TECHNICAL REPORT

An Evaluation System for Selecting the Suitable Distributed Ledger Technology (DLT) for a given use case, leveraging the proposed Decision Tree and Grading System Framework

Author: Dr Michal Kit
Principal Technology Officer
Emerging Technology Division
Blockchain & Climate Institute

Contributor: Dr Luke Riley
Head of Standards Development
Emerging Technology Division
Blockchain & Climate Institute

Contributor: Dr Thusitha Bandara
Deputy Chief Technology Officer
Emerging Technology Division
Blockchain & Climate Institute

Contributor: Mr Chris Poulloura
Chief Technology Officer
Emerging Technology Division
Blockchain & Climate Institute

Contributor: Mr Alastair Marke
Director-General
Blockchain & Climate Institute

Executive Summary

Distributed Ledger Technology (DLT), particularly blockchain, is widely regarded as a transformative innovation with the potential to revolutionize various industries, akin to the impact of the internet. Blockchain, a type of DLT, is a decentralized digital ledger that records data immutably and securely, enabling digital asset transactions without relying on intermediaries. Its decentralized nature, underpinned by cryptographic security and consensus mechanisms, makes it a robust and transparent platform for digital transactions and data management. This has led to its growing adoption across sectors such as finance, healthcare, logistics, and legal services, where it provides significant benefits in terms of cost reduction, transparency, and operational efficiency.

However, despite its promise, blockchain technology is not a one-size-fits-all solution. The enthusiasm surrounding blockchain's potential can sometimes lead to overestimations of its capabilities, resulting in costly projects that do not deliver the expected value. The challenges of blockchain, including energy consumption, computational costs, and complexity, necessitate a cautious approach to its adoption. This highlights a crucial gap in understanding when and how DLT solutions are most appropriate, considering that each use case may have unique requirements that do not align with the inherent characteristics of blockchain or other DLTs.

To bridge this gap, this paper proposes a systematic decision-making framework to guide organizations in evaluating the suitability of DLT solutions. The proposed framework consists of two key components: a **Decision Tree** and a **Grading System**. The Decision Tree provides a structured path to determine whether a DLT is needed and what type of network configuration (public permissionless, public permissioned, or private permissioned) is most appropriate. Following this, the Grading System offers a set of criteria to evaluate and prioritize shortlisted DLT options based on the specific needs of a given use case. By combining these tools, the framework enables decision-makers to make informed, strategic choices about integrating DLTs into their operations.

The primary objective of this paper is to develop a comprehensive process for selecting the most suitable DLT and/or DLT network for any given scenario. The framework addresses both objective and subjective aspects of DLT evaluation, providing clear decision pathways that guide users through critical considerations and criteria. The approach is validated through examples demonstrating its application across various use cases, ensuring that organizations can navigate the complexities of DLT adoption with confidence and clarity, ultimately enhancing decision-making efficiency and reducing associated risks.

1. Introduction

Distributed Ledger Technology (DLT), particularly blockchain, is often described as a transformative innovation that has the potential to revolutionize industries in the same way the internet did. Blockchain, as defined by Singh and Gupta (2018), is a digital ledger system that records and stores data in an immutable and secure manner, enabling the transfer and storage of digital assets without relying on third-party intermediaries. Utilizing cryptography for ensuring the security and validity of transactions, blockchain operates within a decentralized network managed by distributed computers, creating a robust and transparent platform for digital transactions and data management.

The appeal of blockchain technology is evident in its growing adoption across various sectors, such as finance, healthcare, logistics, and legal services. For instance, in the financial industry, blockchain is used to reduce transaction costs, increase transparency, and expedite the settlement of transactions. In healthcare, it offers secure and transparent methods for storing and managing patient records. Similarly, in logistics, blockchain enhances supply chain efficiency by enabling real-time tracking of shipments. These examples highlight blockchain's potential to improve business operations significantly by offering increased security, transparency, and cost-effectiveness.

Despite the promising potential of blockchain technology, there is a need to approach its adoption with caution. There is a risk of overestimating blockchain's capabilities, which could lead to the implementation of projects that ultimately fail to deliver value, often referred to as "white-elephants". This concern underscores a crucial gap in understanding when blockchain or any DLT is the best solution for a given scenario. Blockchain's decentralized nature and reliance on consensus mechanisms, such as Proof of Work (PoW), can introduce complexities and significant costs, particularly in terms of energy consumption and computational resources (Lin, 2020). Additionally, the technology may not always align with the specific needs or constraints of every industry, organization, or application.

Given these challenges, it is clear that a systematic approach is needed to guide organizations in evaluating the suitability of DLT solutions for their unique requirements. This systematic method would help decision-makers assess whether blockchain, or any other form of DLT, is appropriate for their specific context and, if so, which type of DLT configuration (such as permissionless public networks, permissioned private networks, etc.) best meets their needs. Without such a framework, organizations may either miss out on the potential benefits of DLT or, conversely, invest in complex and costly blockchain solutions that are not well-suited to their operational realities.

To address this gap, a decision-making framework, such as a decision tree, is proposed to systematically guide evaluators through the process of determining the necessity and suitability of DLT for specific use cases. This approach will help in navigating the complexities associated with DLT adoption, providing clarity on when and how blockchain can be a valuable tool, and ensuring that organizations can make informed, strategic decisions about integrating this transformative technology into their operations.

The primary objective of this project is to develop a comprehensive process for an evaluator to select a Distributed Ledger Technology (DLT) and/or a DLT network for any given use case. Given the complexities involved, it is recognized that determining the most suitable DLT or DLT network for a specific use case is inherently a subjective decision, albeit one that must be grounded in objective criteria and facts.

To navigate this complexity, an "Evaluation Process" is essential. This process involves a systematic approach to assessing and analysing various options based on a set of predefined criteria, ensuring that decision-making is both objective and comprehensive while aligning with strategic goals. Typically, this involves several stages, including defining objectives, identifying relevant evaluation criteria, prioritizing these criteria based on their importance, and applying them to the available options to identify the most suitable choice (Jimenez & Mateos, 2011). Such a structured framework not only minimizes bias and enhances clarity but also supports informed decision-making by stakeholders. The evaluation process is widely applied across fields like technology selection, policy analysis, and project management, where decisions must be justified through clear, evidence-based reasoning (Liu & Clemen, 1992).The DLT evaluation process proposed in this paper is composed of two main sections:

- **Decision Tree**: The decision tree presents questions, that can be answered objectively, regarding whether a DLT is required at all, and if it is, what network design is required (with the options being public permissionless, public permissioned, or private permissioned).
- **Grading System**: The grading system presents key criteria that DLTs can be analysed on. For the given use case, the evaluator must identify the essential criteria, discard the redundant criteria, and prioritise the remaining criteria. Subsequently, the evaluator will analyse all shortlisted DLT options, according to the relevant criteria for this use case.

This DLT evaluation process aims to guide organisations through the complexities of choosing appropriate DLT/Blockchain technologies based on their specific needs and operational requirements. By providing a systematic and structured approach, the process will assist evaluators in making informed decisions, reducing the risks associated with technology adoption, and enhancing the overall efficiency of business.

Key objectives include the:

- **Evaluation of the Approach:** To detail a process that allows different distributed ledger technologies and networks to be evaluated according to objective and subjective aspects.
- **Clarification of Decision Criteria**: To identify and define the critical criteria and factors that influence the decision to adopt distributed ledger technologies.
- **Development of Decision Pathways**: To construct decision pathways that guide users through a series of questions and considerations, ultimately leading to a recommendation on whether any distributed ledger technology is appropriate for their specific scenario and if so, what would be the most suitable DLT and/or DLT network.
- **Provision of examples validating the approach**: To offer detailed analysis and examples of various use cases where the DLT evaluation process can be successfully applied.

By achieving these objectives, the project aims to deliver **a proposal for** a robust decision-making tool that empowers organisations to navigate the complex landscape of distributed ledger technologies effectively in ISO/TC 307 Blockchain and Distributed Ledger Technologies and/or CEN-CLC JTC19 Blockchain and Distributed Ledger Technologies.

This technical report provides a structured approach to evaluating DLT solutions and is structured in the following sections. **Section 2: Methodology** outlines the **Guiding Principles** and describes the **Decision-Making Framework** that supports the evaluation. **Section 3: Example User Persona** presents four illustrative scenarios to demonstrate the framework's application. **Section 4: DLT Evaluation Process** provides an overview on the main steps of the approach, starting with the **Decision Tree Evaluation Step** in **Section 5**, followed by **Section 6: Assessing Grading System Criteria**, which covers **Objective** and **Subjective Criteria**. **Section 7** elaborates on the criteria prioritisation, leading to **Section 8: Grading System Criteria Evaluation** and the final **DLT Selection** in **Section 9**. The report concludes with **Section 10: Conclusion**, summarizing key findings, and **Section 11: Future Work**, suggesting areas for further research.

2. Methodology

2.1. Guiding Principles

The development of a robust and effective DLT Decision Tree requires careful consideration of several key factors that guide the evaluation process. In the complex landscape of distributed ledger technologies (DLTs), where numerous solutions and variations exist, the need for a clear and structured methodology becomes essential. The intricacy of blockchain and DLT concepts often poses significant challenges to stakeholders, particularly when technical jargon and complexities obscure the decision-making process. Therefore, it is vital that the evaluation framework is designed to be straightforward and accessible, allowing stakeholders with diverse levels of technical expertise to engage meaningfully. By ensuring that the process is simple and easy to follow, the methodology aims to democratize the evaluation of DLTs, enabling a more inclusive and informed decision-making environment.

To effectively guide users through the evaluation process, the methodology must also be centered around specific goals and objectives that an organization seeks to achieve with DLT adoption. Whether driven by a need for increased transparency, enhanced security, operational efficiency, or cost reduction, the framework is structured to help evaluators assess how well different DLT solutions meet these unique organizational needs. This goal-centric approach ensures that decisions are aligned with strategic objectives, making the evaluation process more relevant and actionable for decision-makers.

Additionally, the methodology must account for the unique requirements and constraints that different contexts impose on DLT adoption. Each industry or use case presents distinct challenges, such as regulatory compliance, adherence to industry standards, or specific data handling needs. By incorporating these context-specific considerations, the framework offers a more comprehensive and realistic approach, reflecting the practical realities of deploying DLTs across diverse scenarios. This adaptability is crucial for providing tailored recommendations that align with the specific demands of various stakeholders, thereby enhancing the overall effectiveness and applicability of the DLT Decision Tree.

Below are the key guiding principles:

1. Clarity and Simplicity

The DLT evaluation process must be simple to understand and use. Each consideration should be clearly defined, avoiding technical jargon where possible. The goal is to make the DLT evaluation process accessible to a broad audience, including stakeholders who may not have a deep technical background.

2. Goal Orientation/System Reliability

The DLT evaluation process should be goal-oriented by being aligned with the specific goals and requirements of the organisations that the evaluator represents. This involves identifying the primary motivations for considering DLT, such as transparency, security, efficiency, or cost reduction. The DLT evaluation process should guide the user towards evaluating how well each DLT (and potentially each DLT network) meets these motivations.

3. Context Awareness

Different use cases in different industries have unique requirements and constraints. The DLT evaluation process must account for the specific context in which the technology will be deployed. This includes regulatory considerations, industry standards, and the nature of the data and transactions involved.

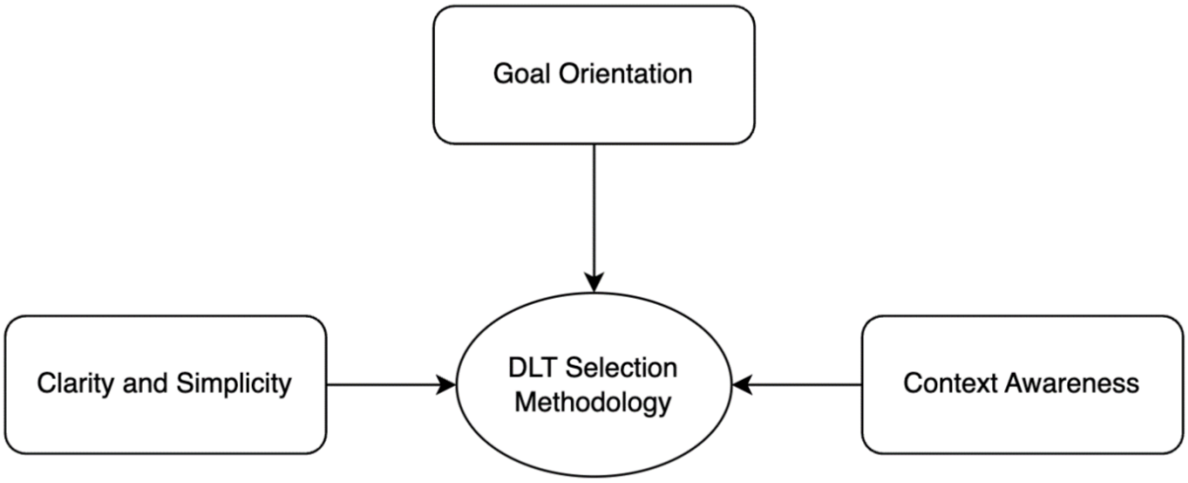

Figure 1 DLT Selection Methodology Guiding Principles

These guiding principles form the foundation of the methodology, ensuring that the evaluation process remains clear, goal-oriented, and context-aware, ultimately supporting more strategic and informed decisions in the evolving field of distributed ledger technologies.

2.2. Decision-Making Framework

To develop a decision-making framework for evaluating DLT options, a systematic analysis of the organizational goals, technical realities, and guiding principles that drive the decision-making process in technology adoption was conducted. The guiding principles **Clarity and Simplicity**, **Goal Orientation**, and **Context Awareness** - were used to inform a structured methodology to ensure that the decision tree is a robust, user-friendly tool for decision-makers. In this section, the methodological steps are detailed to show how the decision tree was structured and how the grading system was implemented to enable evaluators to systematically identify the most suitable DLT or conclude that DLT is not required.

2.2.1. Methodological Steps in Developing the Decision Tree

Step 1: Structuring the Decision Tree Evaluation Steps

To ensure a systematic and clear decision-making process, the decision tree was structured to sequentially guide the evaluator through a series of gates. The process was designed to continue until the evaluator arrives at either an end gate indicating "DLT is not required" or other end gates that prompt further evaluation steps. This structure was considered essential for maintaining clarity and simplicity in the evaluation process, preventing users from becoming overwhelmed by unnecessary complexity at the outset.

- **Decision Tree Evaluation Step**: The evaluators are guided through the decision tree step-by-step, passing through each decision point based on predefined criteria. This process was modelled on proven methodologies such as decision support systems in IT management, where users are led through structured decision paths, ensuring that each decision is logically and sequentially justified Click or tap here to enter text..By breaking down the process into manageable segments, the decision-making becomes more transparent and less prone to error, aligning with the guiding principle of Clarity and Simplicity.

- **Shortlisting DLT Options**: After the evaluator reaches an end gate within the decision tree, a shortlisting process is required to determine which DLTs or DLT networks meet the specific criteria outlined at that point. This shortlisting step mirrors the filtration process commonly found in Multi-Criteria Decision Analysis (MCDA) frameworks, where potential solutions are narrowed down based on their ability to meet critical requirements Click or tap here to enter text..This method ensures that only the most viable options are considered in subsequent stages, thus maintaining a focus on Goal Orientation by aligning the options with the organization's strategic objectives.
- **Grading System Criteria and Evaluation**: Once the shortlisting of DLT options has been completed, the next steps involve a thorough evaluation of the shortlisted options based on a grading system. The evaluation is divided into two main steps—analysing the essential criteria and then the optional criteria. This structure allows for a layered approach, similar to the Analytic Hierarchy Process (AHP), where options are evaluated against a hierarchy of criteria to identify the best fit Click or tap here to enter text..By breaking down the evaluation into these two steps, a more nuanced and adaptable decision-making process is enabled, aligning with the guiding principle of Context Awareness by taking into account industry-specific and situational factors.

Step 2: Implementing the Grading System and DLT Selection

After the structure of the decision tree has been established and the evaluation steps are clearly defined, the grading system is implemented to differentiate between essential and optional criteria, allowing for a comprehensive assessment of each DLT option. This step is crucial for refining the selection process and ensuring that the final decision aligns with both the strategic goals and specific context of the organization.

- **Essential Criteria Step**: In the first stage of the grading system, the evaluator is required to analyse the shortlisted DLTs and DLT networks against essential criteria. This stage functions as a strict filter, where any DLT or network that does not meet these non-negotiable criteria is immediately discarded. This approach is based on exclusionary screening techniques often used in procurement and policy evaluation, where options must pass fundamental checks to be considered further Click or tap here to enter text. This step ensures that only viable options are allowed to proceed, thus enhancing decision-making efficiency, and reducing the risk of pursuing unsuitable technologies.
- **Optional Criteria Step and DLT Selection**: After the essential criteria have been applied, the remaining DLTs or DLT networks are further analysed against a set of optional criteria. This stage prioritizes flexibility and adaptability, allowing for a more tailored evaluation that considers additional, but not necessarily critical, factors. This layered evaluation has been found effective for situations requiring detailed, context-specific decisions. Studies in adaptive decision-making processes, such as those by Kahneman and Tversky Click or tap here to enter text., support the effectiveness of such nuanced approaches, where optional criteria provide additional layers of refinement without overwhelming the decision-maker with complexity.
- **DLT Selection Step**: Following the evaluation against essential and optional criteria, the final grades of all remaining DLT or DLT network choices are processed to reach a conclusion on the most suitable option. This final step ensures that the decision is based on a comprehensive analysis of all relevant factors, aligned with both organizational goals

and contextual requirements. The use of such grading and selection processes has been validated in various fields, including technology adoption and software selection, where structured decision-making frameworks like AHP have proven successful Click here to enter text.Click or tap here to enter text..

Justification for Using the Decision Tree Approach

The decision tree approach has been deemed particularly well-suited for evaluating DLT options because it provides a structured, step-by-step process that aligns with organizational goals, technical realities, and unique industry contexts. The approach is systematic and comprehensive, minimizing ambiguity and ensuring transparency in the decision-making process. The decision tree's sequential evaluation mechanism allows for flexibility in dealing with diverse criteria and requirements while maintaining a clear and straightforward user experience.

Empirical examples from other domains have shown the efficacy of decision trees in systematic software and technology selection processes. For instance, decision trees have been successfully used in the selection of Enterprise Resource Planning (ERP) systems, as documented by Al-Mashari et al.(Al-Mashari et al., 2003). Similar methodologies have also been employed in medical decision-making systems, where decision trees help navigate complex, multi-criteria decisions (Patel et al., 2002).

By grounding the decision tree in robust decision science literature and aligning it with guiding principles - Clarity and Simplicity, Goal Orientation, and Context Awareness - the framework has been designed to provide a systematic, transparent, and effective approach to DLT evaluation. It incorporates best practices from decision-making theories and adapts them to the specific needs of DLT selection, ensuring that evaluators are well-equipped to make informed, goal-aligned decisions. The proposed methodology is not only practical and accessible but also adaptable to a range of contexts, further supporting its effectiveness and applicability.

3. Example User Personas

To assist the user in considering the practical implications of the DLT evaluation process, four example user personas in fictitious scenarios are introduced that will help stakeholders anchor all the following sections. Meanwhile, it is important to note the personas described in this section are no templates for specific use cases and serve only the purpose of illustrating the idea presented in this technical report. There might be other similar use-cases that have specific requirements for which the DLT evaluation process outcome might be different. This approach aligns with the guiding principles by ensuring that the evaluation process remains context-aware, goal-oriented, and adaptable to the unique requirements of different scenarios.

3.1. (A) NPO building a Sustainable Energy Trading System

Scenario 1: Consider a non-profit organisation that plans to build an energy trading system, aimed at promoting sustainable development with transparent transactions between energy producers and consumers, the system would ensure transparency through public transactions so that all transactions can be recorded and auditable in real-time. Participants would be KYC-ed (Know Your Customer) to verify their legitimacy and trustworthiness, ensuring compliance with regulations. Trading rules are required to be publicly verifiable and enforceable, whereas trades should be automatically executed. To align with the UN Sustainable Development Goals, the system is required to be energy-efficient by utilising low-energy solutions and optimised infrastructure. The final system must be secure and tamper-proof, incorporating advanced encryption, and regular security audits to protect against fraud and cyber-attacks. Given the NPO's focus on minimal costs, the system can leverage open-source solutions, cloud services, and volunteer contributions to minimise expenses while maintaining high functionality and reliability.

The NPO will be selecting an evaluator that will balance the requirements of the NPO, the energy producers and the energy consumers.

3.2. (B) Bank Consortium

Scenario 2: Consider a consortium of banks who plan to build a shared system which will be a highly secure and tamper-proof platform, ensuring the integrity and confidentiality of all financial transactions. Participation in the system is restricted to KYC-verified and regulated financial institutions, each of which maintains its own IT infrastructure. Transactions conducted within this system are private and exclusively visible to the involved parties, safeguarding the sensitive nature of money transfers. To accommodate a growing volume of transactions, the system to be built must efficiently handle increasing loads while maintaining a deterministic transaction finality time. Additionally, the underlying technology chosen will need to have robust support and continuous updates, ensuring the system's reliability and long-term viability.

The bank consortium will be selecting an evaluator that will balance the requirements of all the banks.

3.3. (C) DeFi Application

Scenario 3: Consider a company building a DeFi application for a fungible token exchange which will be an inclusive, decentralised platform accessible to everyone. Participants will create wallets without the need for KYC verification, ensuring ease of access and privacy. All transactions conducted on the platform can be publicly visible to maintain transparency within the ecosystem. The system does not require deterministic transaction finality times, allowing for flexible processing speeds. It is assumed that this system will be built on top of an established network, allowing ease of integration into a current network's DeFi ecosystem.

The DeFi application-building company will be selecting an evaluator with knowledge of this domain to perform the evaluation on their behalf.

3.4. (D) Internet of Things (IoT) Platform

Scenario 4: Consider a property management company providing a platform for home IoT (smart) devices owned by users, each user registered on the platform can view their home environments that consist of multiple devices. Each sensing device will update its current state with the platform while the actuating device will make changes to its state when triggered by the platform (e.g. in response to user activity). The system requires a quick response time to ensure user experience. The platform should support the ingestion of a large number of small portions of data coming from millions of devices. Therefore, it should be scalable in terms of storage and processing power.

Again, the IoT Platform developer will be selecting an evaluator who understands the specifics of the IoT domain and can run the DLT evaluation process on their behalf.

4. The DLT Evaluation Process

In this section, every step of the DLT evaluation process will be introduced and described. Firstly, at a high level and then in detail in its own sub-section. In each sub-section, reference to the user personas will be given to anchor the discussion.

The three steps of the DLT evaluation process are as follows:

A. **Decision Tree Evaluation Step**: The evaluator will go sequentially through each gate of the decision tree, until either the evaluator is led to the 'DLT is not required' end gate (in which case the evaluation process for this use case concludes here), or the evaluator is led to any of the other end gates in which case the evaluation process will continue (see page 14 for more details).
B. **Shortlisting DLT Options**: The evaluator, having reached the Decision Tree's end gate, must now shortlist DLTs and/or DLT networks that meet the criteria specified in the particular end gate reached, i.e. whether the DLT can be configurable as 'permissionless public network,' 'permissioned private network,' or 'permissioned public network' (see page 20).
C. **Assessing the Grading System Criteria**: The evaluator now needs to go through each of the grading system criteria, indicating which ones are essential, and which are redundant, and then prioritising the remaining ones (see page 22).
D. **Grading System Evaluation Step**: The evaluator now needs to analyse the shortlisted DLTs and/or DLT networks, according to the grading system criteria.
    i. Essential Criteria Step: Firstly, the evaluator needs to analyse the shortlisted DLTs and/or DLT networks according to the essential criteria. Whenever a DLT/DLT network does not match the essential criteria, it is immediately discarded as an option.
    ii. Optional Criteria Step: Secondly, the evaluator needs to analyse all of the remaining DLT and/or DLT networks according to all of the optional criteria.

    For more details see page 39.
E. **DLT Selection Step:** The evaluator now needs to process the grades of all of the remaining DLT or DLT network choices to come to a final conclusion on which specific DLT or DLT network to select (see page 50).

5. Decision Tree Evaluation Step

The main goal of the decision tree portion of the DLT evaluation process is to determine if the evaluator truly needs a DLT for the specific use case and, if so, what type of DLTs should be shortlisted for the grading portion of the DLT evaluation process. The Decision Tree Evaluation Step is the first step in this structured approach and serves as the foundation for guiding evaluators through a clear decision-making pathway. This step utilizes a set of Yes/No questions, which have been carefully derived from the methodology approach outlined earlier, ensuring that each decision point is grounded in logical reasoning and objective criteria. These binary questions help break down complex considerations into simpler, more manageable parts, allowing evaluators to systematically assess the necessity of a DLT and its optimal configuration—whether it be a public permissionless, public permissioned, or private permissioned network. By starting with the Decision Tree Evaluation Step, the process ensures that only relevant DLT options are considered, aligning with the principles of clarity, goal orientation, and context awareness, and paving the way for a more focused and effective evaluation in subsequent steps.

The following questions determine at the early stage of the DLT evaluation process whether the DLT is needed:

- **Q1 - "Do you need a shared common database?"** - This question helps determine whether multiple parties require real-time access to a single source of truth, with all participants needing assurance of data integrity, transparency, and consistency without relying on a central authority. If the answer is "Yes", DLT becomes highly useful as it enables decentralised data management, where all stakeholders can view and verify transactions in a secure, immutable, and transparent manner. Conversely, if the data-sharing requirements are limited to within a single organisation or do not necessitate real-time, tamper-proof verification by multiple entities, a conventional database may suffice, offering simplicity, speed, and cost-efficiency without the complexity of DLT systems.
- **Q2 - "Are multiple parties involved?"** - This question is crucial in decision-making for choosing between DLT and a traditional database because it directly addresses the need for a decentralised system. DLT is particularly useful when multiple independent entities require a shared, immutable ledger to record and verify transactions without relying on a central authority. This is essential in scenarios where trust between parties is low, and transparency, security, and consensus are critical. If multiple parties need to collaborate but maintain their autonomy while ensuring data integrity and authenticity, DLT provides a robust solution. Conversely, if only a single entity or closely trusted entities are involved, a traditional database might suffice, offering simpler, faster, and more cost-effective data management without the overhead of maintaining a decentralised network.
- **Q3 - "Do the involved parties have conflicting interests/trust issues?"** - If the involved parties have conflicting interests or trust issues, DLT becomes highly useful as it ensures transparency, immutability, and decentralised control, reducing the need for a trusted central authority. DLT's consensus mechanisms allow all parties to verify transactions independently, fostering trust even among adversarial entities. Conversely, if there are no significant trust issues and all parties operate under a unified, trustworthy governance system, again, a traditional database might suffice.
- **Q4 - "Do the parties want to/Can the parties avoid a trusted third party?"** - If the involved parties prefer or require a system where no single entity has control, DLT becomes a highly valuable solution. Conversely, if parties are comfortable with a central

authority managing the database, for example, due to performance-related reasons, a traditional database might be a better choice.

- **Q5 - "Is there a need for an objective immutable log?"** - This question probes the necessity of maintaining a tamper-proof record of transactions or data entries, which is a fundamental feature of DLT systems. If the application requires a transparent, unalterable history of activities, such as in financial transactions, supply chain tracking, or compliance reporting, an immutable log ensures trust and accountability among parties. In contrast, traditional databases allow for data modification and deletion, which may not be suitable for scenarios where data integrity and transparency are paramount. Therefore, if the answer to this question is affirmative, it strongly indicates the appropriateness of adopting DLT over a conventional database to fulfil these specific requirements.
- **Q6 - "Do the transacting rules remain largely unchanged?"** - If the transacting rules are stable and unlikely to change, a Multiparty Computation (MPC) Click or tap here to enter text. solution deployed over a traditional database might be more appropriate due to its established frameworks and ease of management. is a cryptographic protocol that enables multiple parties to jointly compute a function over their inputs while keeping those inputs private. In MPC, each party provides its data without revealing it to others, and the protocol ensures that no individual party learns anything about the other parties' inputs, except what can be inferred from the final result. MPC is widely used in scenarios where privacy is crucial, such as secure voting, private data analysis, and collaborative machine learning, allowing parties to compute results securely without compromising their sensitive information. MPC excels in environments with multiple conflicting parties without a governing entity. Conversely, if transacting rules are expected to evolve or if there is a need for greater flexibility, transparency, or decentralisation in how transactions are processed and validated, DLT could be advantageous. DLTs are designed to handle dynamic, decentralised environments where rules can change and be governed by consensus among participants, making them ideal for applications requiring high levels of security, transparency, and resistance to tampering or fraud.
- **Q7 - "Do the rules governing system access differ between participants?"** - If the answer is "Yes", it suggests a need for a decentralised approach where different participants require distinct access controls, indicating that DLT could be more suitable. DLT inherently supports varied access rules through its consensus mechanisms and permissioned or permissionless structures, allowing for fine-grained control over who can read, write, or validate transactions. This contrasts with traditional databases, which typically rely on centralised access control models that may not accommodate complex, multi-party access requirements as effectively. Nevertheless, a solution more suitable in a non-uniform access scenario without a governing party might be MPC with an access control framework, which would help to mitigate the issues around different rules governing the data access among participants.
- **Q8 - "Do you need the participants to be verified?"** - If the answer is "no," indicating that anyone can participate without identity verification, a permissionless DLT is typically required. Permissionless DLTs, like public blockchains, allow anyone to join and contribute to the network, making them suitable for open, decentralised environments where trust is established through consensus mechanisms rather than participant identity. Conversely, if the answer is "yes," and participants must be verified, this points to the need for a permissioned DLT, either public or private. In a permissioned DLT, access is restricted to verified participants, which enhances security and control, making it ideal for scenarios where participant identity and roles need to be managed tightly, such as in

financial institutions, supply chains, or consortium networks. The next question will help to give a definitive answer.

- **Q9 - "Are the transactions visible to everyone in the network?"** - If the answer is "no," meaning that transaction visibility needs to be restricted to specific participants, this indicates a need for a private permissioned DLT. In this model, only authorised and verified participants can access and validate transactions, ensuring privacy and confidentiality within a controlled network, which is crucial for industries like healthcare or finance where sensitive data is involved. On the other hand, if the answer is "yes," and all transactions should be visible to everyone within the network, a public permissioned DLT is more appropriate. This model still requires participant verification but operates in a more transparent environment where every network participant can observe and validate transactions, making it suitable for scenarios where transparency and accountability among trusted entities are paramount, such as in consortiums or regulated industries.

Should the evaluator reach the **'DLT not required'** end gate, then the evaluation process concludes here as the given use case does not need a DLT network to be integrated. Otherwise, the evaluator will have reached one of the other end gates stating that they need a particular type of DLT network, where each option is described below:

- **Permissioned private DLT network**: only an authorised set of entities can participate in this network, and only an authorised set can read the data on this network.
- **Permissioned public DLT network**: only an authorised set of entities can run a node of this network, yet anyone can read the data on this network.
- **Permissionless public DLT network**: anyone can run a node of this network, and anyone can read the data placed on the network.

Figure 2, below, depicts the above process graphically.

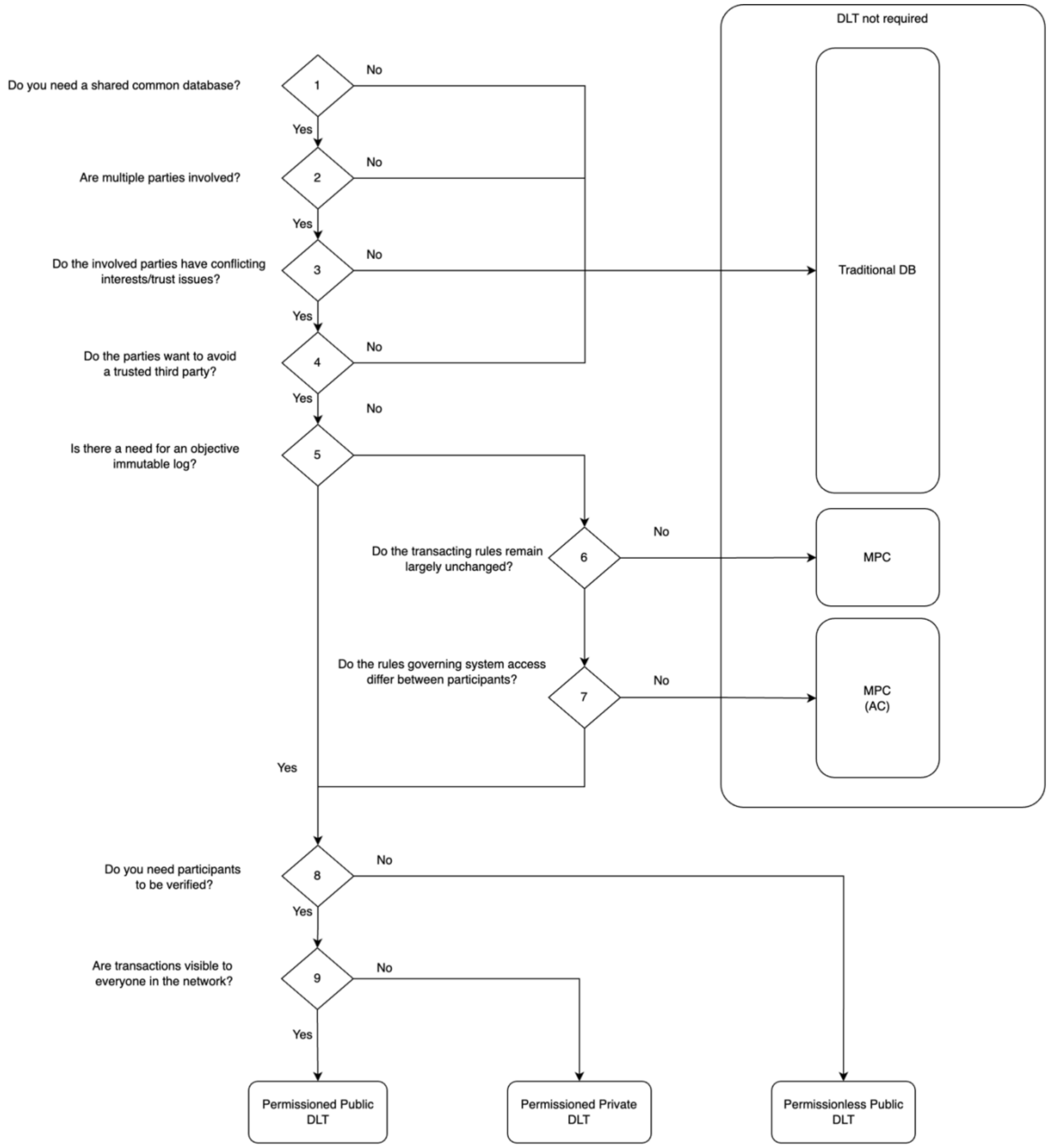

Figure 2 Decision Tree Evaluation Step

5.1. User Persona Examples

The following table illustrates the Decision Tree Evaluation Step executed against the personas and relevant contexts defined in Chapter 3.

Decision Tree Question	NPO Evaluator Responses (A)	Bank Consortium Evaluator Responses (B)	DeFi Application Evaluator Responses (C)	IoT Platform Evaluator Responses (D)
Q1 - “Do you need a shared common database?”	YES	YES	YES	YES
Q2 - “Are multiple parties involved?”	YES	YES	YES	YES
Q3 - “Do the involved parties have conflicting interests/trust issues?”	YES	YES	YES	YES
Q4 - "Do the parties can/want to avoid a trusted third party?"	YES	YES	YES	NO
Q5 - "Is there a need for an objective immutable log?"	YES	YES	YES	
Q6 - "Do the transacting rules remain largely unchanged?"	YES	YES	YES	
Q7 - “Do the rules governing system access differ between participants?”	YES	YES	YES	
Q8 - “Do you need the participants to be verified?”	YES	YES	NO	
Q9 - “Are the transactions visible to everyone in the network?”	YES	NO		

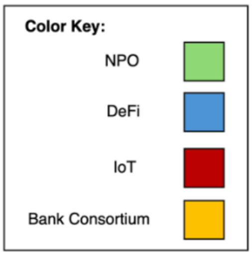

Table 1 DLT Decision Tree Evaluation Step - Example Personas Evaluation

The above table consists of the example answers that the evaluator would provide for each of the questions included in the Decision Tree Evaluation Step. The evaluation terminates with a ‘NO’ answer given to any of the questions Q1-Q8 or reaching Q9 with any answer. Another (perhaps clearer) way of presenting this whole process is visualising on the flow diagram as illustrated in

Figure 3 below.

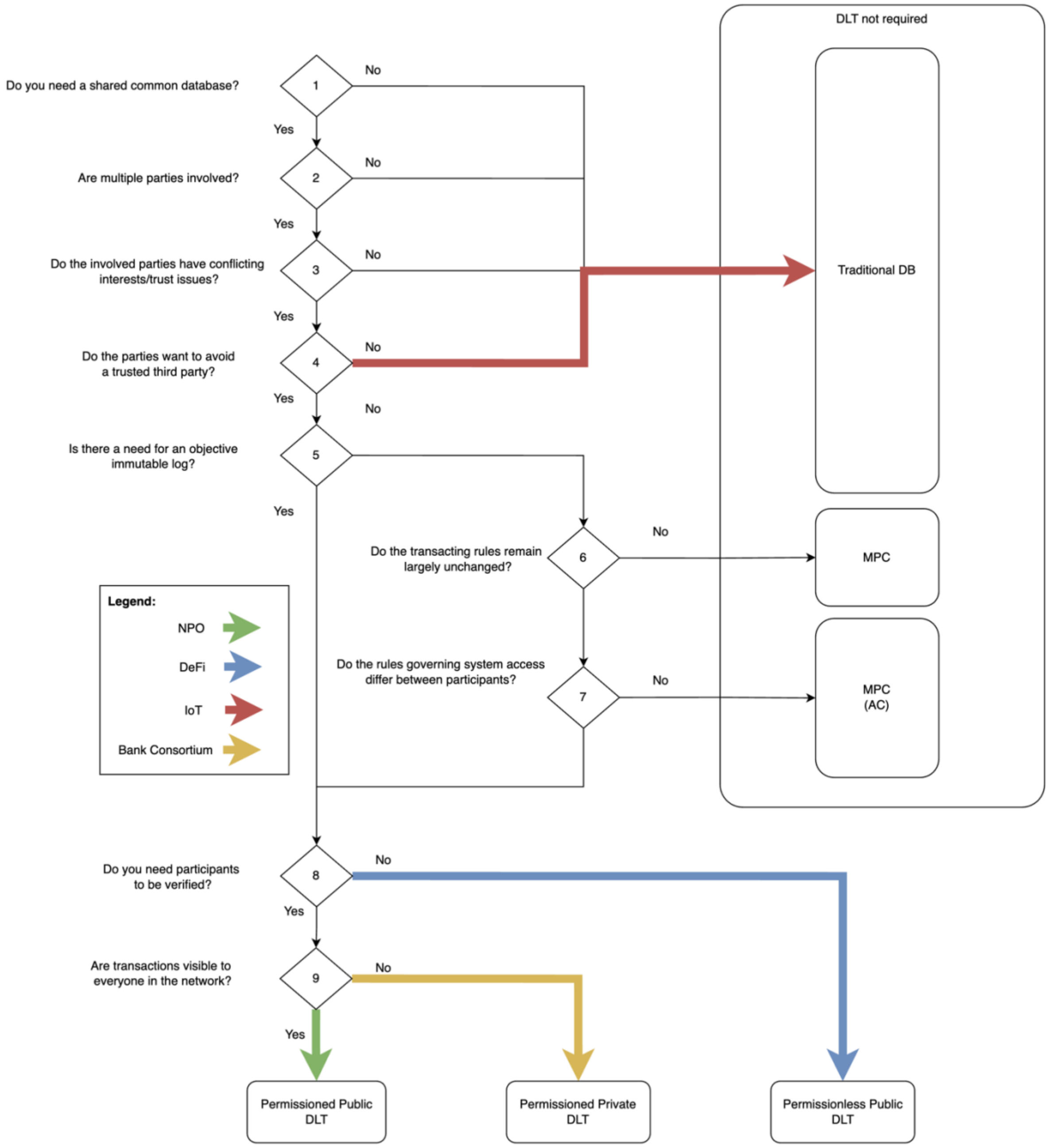

Figure 3 DLT Decision Tree Evaluation Step - Example Personas Evaluation

5.2. Shortlisting DLT Options

If the evaluator determines with the DLT evaluation process that a DLT system is preferable for this particular use case, evaluators must now create a shortlist of either: (a) DLTs configurable to the network type suggested by the Decision Tree; or (b) existing DLT networks already configured as suggested by the Decision Tree.

DLT Networks refer to the specific implementations or instances of DLTs that operate as interconnected ecosystems where nodes (participants) use a particular DLT protocol to validate and share data. Thus, while DLT is the overarching technology framework, DLT networks are its practical applications built to achieve different functionalities.

Examples of each of the DLT categories:

- **Permissioned Private DLT network examples**: If the evaluator determined that a new DLT network needs to be created from scratch, the evaluator would be shortlisting DLTs as an option (***not*** specific DLT networks). That said, it is standard for permissioned private DLT networks to be created from a small number of DLTs, specifically Hyperledger Besu, Hyperledger Fabric, or Corda. Note that Quorum also used to be a popular choice but support for this technology is diminishing, and users are recommended to migrate to Hyperledger Besu (as both DLTs are Ethereum Virtual Machine-based). Additionally, each of the main DLTs for this network type (Besu, Fabric, Corda) has multiple versions that should be considered separate DLTs due to their lack of backward compatibility. Some key version examples are Corda v4, Corda v5, Hyperledger Fabric v1.4, v2.x, v3, and Hyperledger Besu with or without the London hard fork. Finally, the evaluator should be aware that permissionless network-focused DLTs like Cosmos, Substrate, and Avalanche can be configured for permissioned private use. However, due to this non-standard setup, the evaluator should ensure that there is a compelling reason before considering these DLTs as an option.
- **Permissioned Public DLT network examples**: If the evaluator did *not* explicitly assume that a new DLT network needs to be created from scratch, the evaluator could be shortlisting DLTs and/or specific DLT networks. In terms of the DLT options available to the evaluator, gathering these choices will follow similar considerations as discussed in the permissioned private DLT network examples above. The main difference could be that more consideration is provided to DLTs usually designed for permissionless networks, because, as the data is public anyway, the evaluator may consider as beneficial the fact that these DLTs can offer in-built interoperability features to permissionless networks for the same DLT type. For possible DLT network options, the evaluator will have to perform searches for potentially appropriate ones available for the given use case and the given jurisdiction. For example, if the use case operates in the EU, then the DLT network offered by the European Blockchain Services Infrastructure can be appropriate. Whereas if the use case operates in South America, then the DLT network offered by LACNet may be appropriate.
- **Permissionless Public DLT network examples**: If the evaluator assumed that a new DLT network does *not* need to be created from scratch, the evaluator would be shortlisting specific DLT networks. This is because creating a DLT network is an unnecessary additional significant burden for an entity that simply intends to create a blockchain application. For the possible DLT network options, the evaluator should shortlist ones, about which they have a generally positive opinion, out of some of the major networks

(e.g. Ethereum, Solana, Avalanche, Polkadot, Polygon,...) as well as any minor ones that the evaluator wishes to consider (e.g. if they have links to the particular use case).

A representative set of currently available Distributed Ledger Technologies (DLTs) was selected to illustrate the concept of the DLT decision tree in this report. The technologies chosen include Algorand Click or tap here to enter text., Avalanche Click or tap here to enter text., Corda Click or tap here to enter text., Ethereum Click or tap here to enter text., Hedera Click or tap here to enter text., Hyperledger Besu Click or tap here to enter text., Hyperledger Fabric Click or tap here to enter text., Polkadot Click or tap here to enter text., Quorum Click or tap here to enter text., and Solana Click or tap here to enter text..

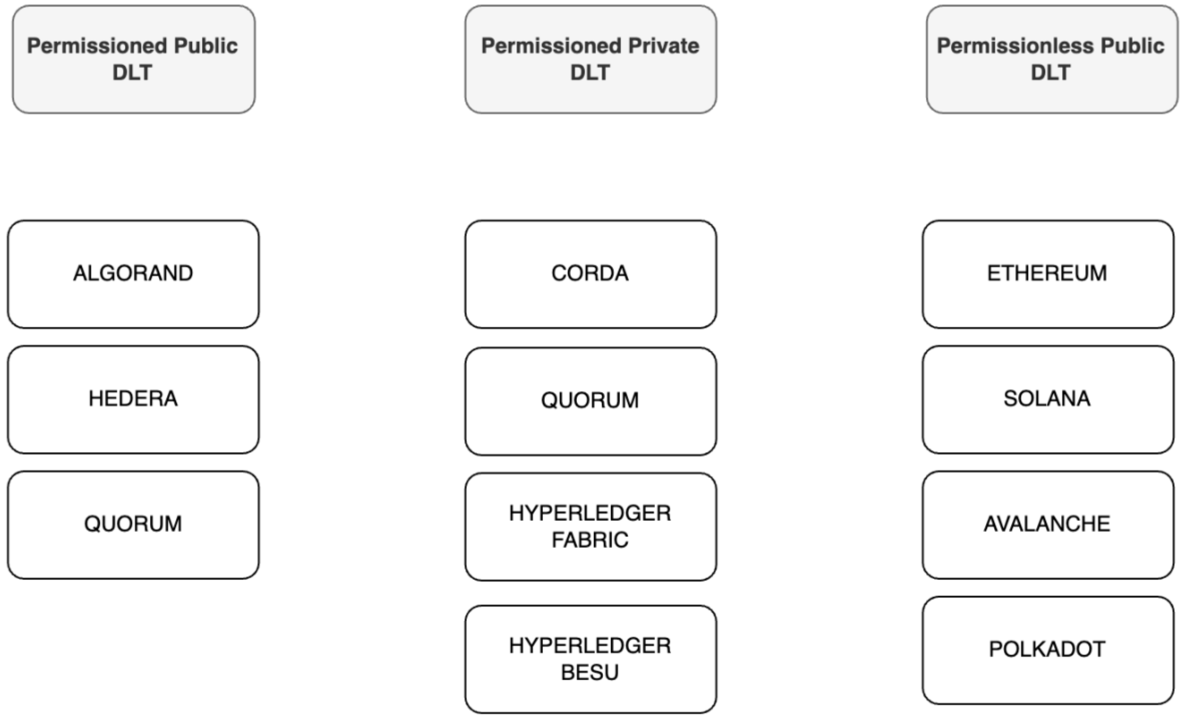

Figure 4 Examples of DLT technologies for each of the DLT category

In the next steps, those lists of DLT technologies above will be filtered out in order to identify the most suitable candidate for the use-cases in evaluation.

6. Assessing the Grading System Criteria

In this section, the criteria for the grading system used in the evaluation process are introduced and divided into two sub-sections: objective criteria and subjective criteria. These criteria can be applied by evaluators to the shortlist of DLTs and/or DLT networks identified in the previous step. When a specific criterion mentioned below refers to a DLT network, it should be understood that, if evaluating from a broader DLT perspective, multiple possible answers or interpretations may exist.

6.1. Objective Criteria

The following criteria are considered objective in the DLT Decision Tree because they are based on concrete, measurable, and technical characteristics of DLTs. These criteria are not subject to subjective interpretation or organizational preferences; instead, they refer to specific features and capabilities that can be evaluated consistently across different DLT platforms. Their objective nature lies in the fact that these characteristics can be clearly defined, quantified, and compared, allowing evaluators to make decisions based on factual, evidence-based analysis rather than subjective judgments or varying organizational contexts.

6.1.1. Programmability

Programmability refers to the ability to deploy and execute custom logic or code on a DLT or DLT network, enabling users to extend the network's functionality beyond its original features. The choices are:

- **None:** In a "none" programmability model, the DLT does not support any form of programmable features or smart contracts. Transactions are executed based solely on pre-defined rules without the ability to customise or extend functionality.
- **Tokens**: In a "tokens" programmability model, the DLT allows users to create and manage digital tokens through predefined scripts or smart contracts. This includes creating, transferring, and managing tokenised assets, which can represent various forms of value or utility.
- **Applications:** In an "applications" programmability model, the DLT supports developing and deploying decentralised applications (DApps) or smart contracts. This model allows users to write and execute complex logic and applications directly on the blockchain, enabling a wide range of functionalities and use cases (including tokenisation).

Programmability Level	Advantages	Disadvantages
None	**Simplicity**: Easier to understand and use, focusing solely on transaction recording and transferring a native asset.	**Limited Functionality**: Restricted to basic functions like simple asset transfers and data recording.

	Security: Fewer attack vectors, reducing the risk of vulnerabilities and exploits.	**Lack of Innovation**: Unable to meet evolving demands for more complex applications.
	Performance: Faster and more efficient transaction processing without the overhead of programmability.	
Tokens	**Token Customization**: Allows creation of custom digital assets, enhancing network functionality beyond simple transactions.	**Complex Use Cases Not Possible**: Unable to implement complex workflows (e.g., "if this, then that") solely with token-based logic.
	Tokenization Use Cases: Supports use cases like digital payments, supply chain tracking, and real-world tokenization schemes.	**Regulatory Challenges**: Token usage may attract scrutiny if considered securities or involve financial transactions.
Applications	**Advanced Tokenization**: Enables both basic and complex tokenization use cases.	**Security Concerns**: Smart contracts and DApps can introduce security risks if not properly audited, leading to exploits and financial losses.
	Versatility: Supports creation of decentralized applications (DApps), smart contracts, and complex business logic, significantly expanding use cases.	**Resource Intensive**: Executing smart contracts requires more computational resources, impacting network performance and scalability.
	Innovation: Encourages innovation by allowing developers to create diverse applications, from DeFi platforms to complex supply chain systems.	**Complex Development**: Developing secure and efficient smart contracts and DApps requires specialized expertise, raising barriers to entry for developers.

The table compares the advantages and disadvantages of DLT networks based on three levels of programmability: **None**, **Tokens**, and **Applications**. Networks with **No Programmability** are simpler, more secure, and have better performance but lack functionality and innovation potential. **Token Programmability** allows for the creation of custom digital assets and tokenization use cases like digital payments but cannot handle complex logic and may face regulatory challenges. **Application Programmability** supports advanced tokenization, versatile DApp creation, and encourages innovation but comes with security risks, requires more resources, and demands specialized development skills, which can limit accessibility.

6.1.2. Transaction Format

Transaction format refers to the structure and organisation of data within a transaction on a DLT or DLT network. Note that this also affects how the ledger data is stored. The choices are:

- **Accounts:** The Accounts transaction format is a model where transactions involve updating balances associated with accounts. Each account has a unique identifier and maintains a balance that can be increased or decreased through transactions.
- **UTXO:** The UTXO (Unspent Transaction Output) transaction format is a model where each transaction creates outputs that are recorded as discrete, spendable units. Each UTXO represents a specific amount of cryptocurrency that has not yet been spent and can be used as an input in future transactions. Each UTXO could be claimable by one or more accounts.

Transaction Format	Advantages	Disadvantages
Accounts	**Simplicity**: Easier to understand and use, similar to traditional financial systems.	**Scalability Issues**: Every transaction modifies the global state, causing potential bottlenecks.
	Smart Contract Implementation: Easier to implement smart contracts.	**Privacy Concerns**: Easier to trace and link transactions to specific users.
	State Management: More intuitive state changes, directly modifying account balances.	**Concurrency Problems**: Simultaneous transactions can lead to conflicts, requiring complex resolution mechanisms.
UTXO	**Parallel Processing**: Allows better parallel transaction processing.	**Complexity**: More complex to implement and understand, requiring careful management of outputs.
	More Easily Auditable Transaction History: Clear linkage of inputs to outputs simplifies auditing.	**Smart Contracts**: More challenging to implement complex smart contracts.
	Flexible Transaction Structuring: Enables combining multiple inputs/outputs for complex transactions.	**State Management**: Requires sophisticated state management for tracking unspent outputs.

The table compares the advantages and disadvantages of using the Accounts and UTXO transaction formats in Distributed Ledger Technologies (DLTs). The Accounts model is simpler and more intuitive, especially for smart contract implementation and state management, but it faces scalability, privacy, and concurrency issues. On the other hand, the UTXO model supports parallel processing, easier transaction auditing, and flexible transaction structuring, yet it is more complex to implement, poses challenges for smart contract development, and requires sophisticated state management. Each format offers distinct benefits and drawbacks depending on the specific use case and design requirements of the DLT.

6.1.3. Ledger Structure

Ledger structure describes how the ledger data is distributed and managed across different nodes in a DLT or DLT network. The choices are:

- **Fully Replicated:** In a fully replicated ledger design, each node maintains a complete copy of the entire ledger, ensuring that every node has access to the full transaction history and state of the network.
- **Sharded:** In a sharded ledger design, the ledger data is partitioned into smaller segments or "shards," with each node responsible for a specific shard. This approach allows nodes to process transactions concurrently within their designated shards. Additionally, the shards can be used for privacy reasons.
- **Hybrid:** A hybrid ledger design combines elements of both fully replicated and sharded approaches. It may involve some nodes maintaining a full copy of the ledger while others handle only specific shards.

Ledger Structure	Advantages	Disadvantages
Fully Replicated	**Consistency**: Complete copy of the ledger across all nodes ensures data consistency.	**Scalability Issues**: High resource requirements as the ledger grows.
	Redundancy: High resilience against node failures; ledger is still accessible.	**Performance Bottlenecks**: Synchronizing the full ledger across all nodes limits transaction speed.
	Security: Difficult for malicious actors to alter the ledger unnoticed.	
	Simplified Verification: Independent transaction verification by all nodes.	
Sharded	**Scalability**: Sharding divides the ledger, improving scalability by distributing storage and processing.	**Complexity**: Requires sophisticated mechanisms for coordination and consistency.
	Improved Performance: Parallel transaction processing across shards enhances throughput.	**Cross-Shard Communication**: Transactions spanning shards can add latency and complexity.
	Efficient Resource Usage: Nodes store and process only a part of the ledger.	**Security Risks**: Shards are potentially vulnerable to attacks like shard takeover if not secured.
	Privacy: Increased privacy as access to each shard can be limited.	

Hybrid	**Balanced Approach**: Combines fully replicated and sharded elements to balance scalability, consistency, and privacy.	**Implementation Complexity**: Designing and managing hybrid structures is complex.
	Flexibility: Provides strong security while maintaining scalability by leveraging redundancy in parts and sharding in others.	**Resource Management**: Managing resources effectively in hybrid systems is challenging.

This table outlines the advantages and disadvantages of different ledger structures in Distributed Ledger Technologies (DLTs). Fully replicated ledgers ensure consistency, redundancy, and security but face scalability and performance issues. Sharded ledgers offer improved scalability, performance, and resource efficiency but are more complex to manage and pose specific security challenges. Hybrid ledgers provide a balanced approach combining elements of both, offering flexibility but requiring complex implementation and resource management.

6.1.4. Transaction Finality

Transaction finality refers to the point at which a transaction, once validated and added to the distributed ledger, is considered irreversible and cannot be undone or altered. In the context of DLT immutability is a core characteristic, meaning that once data is recorded on the ledger, it should remain unchanged and tamper-proof. However, transaction finality can sometimes compromise this immutability. This happens because, in certain DLT systems, mechanisms such as governance, forks, or consensus rule changes may allow for the reversal or modification of transactions under specific conditions. These actions, while sometimes necessary to correct errors, address security breaches, or resolve disputes, create a potential conflict with the fundamental principle of immutability. In other words, if transactions can be reversed or altered after they are recorded, the ledger is no longer perfectly immutable, thus impacting one of the defining features of DLT. The choices are:

- **Deterministic:** Deterministic finality means that once a transaction is validated by the DLT network, it is definitively final and cannot be altered or reversed.
- **Probabilistic:** Probabilistic finality means that the certainty of a transaction being final increases over time, but there is always a non-zero chance it could be reversed or altered.
- **Hybrid:** Hybrid finality describes a process where a transaction initially has probabilistic finality, yet over time transitions to deterministic finality.

Finality Type	Advantages	Disadvantages
Deterministic Finality	**Certainty**: Transactions are final and irreversible once confirmed.	**Consensus Mechanism Pauses**: Safety prioritization may cause network stops during disagreements.
	Simplified Application Logic: No need to handle reversals or reorganizations.	**Scalability Challenges**: May limit transaction throughput and the number of participating nodes.

Probabilistic Finality	**Scalability of Nodes**: Supports a larger number of nodes compared to deterministic networks.	**Uncertainty**: Transactions are never absolutely final; there is a chance of reorganization.
	Decentralization: Allows any node to join the network at any time.	**Latency**: High confidence in finality requires multiple confirmations, increasing transaction latency.
Hybrid Finality	**Flexibility**: Balances between certainty and scalability by combining both deterministic and probabilistic elements.	**Increased Complexity**: Implementation and maintenance are more complex.
	Enhanced Security: Provides robust security by leveraging both types of finality.	**Coordination Overhead**: Requires careful coordination between deterministic and probabilistic components.

The table provides a comparative overview of three types of transaction finality—deterministic, probabilistic, and hybrid—used in DLT/Blockchain networks. Deterministic finality offers certainty and simplified logic but may face pauses and scalability challenges. Probabilistic finality allows greater scalability and decentralization but introduces uncertainty and potential latency issues. Hybrid finality blends the strengths of both, offering flexibility and enhanced security but at the cost of increased complexity and coordination overhead.

6.1.5. DLT (Network) Interoperability

DLT network interoperability refers to the capability of one network of a particular DLT to communicate, share data, and perform transactions with another network of the same DLT type. The choices are:

- **In-built:** In-built interoperability refers to native features or protocols integrated into a DLT network that enable it to directly interact and exchange information with other networks. This can include cross-chain communication mechanisms designed into the network's core infrastructure.
- **Externally Provided:** Externally provided interoperability refers to the use of third-party solutions or services to facilitate interaction between different DLT networks. This can involve middleware, bridges, or interoperability platforms developed outside the core network to enable cross-chain communication and data exchange.

Interoperability Types	Advantages	Disadvantages
Inbuilt Interoperability	**Seamless Integration**: Smooth cross-chain communication and asset transfer within the same ecosystem.	**Limited Ecosystem**: Restricted to chains that adhere to the same protocol or framework.

	Unified Governance: Single governance model across multiple chains.	**Complexity**: Sophisticated architecture needed to support interoperability.
	Optimised Performance: Higher performance and reduced latency for cross-chain transactions.	**Dependence on the Ecosystem**: Reliance on the ecosystem's governance and development pace.
	Security: Standardised security protocols ensure safe cross-chain transactions.	
External Interoperability	**Flexibility**: Can interact with a wide range of other networks through third-party solutions.	**Complex Integration**: Requires significant effort to build and maintain bridges or integration mechanisms.
	Broad Compatibility: Designed to work with many different networks, providing broader integration options.	**Potential Latency**: Additional latency due to cross-network communication.
	Independent Development: Networks can evolve independently, allowing diverse innovation paths.	**Security Risks**: Third-party solutions can introduce vulnerabilities if not well-designed.

The table provides a comparison between inbuilt and external DLT network interoperability. Inbuilt interoperability offers advantages like seamless integration, unified governance, optimised performance, and security but is limited to specific ecosystems, involves complex architecture, and depends on ecosystem governance. In contrast, external interoperability offers flexibility, broad compatibility, and independent development but comes with challenges such as complex integration, potential latency, and security risks associated with third-party solutions.

6.2. Subjective Criteria

The following criteria are considered subjective in the DLT Decision Tree because their evaluation often depends on the specific context, priorities, and risk appetite of the organization or stakeholders involved. Unlike objective criteria that are strictly defined by technical specifications or measurable attributes, these subjective criteria require evaluators to make judgments based on relative importance, trade-offs, and the unique needs of a given scenario. For instance, what one organization might consider "secure" or "cost-effective" can vary greatly depending on its specific industry requirements, available resources, and long-term strategic goals.

The subjective nature of these criteria lies in their dependency on perspective and context, which means they cannot be uniformly assessed across all situations. Instead, they involve a degree of interpretation, prioritization, and weighting based on the evaluator's goals, constraints, and specific use case requirements. This subjectivity necessitates a more flexible evaluation approach where criteria are considered within the framework of an organization's unique objectives and the context in which the DLT solution will be implemented.

For the purpose of this technical report, an arbitrary (and relative) grading is applied to each criterion based on the authors' knowledge and a comprehensive literature review to illustrate the evaluation process. Those gradings can be customised based on the specifics of the scenario and further in-detailed analysis of the DLT solutions. This topic pose as a candidate for future explorations.

6.2.1. Maturity

Maturity refers to the level of development, stability, and adoption of a particular DLT or DLT network. The choices are:

- **High:** Indicates that the DLT has achieved significant development, widespread adoption, and operational stability. It typically has a robust ecosystem, extensive documentation, and a well-established user base.
- **Medium:** Suggests that the DLT is relatively developed and stable but may still be evolving. It has a growing user base and increasing adoption but may not yet have the extensive ecosystem or stability of more mature networks.
- **Low:** Implies that the DLT is still in the early stages of development or adoption. It may have limited use cases, a small user base, and potential stability issues, with ongoing development and experimentation

Maturity Level	Advantages	Disadvantages
High	**Stability and Reliability**: Suitable for mission-critical applications and large-scale adoption.	**Less Flexibility**: Slower to adopt innovations due to established protocols.
	Wide Adoption: Large user base, extensive applications, and widespread integration.	**Inertia**: Governance and development processes may resist significant changes.
	Strong Security: Established security measures minimize risks of vulnerabilities and exploits.	**Complexity**: Increased complexity can lead to challenges in maintenance, upgrades, and governance.
Medium	**Balanced Innovation and Stability**: Offers new features with reasonable reliability.	**Growing Pains**: May encounter scaling issues, governance challenges, or technical debt.
	Growing Ecosystem: Increasing number of users, applications, and integrations.	**Competitive Pressure**: Faces competition from both newer and more mature networks.
	Improving Security: More robust security measures compared to low-maturity networks.	**Partial Adoption**: Struggles to achieve the widespread acceptance of high-maturity networks.
Low	**Innovation Potential**: Open to experimentation and new features.	**High Risk**: Prone to bugs, security vulnerabilities, and instability.
	Community Involvement: Early adopters influence the network's direction and development.	**Limited Adoption**: Fewer users, applications, and integrations limit utility and network effects.

	Opportunity for Growth: Potential for significant growth and industry leadership.	**Uncertain Future**: The long-term viability and success are not guaranteed, posing a risky investment.

The table summarizes the advantages and disadvantages of using DLTs or DLT networks at different maturity levels: high, medium, and low. High-maturity networks offer stability, wide adoption, and strong security but are less flexible and complex. Medium-maturity networks provide a balance between innovation and stability but face challenges like growing pains and competitive pressure. Low-maturity networks allow for innovation and community involvement but come with high risks, limited adoption, and an uncertain future.

6.2.2. Energy Consumption

Energy consumption refers to the amount of electrical energy required to maintain and operate a particular DLT network. The choices are:

- **High:** Indicates that the DLT network requires a substantial amount of electrical energy to operate, often due to resource-intensive consensus mechanisms such as Proof of Work (PoW) Click or tap here to enter text. or large-scale network operations. This can result in significant environmental impact and higher operational costs.
- **Medium:** Suggests that the DLT network has a moderate level of energy consumption. This may be due to less resource-intensive consensus mechanisms or optimisations that balance energy use with network performance.
- **Low:** Implies that the DLT network is designed to be energy-efficient, using minimal electrical power. This is often achieved through energy-efficient consensus mechanisms or other low-power operational approaches.

Energy Consumption Level	Advantages	Disadvantages
High	Strong security through PoW	Significant environmental impact
	High degree of decentralization	High operational costs
	Mature ecosystem with established infrastructure	Negative public perception
Medium	Balanced security and efficiency through hybrid consensus mechanisms	Complexity in implementation and governance
	Better scalability and performance compared to high energy networks	Evolving ecosystem with potential instability
	Improved public perception and fewer regulatory challenges	Not optimal compared to low-energy systems
Low	Environmentally sustainable with minimal carbon footprint	Potential centralization risks due to fewer validators
	Cost efficiency with lower operational expenses	Less proven and may face challenges in achieving

		widespread trust and adoption
	Positive public perception and easier regulatory compliance	

The table compares the advantages and disadvantages of Distributed Ledger Technology (DLT) networks based on their energy consumption levels—high, medium, and low. High energy consumption networks, often associated with Proof of Work (PoW) mechanisms, provide strong security and decentralization but come with environmental and cost drawbacks. Medium-level energy networks strike a balance between security and efficiency, offering improved scalability but at the cost of complexity and ongoing development. Low energy consumption networks are environmentally friendly and cost-efficient but may risk centralization and are less proven in terms of trust and adoption.

6.2.3. Transaction Capacity

Transaction capacity refers to the number of transactions a particular DLT network can process over a given period. The choices are:

- **High:** Indicates that the DLT network can process a large number of transactions per second (TPS), supporting high throughput and scalability to accommodate large volumes of transactions efficiently.
- **Medium:** Suggests that the DLT network has a moderate transaction processing capability, handling a moderate number of transactions per second. It may balance performance with other factors such as security and decentralisation.
- **Low:** Implies that the DLT network has a limited transaction processing capacity, handling fewer transactions per second. This may be due to design constraints or trade-offs in achieving other network objectives like security or decentralisation.

Transaction Capacity	Advantages	Disadvantages
High	**Scalability**: Supports high-demand applications and large user bases.	**Resource Intensive**: Requires significant computational and network resources, increasing costs.
	User Experience: Faster processing enhances user experience and usability.	**Potential Trade-offs**: May compromise decentralization and security for higher capacity.
	Adoption: Encourages greater adoption for real-time applications like financial services and IoT.	**Complexity**: Requires advanced solutions like sharding, layer 2 protocols, or novel consensus mechanisms.
Medium	**Balanced Performance**: Balances scalability with stability and security.	**Growth Limitations**: May become a bottleneck as network demand increases, requiring future upgrades.

	Moderate Resource Requirements: Lower operational costs, supporting decentralization.	**Performance Fluctuations**: May experience delays or increased fees during peak usage times.
	Versatility: Suitable for a wide range of applications, from small projects to moderate demands.	**Competitiveness**: May struggle to compete with high-capacity networks for high-throughput applications.
Low	**Simplicity**: Easier maintenance, focusing on robustness and security over scalability.	**Scalability Issues**: Severely limits network's ability to scale, unsuitable for high-demand applications.
	Resource Efficiency: Requires fewer computational resources, reducing operational costs.	**User Experience**: Slower processing and potential congestion lead to poor user experiences.
	Security: Prioritizes security and decentralization, reducing vulnerability to attacks.	**Adoption Challenges**: Limited capacity may hinder adoption for high-throughput applications.

This table provides a concise comparison of the advantages and disadvantages associated with using Distributed Ledger Technology (DLT) networks of varying transaction capacities: high, medium, and low. High-capacity networks offer scalability and better user experience but at the cost of higher resource needs and potential complexity. Medium-capacity networks provide a balanced approach with moderate resource requirements but may face growth and competitive challenges. Low-capacity networks prioritize simplicity, security, and resource efficiency but are less suitable for high-demand applications due to scalability and user experience issues.

6.2.4. Security

Security refers to the measures and mechanisms in place to protect a particular DLT or DLT network from attacks, fraud, and unauthorised access, ensuring the integrity and confidentiality of data. The choices are:

- **High:** Indicates that the DLT network employs robust security mechanisms and protocols, such as strong cryptographic techniques, secure consensus algorithms, and rigorous validation processes, making it highly resistant to attacks and vulnerabilities.
- **Medium:** Suggests that the DLT network has a moderate level of security, with effective but potentially less comprehensive security measures compared to high-security networks. It may balance security with other factors like performance and scalability but may have some vulnerabilities.
- **Low:** Implies that the DLT network has weaker security measures, which may include less effective encryption, outdated or less secure consensus algorithms, or inadequate protection against common threats, making it more susceptible to attacks and data breaches.

Security Level	Advantages	Disadvantages
High	Robustness: Highly resistant to attacks.	Resource Intensity: High operational costs due to significant computational resources needed.
	Trust and Reliability: High confidence in network integrity and reliability.	Complexity: Increased complexity in development and maintenance.
	Regulatory Compliance: Better positioned for regulatory standards.	Potential for Slower Innovation: Thorough vetting and testing may slow innovation.
Medium	Balanced Protection: Adequate security with resource efficiency.	Moderate Risk: Vulnerable to sophisticated attacks or emerging threats.
	Scalability: Better performance and scalability compared to high-security networks.	Potential Trade-offs: Security might be traded off for transaction capacity or energy efficiency.
	Flexibility: Faster implementation of new features and improvements.	Trust Concerns: Adequacy of security may be a concern for sensitive applications.
Level	Resource Efficiency: Lower operational costs and increased accessibility.	High Vulnerability: Susceptible to a wide range of attacks.
	Simplicity: Easier to develop, maintain, and upgrade.	Trust Issues: Lower confidence in network reliability and integrity.
	Rapid Innovation: Faster implementation of new features.	Regulatory Challenges: Higher risk of non-compliance with regulatory standards.

The table presents a concise comparison of the advantages and disadvantages associated with Distributed Ledger Technology (DLT) networks across different levels of security: high, medium, and low. High-security networks offer robustness, trust, and regulatory compliance but come with high resource demands and potentially slower innovation. Medium-security networks strike a balance between security and performance but may face moderate risks and trust concerns. Low-security networks provide simplicity, cost efficiency, and rapid innovation but are vulnerable to attacks and regulatory issues.

6.2.5. Cost

Cost refers to the total expenses associated with operating and participating in a specific DLT network, including both nodes' running costs and transaction costs.

- **High:** Indicates that the DLT network incurs substantial expenses. This includes high costs for running nodes (such as hardware, energy, and maintenance) and high transaction fees (which can make transactions expensive for users). High-cost networks may require significant investment for participation and operation.

- **Medium:** Suggests that the DLT network has moderate costs. Node running costs and transaction fees are manageable but not minimal. Participants face reasonable expenses related to both maintaining infrastructure and executing transactions.
- **Low:** Implies that the DLT network has minimal costs. Node running expenses are low due to efficient resource use or scalable infrastructure, and transaction fees are relatively inexpensive, making it cost-effective for users and operators.

Cost Level	Advantages	Disadvantages
High	**Security and Stability**: High security and robust infrastructure.	**Barrier to Entry**: High costs deter new users and smaller participants.
	Incentivised Participation: Higher fees incentivize miners/validators.	**Scalability Issues**: Prohibitive costs as the network scales.
	Quality of Service: Better maintenance, updates, and support.	**Negative Perception**: Users may migrate to lower-cost alternatives.
Medium	**Balanced Affordability**: Accessible while maintaining reasonable security and performance.	**Resource Allocation Trade-offs**: Balancing between cost and factors like security and scalability.
	Sustainable Growth: Supports broader applications and user base without high-cost barriers.	**Variable Costs**: Costs can fluctuate with network usage and demand.
	Incentive Alignment: Moderate fees ensure adequate security and decentralization.	**Competitive Pressure**: Competition from high-cost, high-security and low-cost, high-efficiency networks.
Low	**Accessibility**: More accessible to users and developers, promoting wider adoption.	**Security Concerns**: Lower costs can mean reduced security measures.
	User Attraction: Low fees attract more users and applications.	**Incentive Challenges**: Low fees may fail to incentivize network security adequately.
	Efficiency: Better resource utilization and streamlined processes.	**Sustainability Issues**: Low costs might not sustain long-term maintenance and development.

This table summarizes the advantages and disadvantages of Distributed Ledger Technologies (DLT) networks categorized by high, medium, and low costs. High-cost networks provide robust security and incentivized participation but can deter new users due to prohibitive fees. Medium-cost networks balance affordability and security, making them sustainable for broader applications but may face cost variability and competitive pressures. Low-cost networks enhance accessibility and user growth, but their lower security and sustainability might challenge long-term stability and development. Each cost level presents trade-offs between security, accessibility, and growth potential.

7. Criteria Selection and Preference Ordering under the Grading System

The evaluator is required to assess each criterion, identifying those that are essential, eliminating any that are redundant for the specific use case, and then ranking the remaining criteria. To facilitate this process, two tables are provided. The first table defines the criteria to be included in the evaluation, specifying the essential "must-have" or "must-not-have" elements of these criteria. The second table ranks the remaining optional criteria. Both tables are critical for identifying the most suitable Distributed Ledger Technology (DLT) or DLT network for the evaluator's use case.

The following explains the details of both tables:

Table 2:

- Column A lists all the criteria.
- In Column B, the evaluator must determine which criteria will be included in the evaluation.
- For each included criterion, Column C allows the evaluator to optionally select "must-have" choices for the DLT or DLT network.
- Similarly, in Column D, the evaluator can select "must-not-have" choices for each included criterion.
- If a criterion is not included in the evaluation, or if no "must-have" or "must-not-have" choices are required, the evaluator should select "N/A" in Columns C and D.

Criteria	Included in Evaluation	Must-Have Choice(s)	Must-Not-Have Choice(s)
Programmability	{Yes, No}	{N/A, None, Tokens, Applications}	{N/A, None, Tokens, Applications}
Transaction Format	{Yes, No}	{N/A, Accounts, UTXO}	{N/A, Accounts, UTXO}
Ledger Structure	{Yes, No}	{N/A, Fully Replicated, Sharded, Hybrid}	{N/A, Fully Replicated, Sharded, Hybrid}
Transaction Finality	{Yes, No}	{N/A, Deterministic, Probabilistic, Hybrid}	{N/A, Deterministic, Probabilistic, Hybrid}
DLT network Interoperability	{Yes, No}	{N/A, Inbuilt, External}	{N/A, Inbuilt, External}
Maturity	{Yes, No}	{N/A, High, Medium, Low}	{N/A, High, Medium, Low}
Energy Consumption	{Yes, No}	{N/A, High, Medium, Low}	{N/A, High, Medium, Low}
Transaction Capacity	{Yes, No}	{N/A, High, Medium, Low}	{N/A, High, Medium, Low}
Security	{Yes, No}	{N/A, High, Medium, Low}	{N/A, High, Medium, Low}
Cost	{Yes, No}	{N/A, High, Medium, Low}	{N/A, High, Medium, Low}

Table 2 Essential Criteria Selection

Table 3:

- Column A lists all the criteria.
- In Column B, the evaluator must select "No" if the criterion is included in the evaluation and any choices have been listed in Table 2, Column C (the "must-have" column). The evaluator should select "Yes" if the criterion is included in the evaluation and has remaining choices not listed in Table 2. For all other scenarios, such as when a criterion is not part of the evaluation or all choices are listed in Table 2, the evaluator should select "N/A."
- If "Yes" is selected in Column B, the evaluator must rank the remaining choices in Column C. For example, if only the "none" option was listed in Table 2 for the programmability criterion, the evaluator could rank the remaining choices in Table 3's Column C (e.g., "applications > tokens").
- In Column D, the evaluator prioritises the non-essential criteria, which are those with remaining choices to rank. The evaluator ranks these criteria in reverse order, assigning higher numbers to the most preferred choices. If criteria are considered of equal importance, the same rank can be assigned to multiple rows.

Criteria	Has Remaining Choices to Rank	Ranking the Remaining Choices	Ranking the Non-Essential Criteria
Programmability	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Transaction Format	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Ledger Structure	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Transaction Finality	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
DLT network Interoperability	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Maturity	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Energy Consumption	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Transaction Capacity	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Security	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}
Cost	{N/A, Yes, No}	*Use symbols > or =*	{N/A, integer}

Table 3 Ranking the Criteria and Criteria Choices

With this process, the evaluator selects the evaluation criteria, determines the essential and non-essential elements, ranks all criteria with non-essential choices, and ranks the remaining choices within each criterion.

The next section will explain how the evaluator uses these tables to rank shortlisted DLTs or DLT networks. Following this, we will demonstrate how the ranking system is applied to weight the DLTs and DLT networks to identify the best overall fit. Finally, the key factors considered for each criterion will be discussed in detail.

7.1. User Persona Examples

The following are examples of the essential criteria selection for each of the persona defined in Section 3 (see page 11) as well as criteria and remaining choices ranking.

A. NPO Persona:

Criteria	Included in Evaluation	Must-Have Choice(s)	Must-Not-Have Choice(s)
Programmability	Yes	N/A	None
Transaction Format	No	N/A	N/A
Ledger Structure	No	N/A	N/A
Transaction Finality	No	N/A	N/A
DLT network Interoperability	No	N/A	N/A
Maturity	No	N/A	N/A
Energy Consumption	Yes	Low	Medium, High
Transaction Capacity	No	N/A	N/A
Security	Yes	High	Low
Cost	Yes	Low	Medium, High

Table 4 Essential Criteria Selection for the NGPO persona

For simplicity, the ranking criteria and criteria choices table consist only of the essential and non-essential criteria. The redundant criteria (i.e. those marked with the answer 'No' in Table 4) are omitted.

Criteria	Has Remaining Choices to Rank	Ranking the Remaining Choices	Ranking the Non-Essential Criteria
Energy Consumption	No	N/A	N/A
Cost	No	N/A	N/A
Programmability	Yes	*Applications > Tokens*	2
Security	Yes	*High > Medium*	1

Table 5 Ranking the Criteria and Criteria Choices for the NGPO persona.

B. Bank Consortium Persona:

Criteria	Included in Evaluation	Must-Have Choice(s)	Must-Not-Have Choice(s)
Programmability	Yes	N/A	None
Transaction Format	No	N/A	N/A
Ledger Structure	Yes	N/A	Fully Replicated
Transaction Finality	Yes	Deterministic	Probabilistic
DLT network Interoperability	No	N/A	N/A
Maturity	Yes	High	Low
Energy Consumption	No	N/A	N/A
Transaction Capacity	Yes	High	Low

Security	Yes	High	Medium, Low
Cost	No	N/A	N/A

Table 6 Essential Criteria Selection for the Bank Consortium persona

Criteria	Has Remaining Choices to Rank	Ranking the Remaining Choices	Ranking the Non-Essential Criteria
Security	No	N/A	N/A
Transaction Capacity	Yes	High > Medium	5
Programmability	Yes	*Applications > Tokens*	4
Transaction Finality	Yes	*Deterministic > Hybrid*	3
Ledger Structure	Yes	*Sharded = Hybrid*	2
Maturity	Yes	*High > Medium*	1

Table 7 Ranking the Criteria and Criteria Choices for the Bank Consortium persona

C. DeFi Application Persona:

Criteria	Included in Evaluation	Must-Have Choice(s)	Must-Not-Have Choice(s)
Programmability	Yes	Tokens, Applications	none
Transaction Format	Yes	Accounts	N/A
Ledger Structure	Yes	Fully Replicated	Sharded, Hybrid
Transaction Finality	No	N/A	N/A
DLT network Interoperability	No	N/A	N/A
Maturity	No	N/A	N/A
Energy Consumption	No	N/A	N/A
Transaction Capacity	Yes	High	Low
Security	Yes	High	Low
Cost	No	N/A	N/A

Table 8 Essential Criteria Selection for the DeFi application persona

Criteria	Has Remaining Choices to Rank	Ranking the Remaining Choices	Ranking the Non-Essential Criteria
Programmability	No	N/A	N/A
Ledger Structure	No	N/A	N/A
Transaction Format	Yes	*Accounts > UTXO*	3
Security	Yes	*High > Medium*	2
Transaction Capacity	Yes	*High > Medium*	1

Table 9 Ranking the Criteria and Criteria Choices for the DeFi application persona

8. Grading System Criteria Evaluation

Now that the evaluator has chosen the criteria to select the DLT and/or DLT network for this particular use case, the evaluator can move on to evaluating each DLT and/or DLT network on the shortlist against the chosen criteria.

8.1. Objective Criteria

In this section, each objective criteria are described, including the positives and negatives of each of its options. Additionally, information is given for how the evaluator can come to a conclusion on what particular criteria option each DLT or DLT network satisfies.

8.1.1. Programmability

From Table 2 the criteria options are ‘none’, ‘tokens’ and ‘applications. To determine the level of programmability a particular DLT network implements, the evaluator can follow these steps:

a. Review the Whitepaper/Documentation: The network's whitepaper or technical documentation will typically outline its programmability features, including whether it supports tokens, smart contracts, or decentralised applications;
b. Explore the Network’s Development Tools: Check if the network provides development tools, SDKs, or APIs for creating and managing tokens or smart contracts;
c. Examine Smart Contract Development Environments: Networks with full programmability will often have development environments specifically for developing and deploying smart contracts;
d. Check for Token Standards: Refer to established token standards (e.g., ERC-20, ERC-721 on Ethereum) that indicate the network's support for creating and managing custom tokens;
e. Consult Developer Communities: Engage with developer forums or communities to gather insights on the types of applications being built on the network and the programmability features they utilise; and
f. Inspect the Ecosystem: Analyse the network's ecosystem for existing dApps, DeFi projects, and other programmable solutions that indicate a high level of programmability.

Example DLT categorisation:

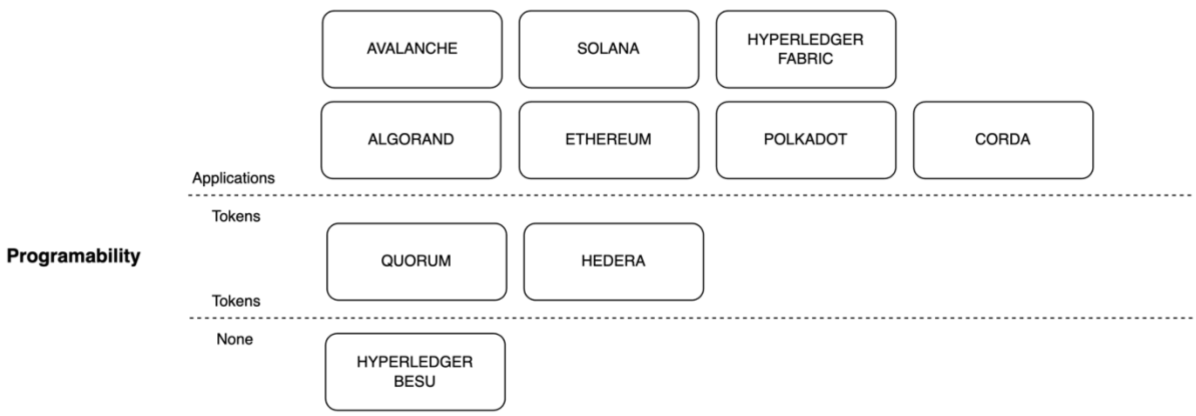

Figure 5 DLT ranking against the Programmability grades

8.1.2. Transaction Format

From Table 2, the criteria options are 'accounts' and 'UTXO'. To determine whether a particular DLT network uses the accounts or UTXO model, the evaluator can follow these steps:

a. Review the Whitepaper/Documentation: Check the network's whitepaper or technical documentation, which typically describes the transaction format and overall architecture;
b. Examine the Source Code: If the DLT is open-source, review the source code on repositories like GitHub. Refer to how transactions are structured and processed;
c. Explore Blockchain Explorers: Use a blockchain explorer to inspect transactions. In the UTXO model, one can see transactions referencing previous transaction outputs. In the accounts model, one can see direct updates to account balances;
d. Query Developer Forums: Participate in developer forums or communities associated with the DLT. Developers and community members can provide insights into the transaction model used; and
e. Network Clients/Wallets: Analyse how network clients or wallets handle transactions. UTXO-based wallets manage unspent outputs, whereas account-based wallets simply display balances.

Example DLT categorisation:

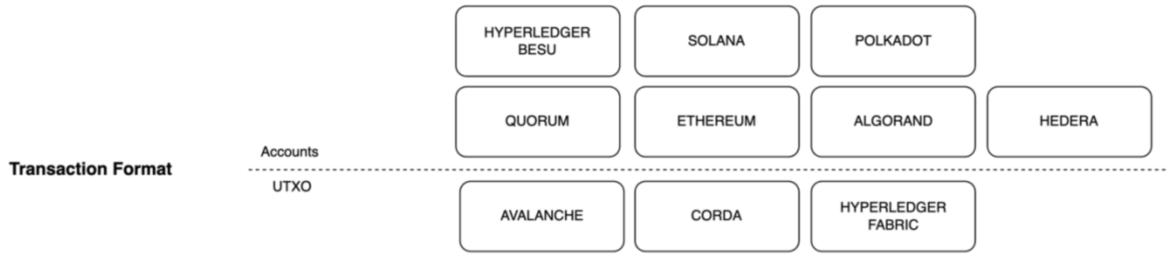

Figure 6 DLT ranking against the Transaction Format grades

8.1.3. Ledger Structure

From Table 2, the criteria options are 'Fully Replicated', 'Sharded' and 'Hybrid'. To determine the ledger structure of a particular DLT network, the evaluator can follow these steps:

a. Review the Whitepaper/Documentation: The network's whitepaper or technical documentation should describe the ledger structure and how data is distributed and managed across the network;
b. Analyse the Consensus Mechanism and Data Distribution: Fully replicated ledgers are typically used in networks with consensus mechanisms that require all nodes to validate all transactions. Sharded ledgers will detail how shards are created, and managed, and how nodes are assigned to shards. Hybrid structures will describe a combination of approaches, often outlining specific components or layers that use different methods;
c. Examine Network Nodes and Data Storage: Investigate how nodes store data. If each node stores a full copy of the ledger, it indicates a fully replicated structure. If nodes store only parts of the ledger and there is a clear division of data responsibilities, the network likely uses sharding. Hybrid structures will show a mix of full and partial data storage strategies;

d. Consult Developer Communities and Forums: Engage with developers and community members who can provide insights into the network's ledger structure and their experiences with data storage and management; and
e. Refer to Specific Protocols or Features: Identify protocols or features that indicate sharding or hybrid approaches, such as cross-shard communication mechanisms or layers that handle different types of data storage.

Example DLT categorisation:

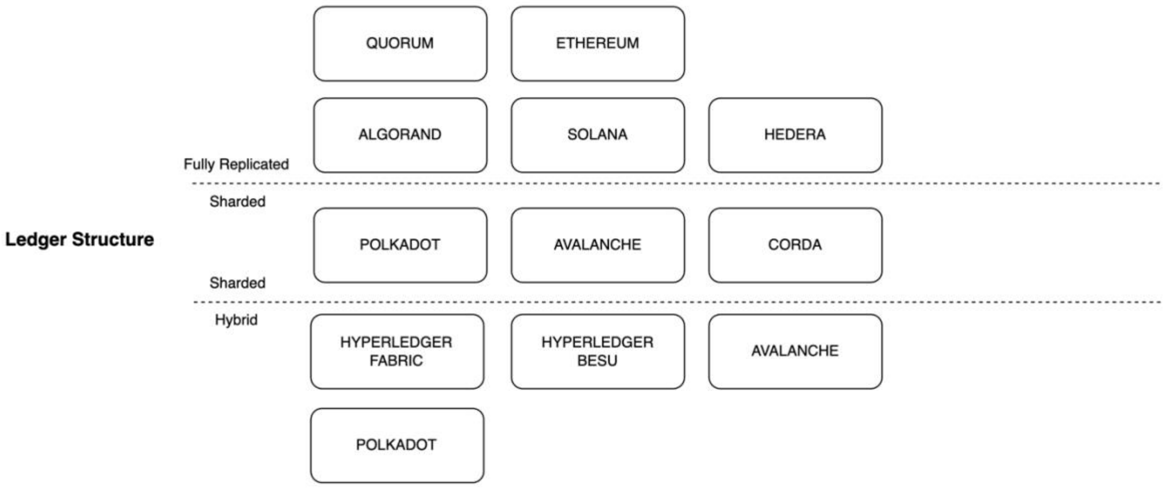

Figure 7 DLT ranking against the Ledger Structure grades

8.1.4. Transaction Finality

From Table 2, the criteria options are 'Deterministic', 'Probabilistic', and 'Hybrid'. To determine the type of transaction finality a particular DLT network implements, the evaluator can follow these steps:

- Review the Whitepaper/Documentation: The network's whitepaper or technical documentation will typically describe the consensus mechanism and how finality is achieved;
- Analyse the Consensus Mechanism: Deterministic finality is often associated with consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT) Click or tap here to enter text. or its variants. Probabilistic finality is usually associated with Proof of Work (PoW) or similar mechanisms where finality is achieved over time with increasing confirmations. Hybrid finality is often associated with modern Proof of Stake (PoS) Click or tap here to enter text. based consensus mechanisms;
- Examine the Network's Block Explorer: Check how transactions are confirmed and how many confirmations are typically required for high confidence. For example, in Bitcoin (probabilistic finality), multiple confirmations are needed for higher certainty. For deterministic finality, look for immediate and irreversible transaction confirmations; and
- Consult Developer Communities: Engage with developer forums or communities to gather insights from developers and users about their experiences with transaction finality on the network.

Example DLT categorisation:

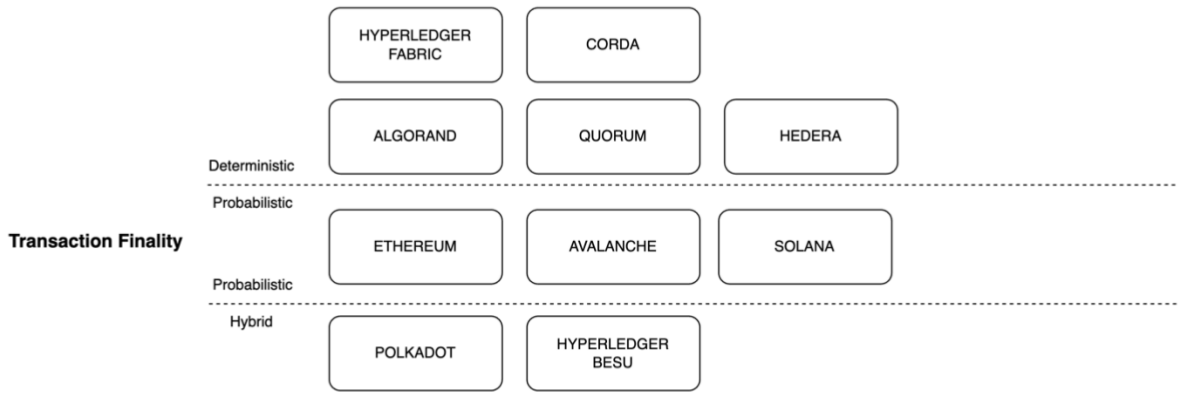

Figure 8 DLT ranking against the Transaction Finality grades

8.1.5. DLT Network Interoperability

From Table 2, the criteria options are 'In-built' and 'External'. To determine the type of interoperability a particular DLT network implements, the evaluator can follow these steps:

a. Review the Whitepaper/Documentation: The network's whitepaper or technical documentation may describe its interoperability features and mechanisms, especially if it is inbuilt. If no mention of interoperability is provided in the whitepaper, there is a good chance that this network will require external interoperability solutions;
b. Explore Interoperability Protocols: Check for specific protocols or frameworks used for interoperability. For example, Cosmos uses the Inter-Blockchain Communication (IBC) protocol Click or tap here to enter text., while Polkadot uses para-chains and relay chains;
c. Analyse Ecosystem Partnerships: Look at the network's partnerships and integrations with other chains. Inbuilt interoperability networks will typically highlight their ecosystem projects, whereas external interoperability may emphasise bridge solutions and collaborations with other networks;
d. Consult Developer Communities: Engage with developer forums or communities to understand how interoperability is achieved and what tools or solutions are commonly used for cross-chain interactions; and
e. Inspect Existing Integrations: Examine existing integrations and use cases. For inbuilt interoperability, you will see native cross-chain applications within the same ecosystem. For external interoperability, you will find various bridges and interoperability solutions connecting to other networks.

Example DLT categorisation:

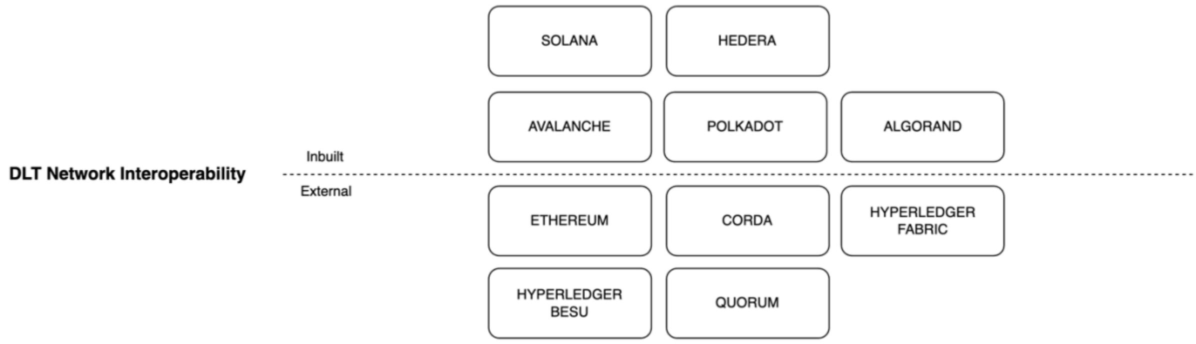

Figure 9 DLT ranking against the Network Interoperability grades

8.2. Subjective Criteria

At this step, an evaluator grades subjective criteria such as Maturity, Energy Consumption, Transaction Capacity, Security, and Cost by assessing how well each DLT solution meets the specific needs and priorities of a given use case. Since these criteria are subjective, their grading depends on the evaluator's perspective, context, and the specific requirements of the organization. For example, a particular DLT solution might be rated as "Low" in Energy Consumption by one evaluator due to its high-power usage relative to the needs of their low-energy application. However, another evaluator with a different use case or tolerance for energy costs might rate the same solution as "Medium" because it fits within their acceptable limits. This variation in grading illustrates the subjective aspect of the evaluation, where different evaluators can arrive at different conclusions based on their unique contexts and priorities.

To assign values such as "High," "Medium," or "Low" to these subjective criteria, evaluators need to rely on a range of sources that provide detailed information about the DLT solutions being considered. These sources can include official documentation, white papers, technical reports, academic research, industry benchmarks, and expert analyses that outline the capabilities, limitations, and performance metrics of different DLTs. By examining such sources, evaluators can gather evidence on aspects like transaction capacity or security features, allowing them to make more informed and nuanced judgments. The grading process, therefore, combines this objective information with the evaluator's subjective interpretation of how well the DLT meets the specific goals and constraints of their scenario. This approach ensures that the evaluation is both evidence-based and aligned with the unique needs of each use case.

For the purpose of this technical report, in all examples an arbitrary grading has been applied to each criterion based on the authors' knowledge and a comprehensive literature review to illustrate the evaluation process.

8.2.1. Maturity

From Table 2, the criteria options are 'high', 'medium' and 'low'. To rate the maturity of a particular DLT or DLT network as high, medium, or low, an evaluator can consider the following indicators:

a. **Development Stage:**
   - High: Mature, well-established core features with infrequent major updates.
   - Medium: Stable core features with ongoing development and improvements.
   - Low: Early-stage development with frequent updates and changes.

b. **Adoption and Usage:**
   - High: Large user base with extensive applications and widespread integrations.

- Medium: Growing user base with a moderate number of applications and integrations.
- Low: Limited user base and few applications or integrations.

c. **Security and Stability:**
   - High: Robust security protocols and high stability with rare issues.
   - Medium: Improved security measures and relative stability with occasional issues.
   - Low: Frequent security issues, bugs, and instability.

d. **Ecosystem and Community:**
   - High: Large, active community with extensive resources and strong support.
   - Medium: Growing community with increasing resources and support.
   - Low: Small, emerging community with limited resources and support.

e. **Governance and Development Processes:**
   - High: Well-defined, formal governance and development processes.
   - Medium: Established governance and development processes with some formalisation.
   - Low: Informal or evolving governance and development processes.

f. **Market Position and Recognition:**
   - High: Strong market presence and widespread recognition as a leading network.
   - Medium: Increasing market presence and recognition within the industry.
   - Low: Limited market presence and recognition.

Example DLT categorisation:

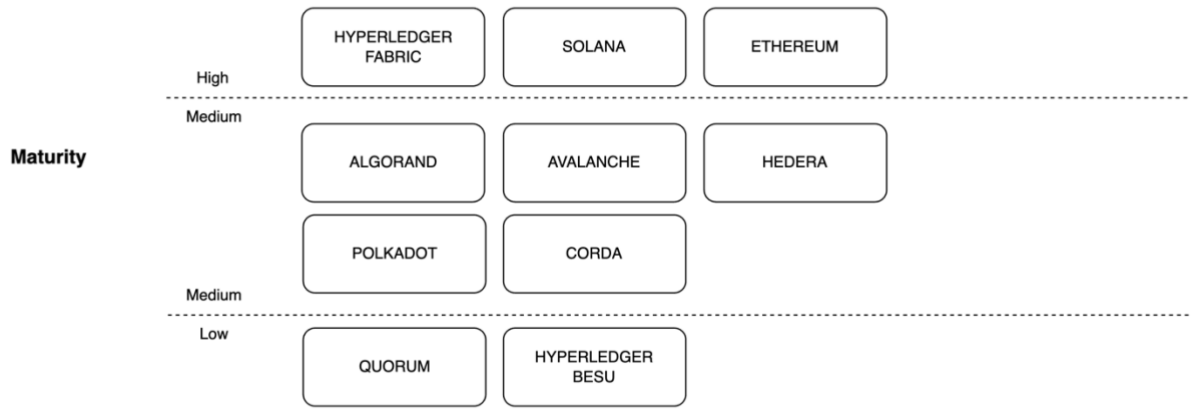

Figure 10 DLT ranking against the Maturity grades

8.2.2. Energy Consumption

From Table 2, the criteria options are 'high', 'medium' and 'low'. To rate the energy consumption of a particular DLT network as high, medium, or low, an evaluator can consider the following indicators:

a. **Consensus Mechanism:**
   - High: Uses Proof of Work (PoW).
   - Medium: Uses hybrid mechanisms like PoW/PoS or PoW with energy-efficient enhancements.
   - Low: Uses Proof of Stake (PoS), Delegated Proof of Stake (DPoS) Click or tap here to enter text., or other low-energy consensus mechanisms.

b. **Energy Metrics:**

- High: Consumes a significant amount of energy per transaction or block, typically measured in kilowatt-hours (kWh).
- Medium: Balances energy consumption with efficiency, consuming moderate energy per transaction or block.
- Low: Consumes minimal energy per transaction or block, significantly lower than PoW networks and still lower than most PoS networks

c. Environmental Impact:
- High: Has a substantial carbon footprint and environmental impact.
- Medium: Reduced environmental impact compared to high consumption networks but still significant.
- Low: Minimal environmental impact, prioritising sustainability.

d. Operational Costs:
- High: High energy costs for miners or validators, potentially impacting network participation.
- Medium: Moderate energy costs, balancing between cost and efficiency.
- Low: Low energy costs, making it accessible to a wider range of participants.

e. Public Perception and Regulatory Impact:
- High: May face negative public perception and regulatory challenges due to high energy consumption.
- Medium: Better public perception and fewer regulatory challenges compared to high consumption networks.
- Low: Positive public perception and minimal regulatory challenges due to low environmental impact.

f. Network Infrastructure:
- High: Requires extensive infrastructure and energy resources to support mining or validation.
- Medium: Moderately intensive infrastructure requirements.
- Low: Minimal infrastructure requirements, focusing on efficiency and sustainability.

Example DLT categorisation:

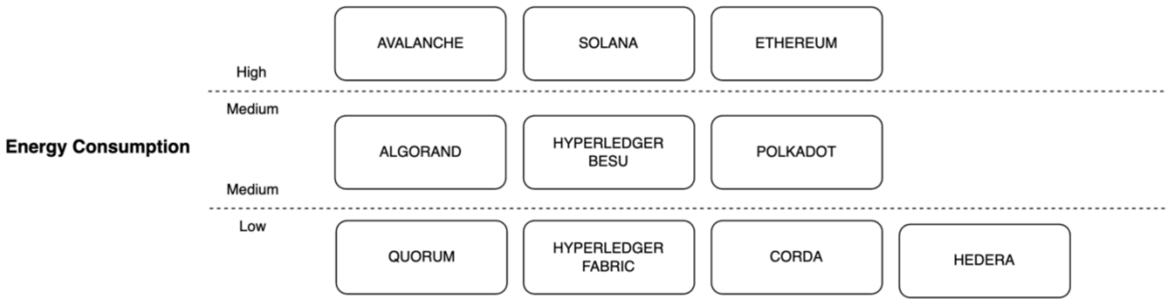

Figure 11 DLT ranking against the Energy Consumption grades

8.2.3. Transaction Capacity

From Table 2, the criteria options are 'high', 'medium' and 'low'. To rate the transaction capacity of a particular DLT network as high, medium, or low, an evaluator can consider the following indicators:

a. Transactions per Second (TPS):
- High: Networks capable of processing thousands or more TPS.
- Medium: Networks processing hundreds to a few thousand TPS.

- Low: Networks processing up to a few hundred TPS.

b. Consensus Mechanism:
- High: Uses consensus mechanisms optimised for high throughput (e.g., PoS with sharding, etc).
- Medium: Uses moderately scalable consensus mechanisms (e.g., standard PoS, hybrid models).
- Low: Uses less scalable mechanisms (e.g., PoW, single-chain committee-based PoS).

c. Network Architecture:
- High: Employs advanced architectures like sharding, sidechains, or layer 2 solutions to enhance capacity.
- Medium: Utilises some optimisations but not to the extent of high-capacity networks.
- Low: Traditional single-chain architecture without scalability enhancements.

d. Latency:
- High: Very low latency, with fast transaction confirmation times.
- Medium: Moderate latency, with acceptable confirmation times for most applications.
- Low: Higher latency, with longer confirmation times impacting user experience.

e. Resource Requirements:
- High: Requires substantial computational and network resources to support high throughput.
- Medium: Moderate resource requirements balancing capacity and efficiency.
- Low: Minimal resource requirements, focusing on efficiency and security.

f. Use Cases and Applications:
- High: Suitable for high-demand applications like high-frequency trading, large-scale payments, and IoT.
- Medium: Adequate for a wide range of applications, including moderate-scale financial services and decentralised apps.
- Low: Best suited for niche applications, small-scale transactions, and highly secure environments.

g. Network Usage Patterns:
- High: Handles high levels of concurrent transactions with minimal performance degradation.
- Medium: Performs well under normal conditions but may experience delays during peak usage.
- Low: Prone to congestion and delays under high transaction volumes.

Example DLT categorisation:

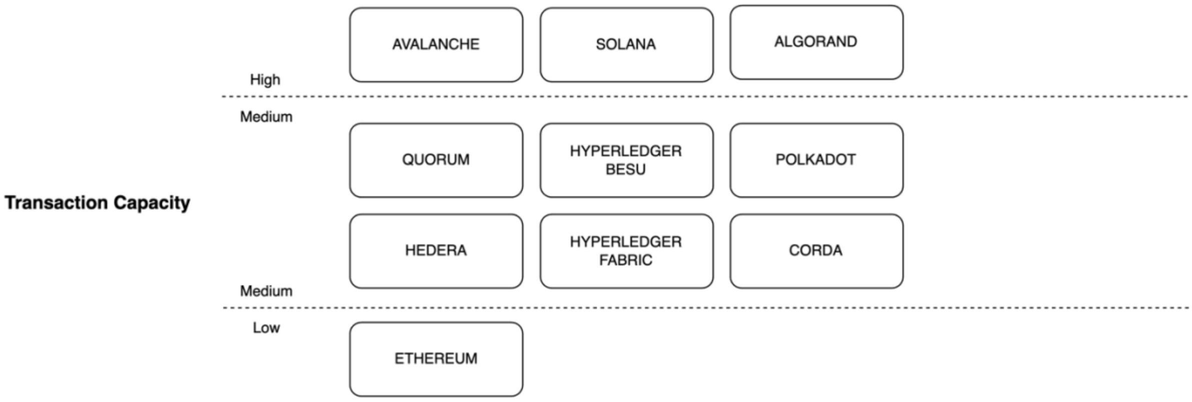

Figure 12 DLT ranking against the Transaction Capacity grades

8.2.4. Security

From Table 2, the criteria options are 'high', 'medium' and 'low'. To rate the security of a particular DLT network as high, medium, or low, an evaluator can consider the following indicators:

a. Consensus Mechanism:
- High: Uses highly secure consensus mechanisms like Proof of Work (PoW) with a large network of miners, or Proof of Stake (PoS) with strong economic incentives and penalties.
- Medium: Uses reasonably secure consensus mechanisms like standard PoS or hybrid models with moderate participation.
- Low: Uses less secure or novel consensus mechanisms with limited network participation and economic incentives.

b. Attack Resistance:
- High: Proven resistance to 51% attacks, Sybil attacks Click or tap here to enter text., double-spending, and other common threats.
- Medium: Moderate resistance to attacks, with some potential vulnerabilities under specific conditions.
- Low: Susceptible to common attacks and lacking robust defence mechanisms.

c. Network Decentralisation:
- High: High degree of decentralisation with many independent validators or miners, reducing the risk of central control.
- Medium: Moderate decentralisation with a reasonable number of independent participants.
- Low: Low decentralisation with a small number of validators or miners, increasing the risk of central control and collusion.

d. Cryptographic Standards:
- High: Utilises state-of-the-art cryptographic standards and regularly updates to mitigate emerging threats.
- Medium: Uses established cryptographic standards with occasional updates.
- Low: Relies on outdated or weaker cryptographic standards with infrequent updates.

e. Security Audits and Reviews:

- High: Regular, comprehensive security audits by reputable third parties, with a strong track record of addressing vulnerabilities.
- Medium: Periodic security audits and reviews with a reasonable response to identified issues.
- Low: Infrequent or no security audits, with a limited response to identified vulnerabilities.

f. Incident Response and Mitigation:

- High: Effective incident response mechanisms and mitigation strategies to address security breaches and vulnerabilities.
- Medium: Adequate incident response mechanisms with some capability to mitigate security breaches.
- Low: Limited or ineffective incident response and mitigation strategies.

g. Community and Developer Support:

- High: Strong community and developer support focused on maintaining and improving security.
- Medium: Moderate community and developer support with reasonable focus on security.
- Low: Limited community and developer support, with minimal focus on security.

Example DLT categorisation:

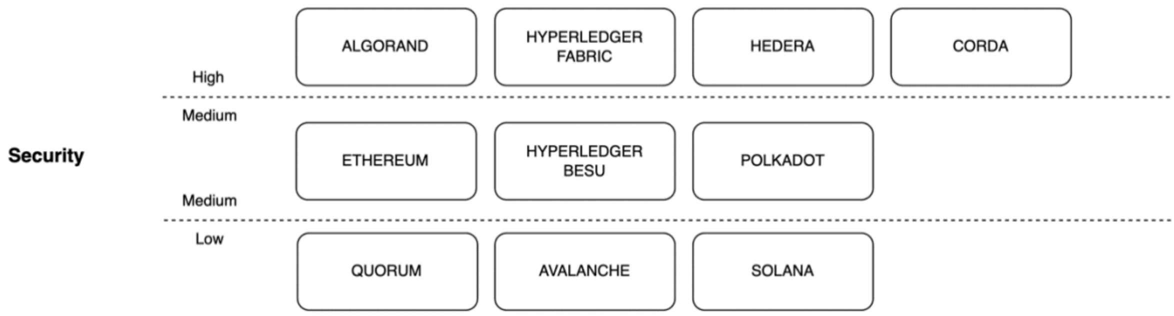

Figure 13 DLT ranking against the Security grades

8.2.5. Cost

From Table 2, the criteria options are 'high', 'medium' and 'low'. To rate the cost of a particular DLT network as high, medium, or low, an evaluator can consider the following indicators:

a. Transaction Fees:

- High: Significantly higher transaction fees compared to the industry average.
- Medium: Moderate transaction fees, balancing affordability and resource allocation.
- Low: Minimal transaction fees, making transactions highly affordable.

b. Infrastructure Costs:

- High: Requires substantial investment in hardware, energy, and maintenance.
- Medium: Requires moderate infrastructure investment, balancing cost and performance.
- Low: Minimal infrastructure investment, focusing on efficiency and cost-effectiveness.

c. Energy Consumption:

- High: High energy consumption, leading to increased operational costs.
- Medium: Moderate energy consumption with balanced operational costs.
- Low: Low energy consumption, reducing overall operational costs.

d. **Network Participation Costs:**
- High: Significant costs for miners or validators to participate and maintain network security.
- Medium: Moderate participation costs, ensuring adequate security without prohibitive expenses.
- Low: Minimal participation costs, promoting broad participation and accessibility.

e. **Scalability Costs:**
- High: Costs may increase significantly with network growth, impacting scalability.
- Medium: Costs scale reasonably with network growth, supporting sustainable scalability.
- Low: Costs remain low and manageable even as the network scales.

f. **User Experience:**
- High: Users may face high fees, potentially impacting adoption and satisfaction.
- Medium: Users experience moderate fees, balancing cost and service quality.
- Low: Users benefit from minimal fees, enhancing adoption and satisfaction.

Example DLT categorisation:

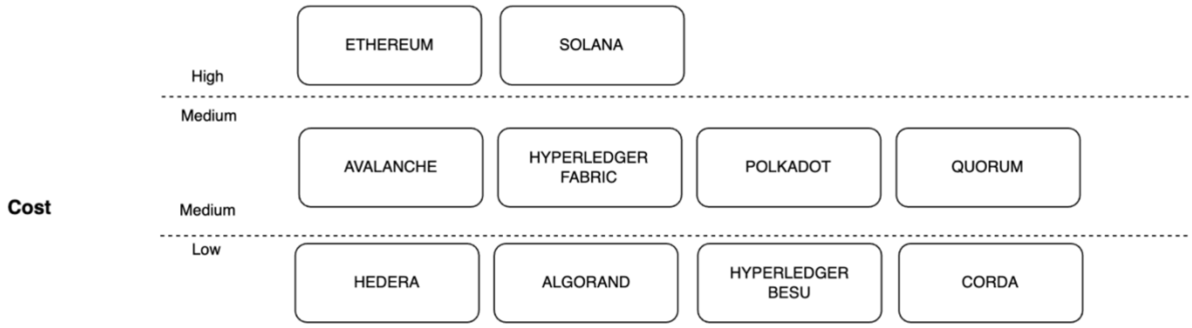

Figure 14 DLT ranking against the Cost grades

9. DLT Selection

Once an evaluator has reached this stage, it is now a fairly simple process to complete, as the evaluator will have chosen and ranked the desired criteria and evaluated what each DLT or DLT network provides.

Therefore, if there is more than one DLT or DLT network option remaining in the shortlist, in order to understand which one is preferred systematically, it is recommended to use a weighting score system, such as the one discussed in the next subsection, and to select the DLT or DLT network with the largest score.

9.1. Weighting Score System

There are various formulae available to interpret the criteria and criteria choice rankings provided by the evaluator. For simplicity, this report will use a specific formula in the examples presented. However, if the evaluator believes an alternative formula is more suitable, the new formula must be agreed upon beforehand to minimise potential biases. It is important to note that the weight formula applies only to criteria that do not have any 'must have' choices selected, as indicated in Table 2, column C.

In Table 3, column C, if three distinct ranks are present, the ranking weights are assigned as follows: 3 for the top-ranked choice, 2 for the middle-ranked choice, and 1 for the lowest-ranked choice. For example, if the rank order for the transaction capacity row is "High > Medium > Low," then a DLT network with high transaction capacity would receive a score of 3, one with medium transaction capacity would score 2, and one with low transaction capacity would score 1. If there are only two distinct ranks, the ranking weight is 3 for the top-ranked choice and 1 for the lowest-ranked choice. For instance, if the rank order for the programmability row is 'applications > tokens,' a DLT with applications programmability would score 3, and a DLT with tokens programmability would score 1. In another example, if the rank order for the maturity row is 'High = Medium > Low,' a DLT with high or medium maturity would score 3, while a DLT with low maturity would score 1.

The full formula for an individual row:

Criteria Score = 'Criteria Column C Rank Score' × 'Criteria Column D Rank Score',

meaning that a full score for a DLT or DLT network being evaluated would be:

Score = Sum of all Criteria Scores

The following section shows the above formula's practical usage.

9.2. User Persona Examples

A: NPO Persona DLT Selection Example

As indicated in the previous step of the DLT Decision Tree process, both the Energy Consumption and the Cost are essential criteria from the perspective of the NPO persona. This effectively filters the set of suitable DLT solutions.

Essential criteria:

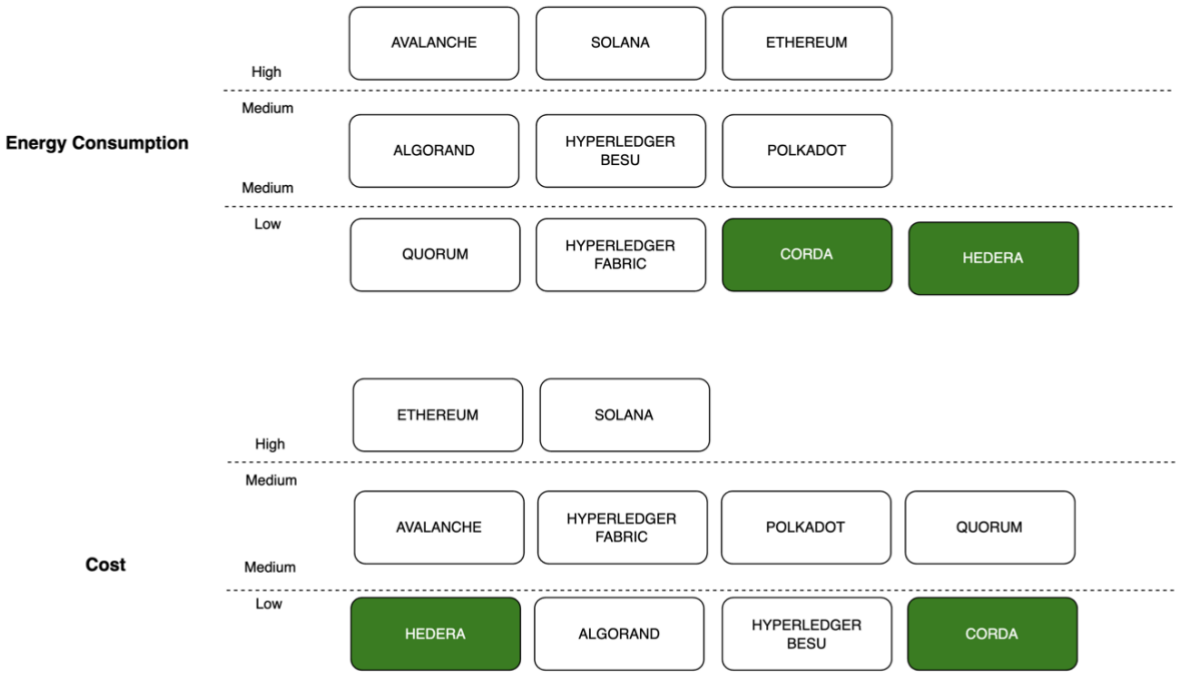

Figure 15 Essential Criteria for the NPO Persona

Non-essential criteria:

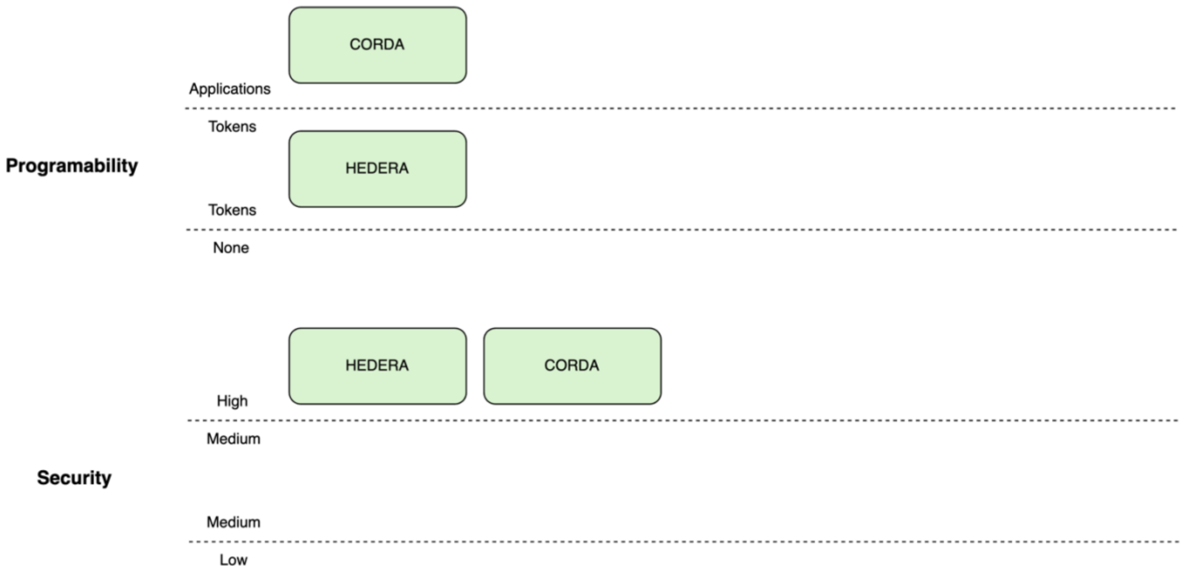

Figure 16 Non-essential Criteria for the NPO Persona

Score calculation for **Corda**:
3 (Programmability - Applications) × **2** (Criteria Rank) + **3** (Security - High) × **1** (Criteria Rank) = **9**

Score calculation for **Hedera**:
2 (Programmability - Tokens) × **2** (Criteria Rank) + **3** (Security - High) × **1** (Criteria Rank) = **7**

Outcome:
Corda receives the higher score and as such is determined to be the most applicable DLT for the NGO use-case scenario.

B: Bank Consortium Persona DLT Selection Example

As indicated in the previous step of the DLT Decision Tree process, the Security is the only essential criteria from the perspective of the Bank Consortium persona. This creates a set of suitable DLT solutions for this scenario.

Essential criteria:

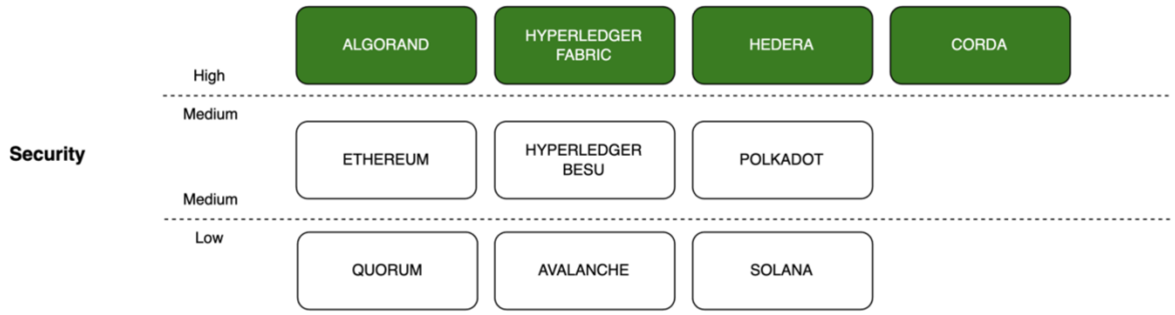

Figure 17 Essential Criteria for the Bank Consortium Persona

From the essential criteria, 4 candidates were shortlisted: Algorand, Hyperledger Fabric, Hedera, Corda.

Non-essential criteria:

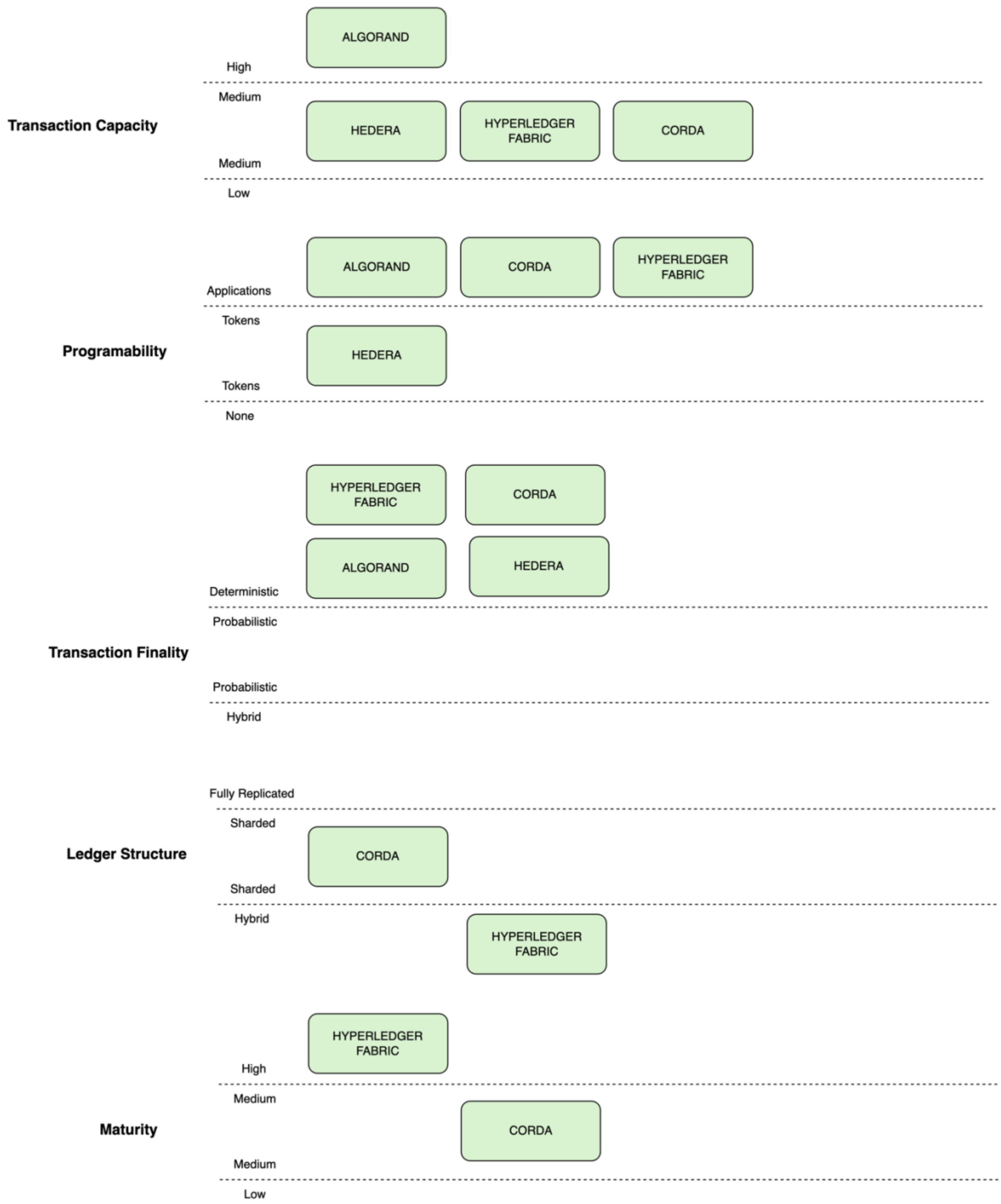

Figure 18 Non-essential Criteria for the Bank Consortium Persona

The shortlist of 4 candidates was further narrowed down to only two that satisfy the allowed values from the set of non-essential criteria. Those candidates are Corda and Hyperledger Fabric. As such, when calculating the score only those two candidates can be considered:

Score calculation for **Corda**:

2 (Transaction Capacity - Medium) × **5** (Criteria Rank) + **3** (Programmability - Applications) × **4** (Criteria Rank) + **3** (Transaction Finality – Deterministic) × **3** (Criteria Rank) + **3** (Ledger Structure - Sharded) × **2** (Criteria Rank) + **2** (Maturity – Medium) × **1** (Criteria Rank) = **39**

Score calculation for **Hyperledger Fabric**:
2 (Transaction Capacity - Medium) × **5** (Criteria Rank) + **3** (Programmability - Applications) × **4** (Criteria Rank) + **3** (Transaction Finality – Deterministic) × **3** (Criteria Rank) + **3** (Ledger Structure - Sharded) × **2** (Criteria Rank) + **3** (Maturity – Medium) × **1** (Criteria Rank) = **40**

Outcome:
Hyperledger Fabric receives the higher score and as such is determined to be the most applicable DLT for the Bank Consortium use-case scenario.

C: DeFi Application Persona DLT Selection Example:

As indicated in the previous step of the DLT Decision Tree process, both the Programmability and the Ledger Structure are essential criteria from the perspective of the DeFi Application persona. This effectively filters the set of suitable DLT solutions.

Essential criteria:

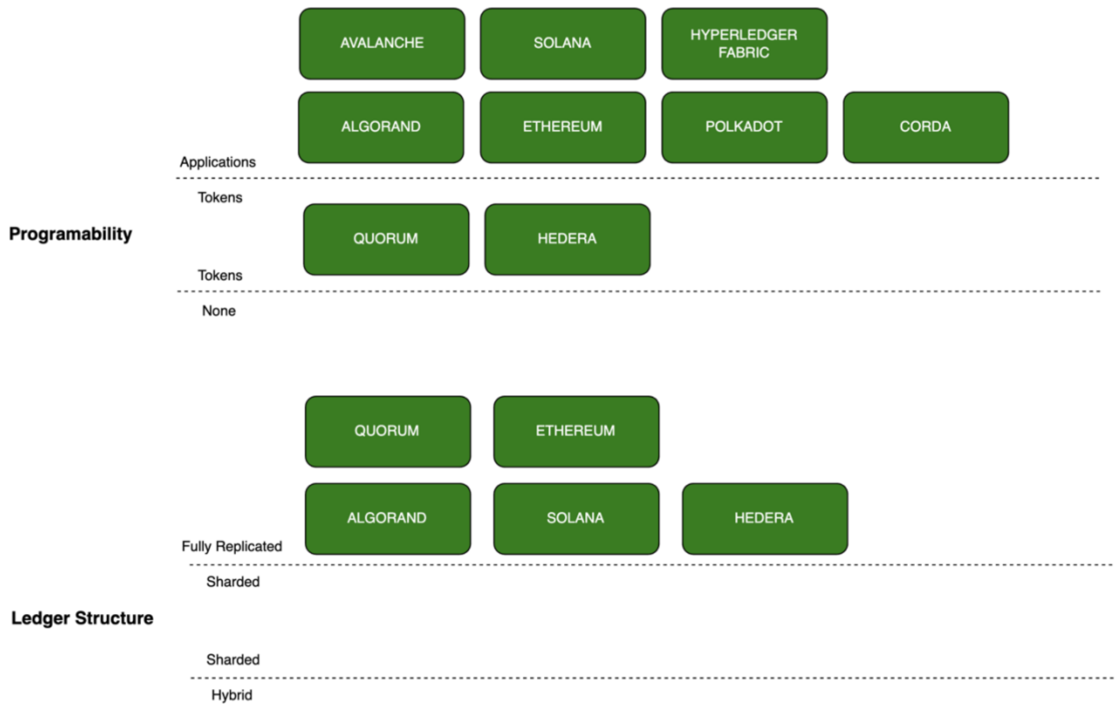

Figure 19 Essential Criteria for the DeFi Application Persona

From the essential criteria 9 candidates were shortlisted: Algorand, Avalanche, Corda, Ethereum, Hedera, Hyperledger Fabric, Quorum, Polkadot, Solana.

Non-essential criteria:

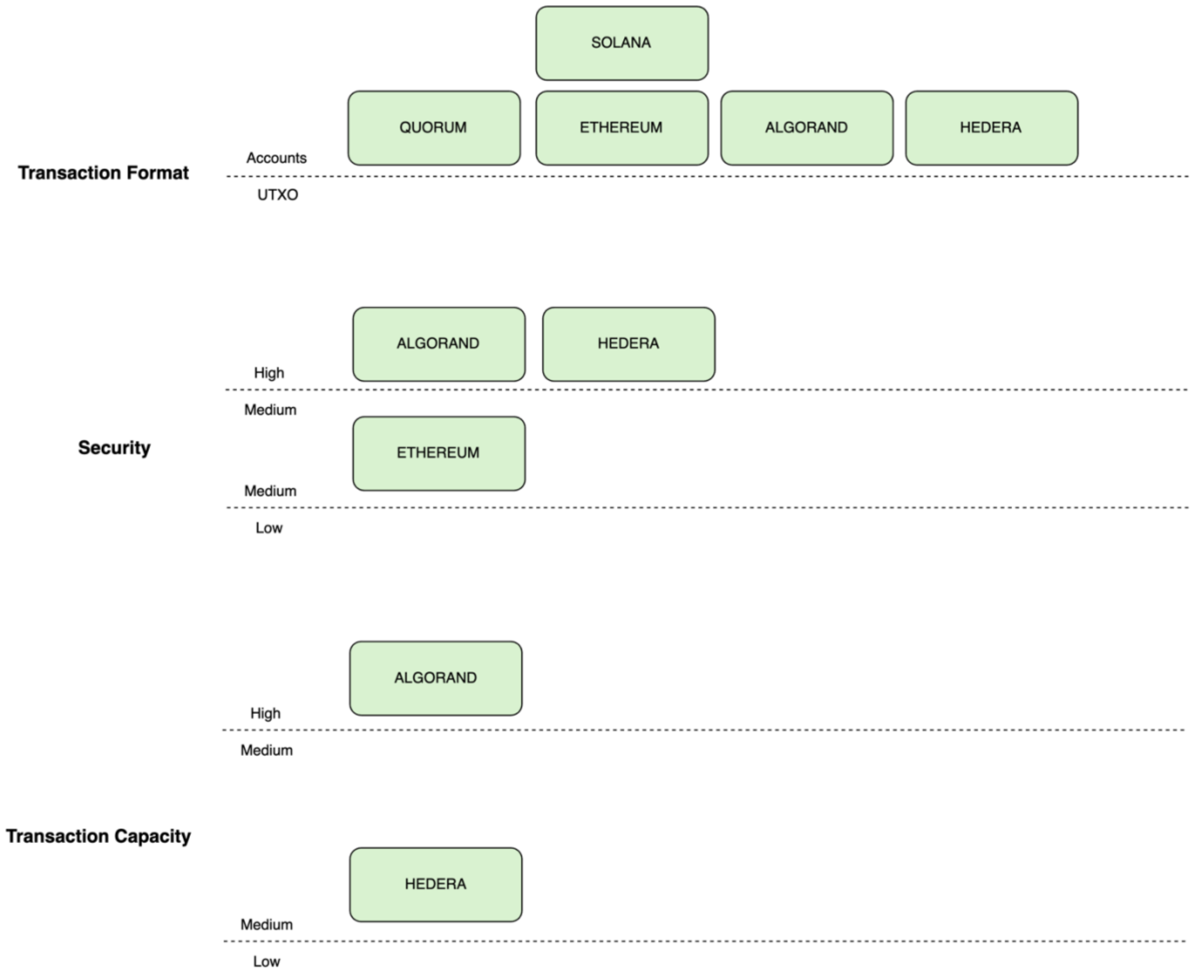

Figure 20 Non-essential Criteria for the DeFi Application Persona

The shortlist of 9 candidates was further narrowed down to only two that satisfy the allowed values from the set of non-essential criteria. Those candidates are Algorand and Hedera. As such, when calculating the score only those two candidates can be considered:

Score calculation for **Algorand**:
3 (Transaction Format - Accounts) × **3** (Criteria Rank) + **3** (Security - Highg) × **2** (Criteria Rank) + **3** (Transaction Capacity – High) × **1** (Criteria Rank) = **18**

Score calculation for **Hedera**:
3 (Transaction Format - Accounts) × **3** (Criteria Rank) + **3** (Security - Highg) × **2** (Criteria Rank) + 2 (Transaction Capacity – High) × **1** (Criteria Rank) = **17**

Outcome:
Algorand receives the higher score and as such is assessed to be the most applicable DLT for the DeFi Application use-case scenario.

10. Conclusions

This technical report has presented a foundational framework for evaluating Distributed Ledger Technologies (DLTs) tailored to specific use cases. By offering a systematic decision tree and grading system, this report provides evaluators with a structured approach to navigate the complexities of DLT selection. The primary goal has been to create a tool that assists organisations in making informed decisions regarding DLT adoption, thereby reducing the risks associated with misuse of this technology and enhancing its operational efficiency.

However, it is important to acknowledge that this report represents an initial step in what must be an ongoing process. The landscape of DLT is dynamic, characterised by rapid advancements and continuous evolution. As such, the framework presented here is not static; it requires regular refinement and updates to remain relevant and effective in addressing the changing needs and challenges faced by organisations.

Moreover, while this report outlines a “happy path” for DLT selection, focusing on the more straightforward scenarios, it does not exhaustively cover the diverse range of possibilities, edge cases, and unique situations that may arise in practice. Many nuanced and complex aspects of DLT selection, which could significantly impact the decision-making process, have been left for future exploration. These aspects will be addressed in subsequent work, which will aim to expand upon the initial ideas presented here, providing more comprehensive guidance for evaluators faced with more challenging or unconventional use cases.

In conclusion, while this technical report lays the groundwork for a robust DLT evaluation process, it is by no means the final word. It should be viewed as a living document, open to continuous improvement and expansion as the technology and its applications evolve. The ongoing development of this framework will be crucial to ensuring its continued relevance and effectiveness in guiding organisations through the ever-changing landscape of distributed ledger technologies.

11. Future Work

While the DLT Decision Tree framework outlined in this report provides a valuable foundation for evaluating Distributed Ledger Technologies, there are several areas where further development and refinement are necessary.

Refinement and Analysis of Edge Scenarios

One critical area for future work involves the refinement of the framework to better handle edge scenarios. For instance, situations where the selection criteria may be contradictory, leading to no clear DLT solution, require more thorough analysis. These edge cases could present significant challenges in real-world applications, where the complexity and specificity of certain use cases might result in conflicting requirements. Future iterations of the framework will need to address these scenarios by introducing mechanisms for resolving contradictions or providing alternative pathways to ensure that evaluators can still arrive at a viable solution.

Proposal for Standardisation: ISO/TC 307/WG 6

The authors have also proposed the DLT Decision Tree framework as a working item for the ISO/TC 307/WG 6 (Use Cases) Click or tap here to enter text.. This initiative aims to contribute to the development of international standards in the field of distributed ledger technologies, particularly in the context of use cases. By aligning the framework with ISO standards, the goal is to create a globally recognised and widely adopted methodology that can be utilised by organisations worldwide. The involvement in ISO/TC 307/WG 6 will also provide valuable feedback and insights, further refining and validating the framework.

Development as a Web Application

Another promising direction for future work is the transformation of the DLT Decision Tree framework into a web-based application. Such an application would automate several steps of the evaluation process, enhancing its usability and accessibility. A web application would allow evaluators to input their specific use case criteria, navigate through the decision tree, and receive tailored recommendations in a more streamlined and efficient manner. Additionally, the application could integrate with databases of DLT solutions, offering real-time updates and the ability to compare different technologies dynamically. This would not only make the evaluation process more efficient but also ensure that it remains up to date with the latest developments in the rapidly evolving DLT landscape.

Ongoing Collaboration and Iteration

Finally, the continued development of the DLT Decision Tree framework will benefit from ongoing collaboration with industry experts, researchers, and practitioners. By fostering a community around this tool, we can ensure that it evolves in response to real-world challenges and remains relevant to the needs of its users. Iterative development, informed by practical application and feedback, will be key to maintaining the utility and accuracy of the framework as the field of distributed ledger technologies continues to mature.

In summary, the DLT Decision Tree framework, while already a robust tool, has significant potential for further development. By addressing edge cases, pursuing standardisation, and developing a web-based application, the framework can be made even more powerful and widely applicable, ensuring it continues to serve as a valuable resource for organisations navigating the complexities of DLT adoption.

12. Acknowledgements

The development of the DLT Decision Tree has been made possible through the collaborative efforts and support of various individuals and organisations.

Gratitude is expressed to the colleagues at the Blockchain and Climate Institute (BCI) for their invaluable guidance and expertise. Special appreciation is extended to Alastair Marke, Director General at BCI; Luke Riley, Head of Standards Development at BCI; Chris Poulloura, Chief Technology Officer at BCI; Thusitha Bandara, Deputy Chief Technology Officer at BCI; and Polly Martin, Senior Research Officer at BCI. Their collective contributions in leadership, technical insights, framework refinement, and research support were crucial to the success of this work.

Thanks, are also extended to BlockStand for their support, not only through financial backing but also for the constructive feedback provided during meetings. The opportunity and platform created by BlockStand for the delivery of this standards contribution were essential to the successful development and dissemination of this work.

The collaboration and dedication of these individuals and institutions were fundamental in making the DLT Decision Tree a reality, and continued partnership in advancing the field of Distributed Ledger Technologies is anticipated with great interest.

13. Bibliography

Agahari, W., Ofe, H., & de Reuver, M. (2022). It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. *Electronic Markets*, *32*(3). https://doi.org/10.1007/s12525-022-00572-w

Alahmad, M., Alshaikhli, I., Alkandari, A., Alshehab, A., Islam, M. R., & Alnasheet, M. (2022). INFLUENCE OF HEDERA HASHGRAPH OVER BLOCKCHAIN. *Journal of Engineering Science and Technology*, *17*(5).

Al-Mashari, M., Al-Mudimigh, A., & Zairi, M. (2003). Enterprise resource planning: A taxonomy of critical factors. *European Journal of Operational Research*, *146*(2), 352–364. https://doi.org/10.1016/S0377-2217(02)00554-4

Avalanche. (n.d.). Retrieved August 20, 2024, from https://www.avax.network/

Carlson, C. R. (1985). Decision Support Systems and Management. In *Languages for Automation*. https://doi.org/10.1007/978-1-4757-1388-6_25

Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. *Proceedings of the Symposium on Operating System Design and Implementation*, *February*. https://doi.org/10.1145/571637.571640

Chen, J., & Micali, S. (2019). Algorand: A secure and efficient distributed ledger. *Theoretical Computer Science*, *777*. https://doi.org/10.1016/j.tcs.2019.02.001

Delegated Proof of Stake. (n.d.). Retrieved August 20, 2024, from https://bitcoinwiki.org/wiki/dpos

Ethereum Foundation. (2018). *Ethereum Blockchain App Platform*. Www.Ethereum.Org.

Hearn, M. (2016). Corda: A distributed ledger (Whitepaper). *Whitepaper*.

Hyperledger Besu. (n.d.). Retrieved August 20, 2024, from https://www.hyperledger.org/projects/besu

Hyperledger Fabric. (n.d.). Retrieved August 20, 2024, from https://www.hyperledger.org/projects/fabric

Inter Blockchain Communication Protocol. (n.d.). Retrieved August 20, 2024, from https://www.ibcprotocol.dev

ISO/TC 307. (n.d.). Retrieved August 20, 2024, from https://www.iso.org/committee/6266604.html

Jimenez, A., & Mateos, A. (2011). GMAA: A DSS Based on the Decision Analysis Methodology - Application Survey and Further Developments. In *Efficient Decision Support Systems - Practice and Challenges From Current to Future*. https://doi.org/10.5772/16546

Kahneman, D., & Tversky, A. (2019). Prospect theory: An analysis of decision under risk. In *Choices, Values, and Frames*. https://doi.org/10.1017/CBO9780511803475.003

Keeney, R. L., & Raiffa, H. (1979). Decisions with Multiple Objectives: Preferences and Value Trade-Offs. In *IEEE Transactions on Systems, Man and Cybernetics* (Vol. 9, Issue 7). https://doi.org/10.1109/TSMC.1979.4310245

Liu, S. T., & Clemen, R. T. (1992). Making Hard Decisions, an Introduction to Decision Analysis. *Technometrics*, *34*(3). https://doi.org/10.2307/1270059

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access*, *7*. https://doi.org/10.1109/ACCESS.2019.2925010

Panagiotakos, G. (2023). Proof of Work. In *Encyclopedia of Cryptography, Security and Privacy*. https://doi.org/10.1007/978-3-642-27739-9_1663-1
Parity Technology. (2019). Polkadot Consensus ·Polkadot Wiki. In *Parity.io*.
Patel, V. L., Kaufman, D. R., & Arocha, J. F. (2002). Emerging paradigms of cognition in medical decision-making. *Journal of Biomedical Informatics*, *35*(1). https://doi.org/10.1016/S1532-0464(02)00009-6
Pierro, G. A., & Tonelli, R. (2022). Can Solana be the Solution to the Blockchain Scalability Problem? *Proceedings - 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering, SANER 2022*. https://doi.org/10.1109/SANER53432.2022.00144
Quorum. (n.d.). Retrieved August 20, 2024, from https://github.com/Consensys/quorum
Saaty, R. W. (1987). The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling*, *9*(3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8
Sybil Attack. (n.d.). Retrieved August 20, 2024, from https://en.wikipedia.org/wiki/Sybil_attack