forming a set of alternatives and collecting initial characteristics to computing an integral quality indicator and generating a recommendation on the selection of the most suitable platform for a given application scenario. Unlike existing approaches, in which the assessment of blockchain systems is performed mainly by separate local parameters, the proposed algorithm ensures the integration of the characteristics of ISO/IEC 25010 with specialized DLT parameters within a single mathematical model.

To formalize the procedure for selecting a distributed ledger platform, a mathematical model of multicriteria assessment is proposed that combines the classical software quality characteristics defined by the ISO/IEC 25010 standard with specialized parameters of the DLT environment. Unlike existing approaches, where the assessment of blockchain platforms is mostly performed by separate indicators of performance, security or scalability, the proposed model treats a platform as a complex software-and-hardware system whose suitability is determined by a set of interrelated characteristics.

The formalization of the DLT platform quality assessment process begins with forming the set of alternatives to be analysed. Each alternative is a separate distributed ledger platform characterized by its own architecture, consensus mechanism, level of decentralization and set of functional capabilities.

$$P=\{P_1,\ P_2,\ \dots,\ P_n\}$$

where P is the set of platforms under study; P_i is the i-th DLT platform; n is the number of alternatives included in the assessment procedure.

The introduction of the set of alternatives is necessary for the subsequent comparative analysis and ranking of platforms. Each alternative is considered as a potential solution for use in a particular application scenario.

To ensure a comprehensive assessment, a set of criteria is formed that combines software quality characteristics with the specific characteristics of distributed ledger technologies:

$$Q=Q_{ISO}\cup Q_{DLT}=\{q_1,\ q_2,\ \dots,\ q_k\}$$

where Q_{ISO} is the set of quality criteria according to the ISO/IEC 25010 standard; Q_{DLT} is the set of criteria specific to distributed ledger technologies; q_j is an individual assessment criterion; k is the total number of criteria.

The set Q_{ISO} may include criteria of functional suitability, performance, reliability, compatibility, security and maintainability of software. The set Q_{DLT} includes indicators of decentralization, consensus reliability, transaction finality, auditability, the trust model, cross-network interoperability and the efficiency of interaction between on-chain and off-chain components.

Based on the formed set of criteria, an initial data matrix is created

$$X=[x_{ij}],\qquad i=1,\ \dots,\ n;\qquad j=1,\ \dots,\ k$$

where x_{ij} is the value of the j-th criterion for the i-th platform; i is the alternative index; j is the criterion index.

The matrix X contains the initial quantitative or expert estimates of all platforms against all criteria. It serves as the basis for the subsequent procedures of data normalization and aggregation.

When forming the assessment matrix, situations may arise in which individual values are missing.

$$x_{ij}=\varnothing$$

In this case, a procedure for handling missing data is applied:

$$x_{ij}=\begin{cases}\bar{x}_j, & \text{expert or average value;}\\ 0, & \text{critical absence of the indicator.}\end{cases}$$

$$\begin{cases}\bar{x}_j, & \text{expert or average value;}\\ 0, & \text{critical absence of the indicator.}\end{cases}$$

where x_j is the mean or expert-determined value of the j-th criterion.

Using the mean value makes it possible to avoid losing an alternative because of incomplete data. At the same time, a critical absence of a parameter is interpreted as the absence of the corresponding property, which is reflected by a zero score.

Since different criteria may be measured in different units, the next stage is data normalization. For maximization criteria, the following relation is used

$$r_{ij}=\frac{x_{ij}-x_j^{\overline{\min}}}{x_j^{\max}-x_j^{\min}}$$

where r_{ij} is the normalized value of the criterion; $x_j^{\max}$ is the maximum value of the criterion among all platforms; $x_j^{\min}$ is the minimum value of the criterion.

For minimization criteria, the following formula is used

$$r_{ij}=\frac{x_j^{\max}-x_{ij}}{x_j^{\max}-x_j^{\min}}$$

Such normalization brings all indicators to a single interval $[0|1]$, where a higher value always corresponds to better quality.

If all alternatives have the same value of a certain criterion, the following condition is used

$$x_j^{max}=x_j^{min},$$

then

$$r_{ij}=1.$$

After normalization is completed, the matrix is formed

$$R=[r_{ij}], \qquad r_{ij}\in[0;1]$$

The matrix R is used for the subsequent calculation of integral quality characteristics.

The block for calculating DLT-specific characteristics begins with the assessment of decentralization, since it is precisely this property that distinguishes DLT platforms from traditional centralized information systems. Decentralization here is not reduced merely to the number of nodes in the network, but is considered as a complex characteristic that takes into account the distribution of control, the participation of validators in maintaining consensus and the geographical placement of the infrastructure. For this, the following formula is used

$$D_d=w_1(1-G)+w_2N_v+w_3G_{geo},$$

subject to

$$\sum_{i=1}^{3} w_i = 1.$$

In the formula above, D_d denotes the integral decentralization indicator of the DLT platform. The parameter G characterizes the level of control concentration in the network, for example the concentration of computational resources, validator powers, stake share or managerial influence in the hands of a limited number of participants. Since an increase in concentration reduces actual decentralization, the formula uses the expression $(1|G)$, which reflects the inverse effect of centralization on platform quality. The indicator N_v characterizes the participation of nodes or validators in maintaining the network and reaching consensus. The higher the value of N_v, the more distributed the transaction confirmation process is. The parameter G_{geo} reflects the geographical distribution of nodes, which is important for the network's resilience to regional outages, regulatory restrictions or infrastructure failures. The coefficients w_1, w_2, w_3 determine the weight of each decentralization component, and the condition $\sum_{i=1}^{3} w_i = 1$ ensures the normalization of their contributions. Thus, a value of D_d close to one indicates a high level of decentralization, whereas a low value indicates the dominance of centralized control mechanisms.

The next characteristic is consensus reliability, which determines the platform's ability to maintain a consistent state of the distributed ledger in the presence of failures, network delays or potentially malicious behaviour of some participants. For DLT platforms this indicator is critical, since it is the consensus mechanism that guarantees that all correct nodes share the same view of the system state. Consensus reliability is determined by the formula

$$C_r = P_{\text{cons}}(n,\ f) \cdot (1 - P_{\text{fork}})$$

where C_r is the integral consensus reliability indicator, $P_{cons}(n, f)$ denotes the probability of correctly reaching consensus in the presence of n nodes and f faulty or malicious nodes, and P_{fork} characterizes the probability of a chain fork. The expression $(1|P_{fork})$ is used because, as the probability of fork situations increases, confidence in the stability of the ledger state decreases. The multiplicative form of the formula means that high consensus reliability is possible only when two conditions are met simultaneously: the consensus mechanism must be fault-tolerant, and the risk of alternative branches or state ambiguity must be low.

For platforms that use Byzantine fault tolerance, the model takes into account the boundary condition

$$BFT : f < n/3$$

In this inequality, f denotes the number of faulty, incorrect or potentially malicious nodes, and n is the total number of nodes participating in reaching consensus. The meaning of the condition is that a system with BFT properties can preserve the correctness of agreement only when the number of incorrect nodes is less than one third of the total number of participants. If this limit is exceeded, the system loses the guarantees of correct consensus, and therefore its resilience should be assessed as critically low.

To represent this dependence quantitatively, a piecewise function is used

$$P_{\text{cons}}(n,\ f) = \begin{cases} 1 - fn, & f < n/3 \\ 0, & f \geq n/3 \end{cases}$$

In this formula, $P_{cons}(n, f)$ reflects the probability of correctly reaching consensus. If the number of faulty or malicious nodes does not exceed the permissible limit, the consensus probability decreases in proportion to the share of such nodes in the network. If, however, the condition holds, the value $P_{cons}(n,f)$ is taken to be zero, since the system loses its formal resilience guarantees. This formulation makes it possible to embed the theoretical BFT constraint into a practical assessment model for a DLT platform.

The transaction finality indicator characterizes the degree of irreversibility of records after their confirmation by the network. In a DLT environment, a transaction may be included in a block, but this does not always mean its finality, since under certain conditions a regrouping or reorganization of the chain is possible. Therefore, finality in the model is defined through the probability of the absence of reorganization after a certain number of confirmations:

$$F_t = 1 - P_{\text{reorg}}(k)$$

In this formula, F_t denotes the transaction finality indicator, $P_{reorg}(k)$ is the probability of chain reorganization after k confirmations, and k is the number of confirmation blocks or consensus rounds after which a transaction is considered accepted. If the reorganization probability $P_{reorg}(k)$ is low, then the indicator F_t approaches one, which means a high level of record irreversibility. If, however, the reorganization risk remains significant, finality decreases, and the platform becomes less suitable for scenarios where the legal, financial or accounting finality of transactions is critical.

The next indicator is auditability, which reflects the ability to verify, trace and confirm the authenticity of transactions within a DLT platform. For blockchain systems, auditability is of particular importance, since a distributed ledger is often used as a means of ensuring the transparency and immutability of data. In the model, auditability is determined by the formula

$$A = V_t \cdot (1 - P_{\text{tamper}}) \cdot C_{\text{audit}}$$

In the formula above, A is the integral auditability indicator, V_t characterizes transaction traceability, P_{tamper} denotes the probability of unauthorized modification or distortion of records, and C_{audit} reflects the completeness of audit coverage. The parameter V_t shows how fully the path of a transaction can be traced from the moment of its initiation to its final recording in the ledger. The expression $(1|P_{tamper})$ is used to account for the resistance of records to tampering, since as the modification risk increases, platform quality decreases. The indicator C_{audit} characterizes the presence and completeness of mechanisms for auditing, logging, state verification and data integrity confirmation. The multiplicative nature of the formula means that auditability cannot be high if at least one of the components has a low value.

To describe the architectural trust model, the indicator T_m is used, which takes into account different ways of forming trust between participants of a DLT network. In public blockchain platforms, trust is mostly formed through openness of participation, cryptographic confirmation and economic incentives, whereas in permissioned systems it depends more on authentication procedures, access control and organizational governance. In general form, the trust model is represented by the formula

$$A = V_t \cdot (1 - P_{\text{tamper}}) \cdot C_{\text{audit}}$$

subject to

$$\sum_{i=1}^{3} \mu_i = 1.$$

In this formula, T_m is the integral trust model indicator, T_{open} characterizes the level of network openness for participants, T_{perm} describes the level of permissioned control, T_{gov} reflects the maturity and effectiveness of network governance mechanisms, and μ_1, μ_2, μ_3 are the weighting coefficients of the corresponding components. The condition $\sum_{i=1}^{3} \mu_i = 1$ ensures the normalization of the weights and makes it possible to change the significance of the trust components depending on the platform type. For open decentralized networks, greater weight may be given to T_{open}, for enterprise DLT solutions — to T_{perm}, and for systems with a developed mechanism of collective governance — to T_{gov}.

Cross-network interoperability characterizes the ability of a DLT platform to interact with other blockchain networks, external services, enterprise information systems, digital identifiers, APIs and off-chain components. This characteristic is important, since modern DLT solutions often operate not in isolation but as part of a complex digital ecosystem. To assess it, the following formula is used

$$I_x = \sum_{(s=1)}^{p} \lambda_s S_s,$$

subject to

$$\sum_{s=1}^{p} \lambda_s = 1$$

In this formula, I_x denotes the integral cross-network interoperability indicator, S_s is the s-th interoperability component, p is the number of interoperability components, and λ_s is the weighting coefficient of the corresponding component. S_s may include support for cross-chain protocols, the presence of bridges between networks, compatibility with smart contracts of other platforms, support for standard APIs, integration with external databases and the ability to exchange data with off-chain services. The weighting coefficients λ_s make it possible to adapt the model to a specific scenario: for IoT or supply chain systems, integration with external data sources may be more important, whereas for DeFi services — cross-chain interaction and the transfer of digital assets between networks.

The last indicator in the block of DLT-specific characteristics is the balance of on-chain/off-chain architecture. Many modern DLT platforms use a combined approach in which critical records are committed to the distributed ledger, while part of the computations, data or service logic is moved to the off-chain environment. This approach increases performance and scalability but creates risks of losing consistency between different layers of the system. To assess this property, the following formula is applied

$$B_{oc} = \eta_1 E_{on} + \eta_2 E_{off} + \eta_3 (1 - L_s),$$

subject to

$$\sum_{i=1}^{3} \eta_i = 1$$

In this formula, B_{oc} is the balance indicator of on-chain/off-chain architecture, E_{on} characterizes the efficiency of on-chain components, E_{off} reflects the efficiency of off-chain components, and L_s denotes the synchronization losses between the two layers of the system. The parameters η_1, η_2, η_3 are the weighting coefficients of the corresponding components. The expression $(1|L_s)$ is used because, as synchronization losses increase, the quality of the hybrid architecture decreases. Thus, a high value of B_{oc} means that the platform effectively combines the immutability and transparency of the on-chain layer with the performance and scalability of the off-chain components.

After the individual DLT-specific characteristics have been calculated, they are aggregated into a single integral DLT quality indicator. This stage is necessary because the indicators of decentralization, consensus, finality, auditability, the trust model, cross-network interoperability and the balance of on-chain/off-chain architecture characterize different aspects of platform operation and cannot be directly compared with one another. To generalize them, the following formula is used

$$Q_{\text{spec}}(P_i)=\sum_{j=1}^{7} b_j \; q_j^{\text{DLT}}(P_i),$$

subject to

$$\sum_{j=1}^{7} b_j=1$$

In the relation above, $Q_{spec}(P_i)$ is the integral assessment of the DLT-specific characteristics of platform P_i. The parameter $q_j^{DLT}(P_i)$ characterizes the value of the j-th specialized criterion for platform P_i. Such criteria include the indicators of decentralization D_d, consensus reliability C_r, transaction finality F_t, auditability A, the trust model T_m, cross-network interoperability I_x and the balance of on-chain/off-chain architecture B_{oc}. The coefficient b_j determines the significance of the corresponding criterion in the overall assessment. The normalizing condition

$$\sum_{j=1}^{7} b_j=1$$

guarantees that all criteria form a single assessment scale and that none of them dominates the others uncontrollably.

The obtained indicator $Q_{spec}(P_i)$ characterizes the platform solely in terms of the properties of distributed ledger technology and makes it possible to assess its architectural suitability for use in a decentralized environment.

In parallel, the platform is assessed as a software product in accordance with the ISO/IEC 25010 standard. For this, the integral ISO component is used:

$$Q_{\text{ISO}}(P_i)=\sum_{s=1}^{m} a_s \; q_s^{\text{ISO}}(P_i),$$

subject to

$$\sum_{s=1}^{m} a_s=1.$$

Here, $Q_{ISO}(P_i)$ is the integral assessment of the software quality of platform P_i. The parameter $q_s^{ISO}(P_i)$ describes the value of the s-th criterion of the ISO/IEC 25010 standard. Such criteria may include functional suitability, performance, reliability, compatibility, information security, maintainability and portability of software. The coefficient a_s determines the weight of the corresponding criterion in the overall ISO assessment. The condition

$$\sum_{s=1}^{m} a_s=1.$$

ensures the normalization of the weighting coefficients and the comparability of the results between different platforms.

Thus, the indicator $Q_{ISO}(P_i)$ characterizes the implementation quality of the platform as a software complex, independently of the features of the distributed ledger technology.

After the two integral components have been obtained, the final platform quality indicator is calculated:

$$Q^*_{\text{DLT}}(P_i) = \alpha Q_{\text{ISO}}(P_i) + \beta Q_{\text{spec}}(P_i)$$

subject to

$$\alpha + \beta = 1, \qquad \alpha, \ \beta \in [0;1]$$

In this formula, $Q^*_{DLT}(P_i)$ is the integral quality assessment of the DLT platform P_i. The indicator $Q_{ISO}(P_i)$ characterizes the software quality of the system, whereas $Q_{spec}(P_i)$ describes its DLT-specific properties. The coefficients α and β determine the relative importance of each component. If the software characteristics are critical for the application scenario, the value α may be increased. If, however, the main attention is paid to the properties of the distributed ledger, greater weight is given to the coefficient β.

The proposed formula is central to the entire assessment model, since it ensures the integration of two different groups of characteristics within a single mathematical space. Its distinctive feature is the ability to adapt to a specific application scenario. For enterprise information systems, where software reliability, support and compatibility are critical, it is advisable to increase the coefficient α. For financial services, digital platforms and decentralized ecosystems, on the contrary, greater significance is acquired by the coefficient β, which strengthens the influence of the DLT-specific characteristics.

In fact, the indicator $Q^*_{DLT}(P_i)$ is a generalized quantitative assessment of a platform's suitability for use in a given scenario. It is precisely on the basis of this indicator that, at the final stage of the algorithm, the ranking of alternatives, the analysis of architectural trade-offs between security, decentralization and performance, and the formation of a recommendation on the choice of the most appropriate DLT platform are carried out.

It is the indicator $Q^*_{DLT}(P_i)$ that is the main result of assessing an individual platform and is used at the subsequent stages of the algorithm.

After the assessment of all alternatives is completed, a vector of integral scores is formed:

$$Q^* = [Q^*_{\text{DLT}}(P_1), \ Q^*_{\text{DLT}}(P_2), \ \ldots, \ Q^*_{\text{DLT}}(P_n)].$$

Here, Q^* is an ordered set of the assessment results of all platforms that participated in the study. Each element of the vector contains the integral score of the corresponding alternative. Forming such a vector makes it possible to move from the analysis of individual platforms to their collective comparison.

Based on the formed vector, the alternatives are ranked:

$$P_{(1)} \succ P_{(2)} \succ \ldots \succ P_{(n)}$$

where

$$Q^*_{\text{DLT}}(P_1) \geq Q^*_{\text{DLT}}(P_2) \geq \ldots \geq Q^*_{\text{DLT}}(P_n)$$

In this notation, the symbol $\succ$ denotes the preference of one platform over another. Platform $P_{(1)}$ has the highest integral score and occupies first place in the ranking. Platform $P_{(n)}$ has the lowest score and occupies the last position. Ranking makes it possible to obtain an ordered list of alternatives and to determine their relative advantages.

In some cases, several platforms may have identical or very close values of the integral indicator. To resolve such situations, the priority criterion rule is used:

$$P_a > P_b,\ \ q_{\text{priority}}(P_a) > q_{\text{priority}}(P_b).$$

Here, P_a and P_b are platforms that have identical or close values of the integral score. The parameter $q_{priority}$ denotes the criterion that is most important for a particular application scenario. For example, for financial systems such a criterion may be transaction finality or consensus reliability, for state registries — auditability, and for IoT systems — cross-network interoperability.

The final stage of the algorithm is the formation of a recommendation on the choice of the optimal platform:

$$P^* = \underset{P_i \in P}{\arg\max}\ \ Q^*_{\text{DLT}}(P_i)$$

In this formula, P^* denotes the recommended platform, which has the highest value of the integral quality indicator. The operator *arg max* determines the alternative from the set P for which the value of the function $Q^*_{DLT}(P_i)$ is maximal. The obtained result is a formalized recommendation on the choice of a DLT platform and is used to support decision-making in a particular application scenario.

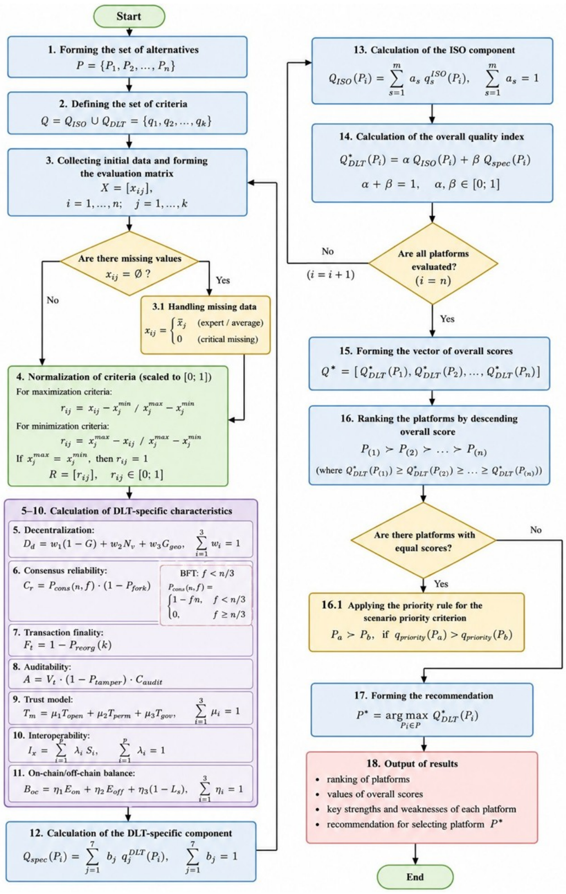

Figure 1: Algorithm for computing the general quality assessment model of DLT platforms

At the final stage of the algorithm, the assessment results are interpreted, which includes the analysis of the platform ranking, the values of the integral quality indicators and the contribution of individual criteria to the overall assessment. On the basis of the obtained values $Q^*_{DLT}(P_i)$, the strengths and weaknesses of each DLT platform are determined, architectural trade-offs between decentralization, security, performance and compatibility are revealed, and a recommendation on the advisability of using the platform in a particular application scenario is formed. The result of the algorithm is a ranking of alternatives and a justified choice of the optimal platform P^* that best meets the established requirements and assessment priorities.

That is, the optimal platform is considered to be the one for which the integral quality indicator is maximal.

After the integral values have been calculated, an ordered list of DLT platforms is obtained. It should not be perceived as a simple rating detached from the conditions of the task. The position of each alternative is explained by which properties gave it an advantage and which became a constraint. On this basis, a recommendation on a DLT solution is formed, taking into account security, performance, decentralization and compatibility.

In this work, DLT-QM is presented as a sequence of assessment actions. First, the characteristics are selected, then they are normalized, after which the weighting coefficients are applied and the integral score is calculated. The advantage of such an approach lies not in obtaining a single fixed rating, but in the ability to reconfigure the assessment for the purpose of a particular blockchain system.

In the financial scenario, greater weight is given to consensus reliability, transaction finality and auditability: a state error here directly affects the accounting of operations. For IoT-oriented distributed ledger platforms, the emphasis is different. There, interoperability, consistent on-chain/off-chain interaction and stable data exchange between elements of the distributed environment become more important.

3. Experimental Validation

The experimental study was carried out to verify the practical suitability of the proposed DLT-QM model for the multicriteria assessment of distributed ledger platforms. Ethereum, Hyperledger Fabric, Polygon, Avalanche, Solana and Corda were chosen as alternatives, which makes it possible to cover different architectural classes of DLT systems, in particular public blockchain networks, permissioned platforms, hybrid solutions and enterprise systems. For each platform, a normalized vector of DLT characteristics D_d, C_r, F_t, A, T_m, I_x, B_{oc} was formed, after which a scenario-oriented assessment was performed for the financial scenario, e-government, IoT/supply chain and the balanced scenario

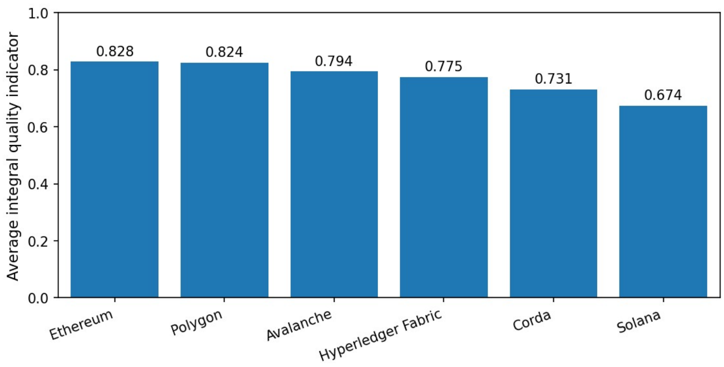

Figure 2: Integral assessment of DLT platforms using the DLT-QM model

Figure 2 shows that the integral score is related to the architectural profile of the platform. For the given set of weights, Ethereum took the highest place. This is explained by the combination of decentralization, an established trust model and developed means of cross-network interaction in the blockchain ecosystem. At the same time, this result does not imply the automatic superiority of this platform for all scenarios.

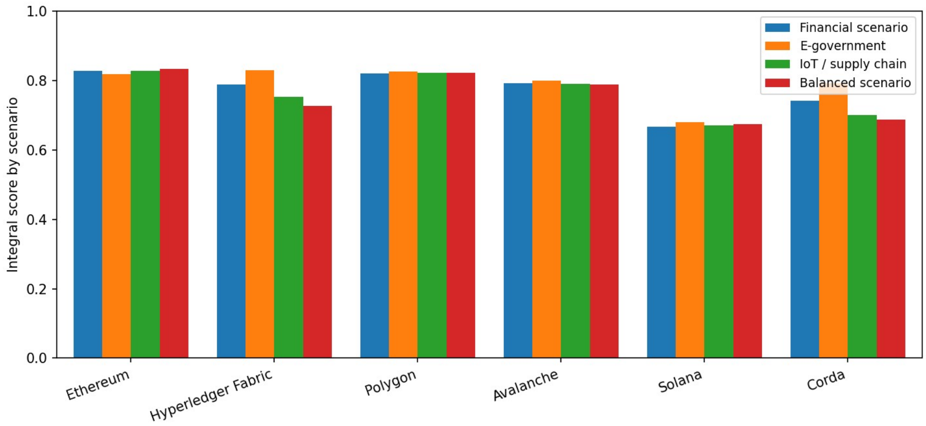

Figure 3: Scenario-oriented assessment of DLT platforms

Figure 3 shows that a change in the application context also changes the contribution of individual criteria. For e-government, auditability, transaction finality and the integrity of information processes become more important, since they support trust in the digital service.

The validation on the selected blockchain platforms produced not only final scores. From the criteria profile, it is possible to see where a trade-off arises between decentralization, performance, security and cross-network interoperability. This makes DLT-QM suitable for decision support and preliminary architectural analysis.

Conclusions

The paper presents a quality assessment model for DLT platforms based on ISO/IEC 25010. Its essence lies in combining software quality engineering characteristics with parameters of the blockchain environment: decentralization, consensus reliability, transaction finality, auditability, the trust model and cross-network interoperability. In this approach, a DLT platform is assessed as an architectural solution, and its suitability is determined by the particular use scenario.

The experimental part showed that the proposed approach can be applied to real distributed ledger platforms. The integral indicators helped to highlight the strengths and limitations of the blockchain systems considered. The sensitivity analysis confirmed that the result changes together with the criteria weights, so the ranking should be interpreted only within the chosen scenario.

Further work can focus on expanding the set of DLT-specific characteristics. It is advisable to separately take into account energy efficiency, resistance to post-quantum attacks and decentralized governance mechanisms. A practical continuation is the creation of an information system for the automated assessment of blockchain platforms using real-time telemetry data of distributed ledger systems.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Y.DLiu, Q. Lu, L. Zhu, H.-Y Paik, Z. Xing, A Systematic Literature Review on Blockchain Governance. J. Syst. Softw., (2023) 197, 111576, doi.or/10.1016/j.jss.2022.111576

[2] J. Xu, S. Lee, Analysis for Blockchain Application Quality. In: CEUR Workshop Proceedings, (2020), 2800.

[3] O. Barkovska, Systematyzatsiia Znan pro Typy ta Arkhitektury Blokchein-Rishen [Systematization of knowledge about types and architectures of blockchain solutions]. Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu, 2025. [Ukrainian].

[4] O. Shmatko, Analiz stiikosti ta bezpekovosti informatsiinykh system u post-quantum seredovyshchi [Analysis of resilience and security of information systems in a post-quantum environment]. Zakhyst informatsii, 25(1), 2023). [Ukrainian].

[5] H. Tereshchenko, Analiz i obgruntuvannia vykorystannia naiavnykh blokchein-protokoliv dlia zabezpechennia bezpeky tsyfrovykh aktyviv [Analysis and substantiation of the use of existing blockchain protocols for ensuring the security of digital assets], (2024). Informatsiini tekhnolohii ta suspilstvo, doi:10.32782/ITSSI-2024-467 [Ukrainian].

[6] V. Zhebka, S. Zhebka, T. Bazhan, P. Skladannyi, V. Sokolov, Methodology for Choosing a Consensus Algorithm for Blockchain Technology, In: CEUR Workshop Proceedings, 2024, 3665, 106-113.

[7] F. Casino, T. Dasaklis, C. Patsakis, A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open Issues. Telemat. Inform., 36, 55-81, 2019, doi:10.1016/j.tele.2018.11.006

[8] R. Belchior, A. Vasconcelos, S. Guerreiro, M. Correia, A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Computing Surveys, 54 (8), 1-41, 2021, doi:10.1145/3471140

[9] K. Christidis, M. Devetsikiotis, Blockchains and Smart Contracts for the Internet of Things. In: IEEE Access, 4, 2292-2303, 2016, doi:10.1109/ACCESS.2016.2566339

[10] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, Blockchain Challenges and Opportunities: A survey. Int. J. Web Grid Serv., 14 (4), 352-375, 2018, doi:10.1504/IJWGS.2018.095647

[11] V. Malinov, V. Zhebka, I. Kokhan, K. Storchak, T. Dovzhenko, Cryptocurrency as a Tool for Attracting Investment and Ensuring the Strategic Development of the Bioenergy Potential of Processing Enterprises in Ukraine. Lect. Notes Data Eng. Commun. Technol., 2024, 195, p. 387-405, doi:10.1007/978-3-031-54012-7_17

[12] V. Malinov, V. Zhebka, O. Zolotukhina, T. Franchuk, V. Chubaievskyi, Biomining as an Effective Mechanism for Utilizing the Bioenergy Potential of Processing Enterprises in the Agricultural Sector. In: CEUR Workshop Proceedings, 2023, 3421, p. 223-230.