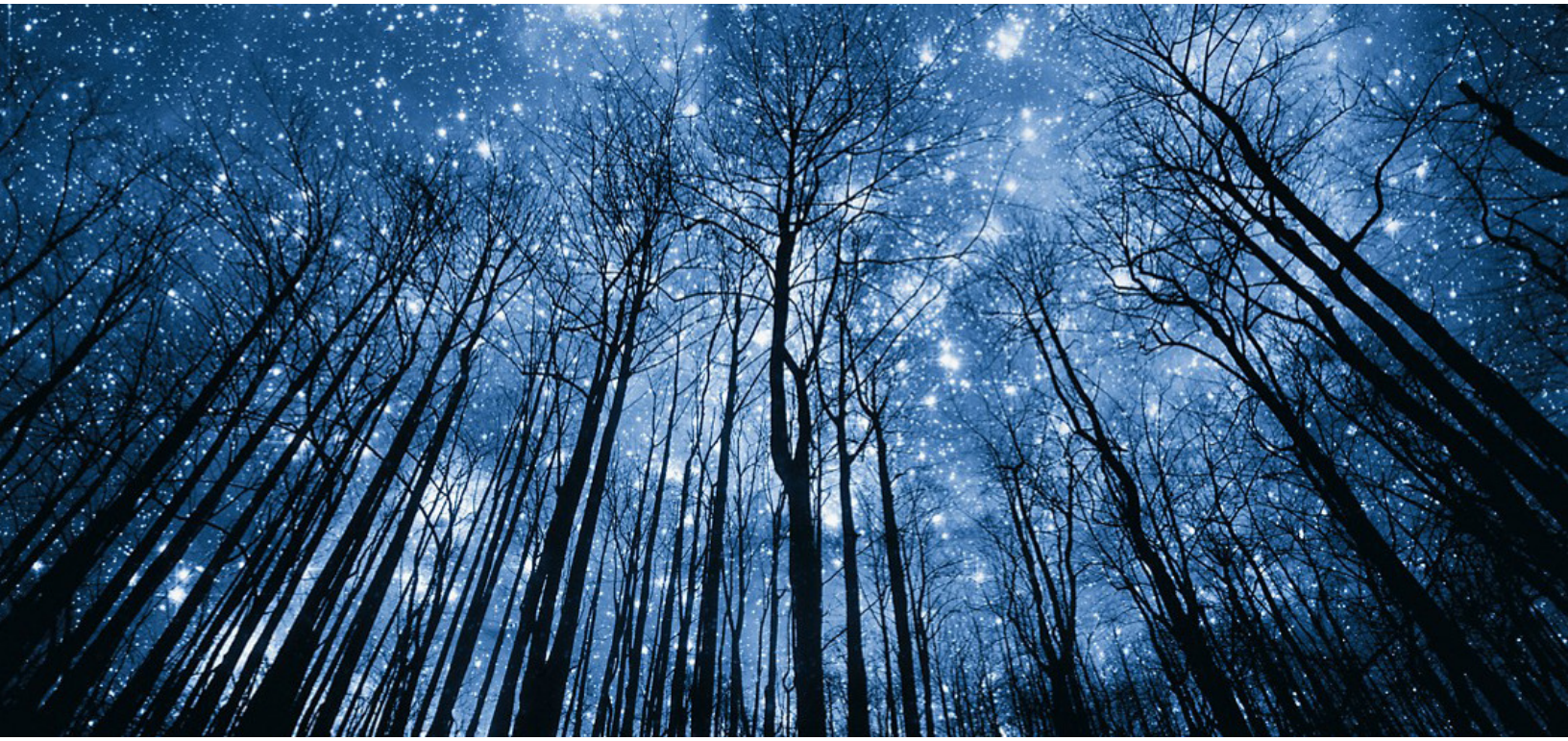
DELL Technologies

BUMPY LANDING: DISTRIBUTED LEDGERS IN A CENTRALIZED WORLD



Steve Todd
Fellow, P&O CTO
Dell Technologies

Frank Macha
Sr. Principal Engineering Technologist
Dell Technologies

DELL Technologies
Proven Professional

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across Dell's multiple technologies and products with both skill and outcome-based certifications.

Proven Professional exams cover concepts and principles which enable professionals working in or looking to begin a career in IT. With training and certifications aligned to the rapidly changing IT landscape, learners can take full advantage of the essential skills and knowledge required to drive better business performance and foster more productive teams.

Proven Professional certifications include skills and solutions such as:

- Data Protection
- Converged and Hyperconverged Infrastructure
- Cloud and Elastic Cloud
- Networking
- Security
- Servers
- Storage
- …and so much more.

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Table of Contents

Table of Contents 3
Introduction 4
Increasing DLT Business Value 7
Corporate Obstacles to DLT Feasibility 10
Review of DLT Governance Requirements 11
Virtualization / Standard Deployment 12
Single Versus Multi-Tenant 13
Data Classification and Mapping 14
Network Connectivity / Application Placement 14
Application Deployment and Operation 16
Security and Compliance 17
Use Case: Hedera Governance Council 17
Day 0 Operations 21
Day 1 Operations 22
Day 2 Operations 23
A Vision for Moving Forward 25
Conclusion 30
Bibliography 32

Introduction

In June 2018, Dell Technologies published a paper[i] highlighting the benefits, obstacles, and solutions related to implementing distributed ledger technology (DLT) in an enterprise environment.

The paper identified four use cases driving interest in enterprise DLTs:

1. Management/transfer of data assets
2. Broadcast of data
3. Credential verification
4. Supply chain transparency

The paper also identified a long list of implementation concerns:

- Performance
- Time-to-finality
- Data consistency
- Multi-chain or multi-ledger
- Secure and portable smart contracts
- Smart contract instrumentation and auditability
- Search capabilities

Finally, the paper posited that the diversity of the Dell Technologies product portfolio could solve the implementation concerns and bring business benefits to the four use cases. Figure 1 highlights DLT-relevant areas addressed by Dell Technologies' diverse product portfolio circa 2018.

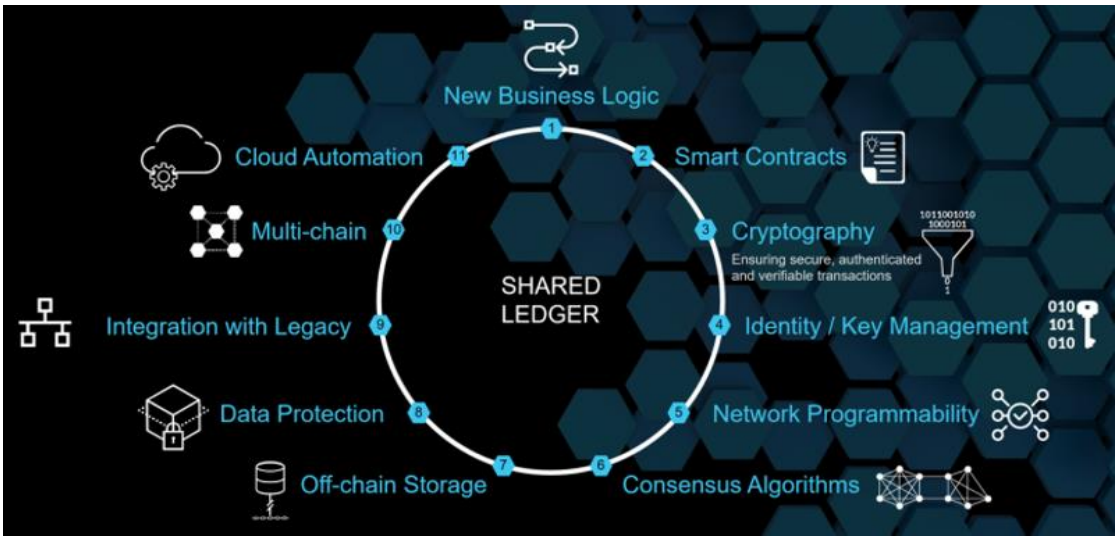
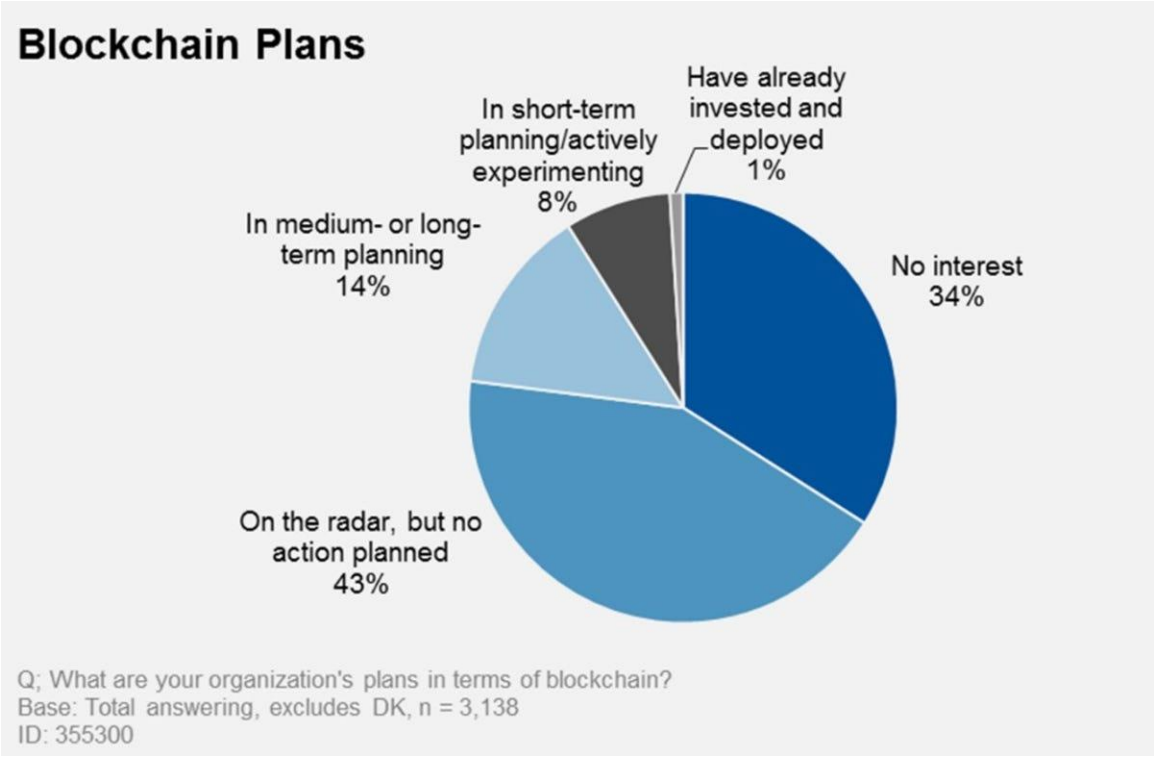


Figure 1 - 2018 Technology Portfolio for Distributed Ledger Technology

Despite the optimism, little progress occurred after the release of the paper. As a result, enterprise adoption of distributed ledger technology lagged.

Several news sources reported on the slow enterprise adoption of DLTs.

For example, a ZDNET report[ii] discussing a Gartner blockchain survey in 2018 stated that "the majority of enterprise players have no intention to develop or use distributed ledger technologies." Figure 2 depicts the Gartner survey of enterprise blockchain from five years ago.



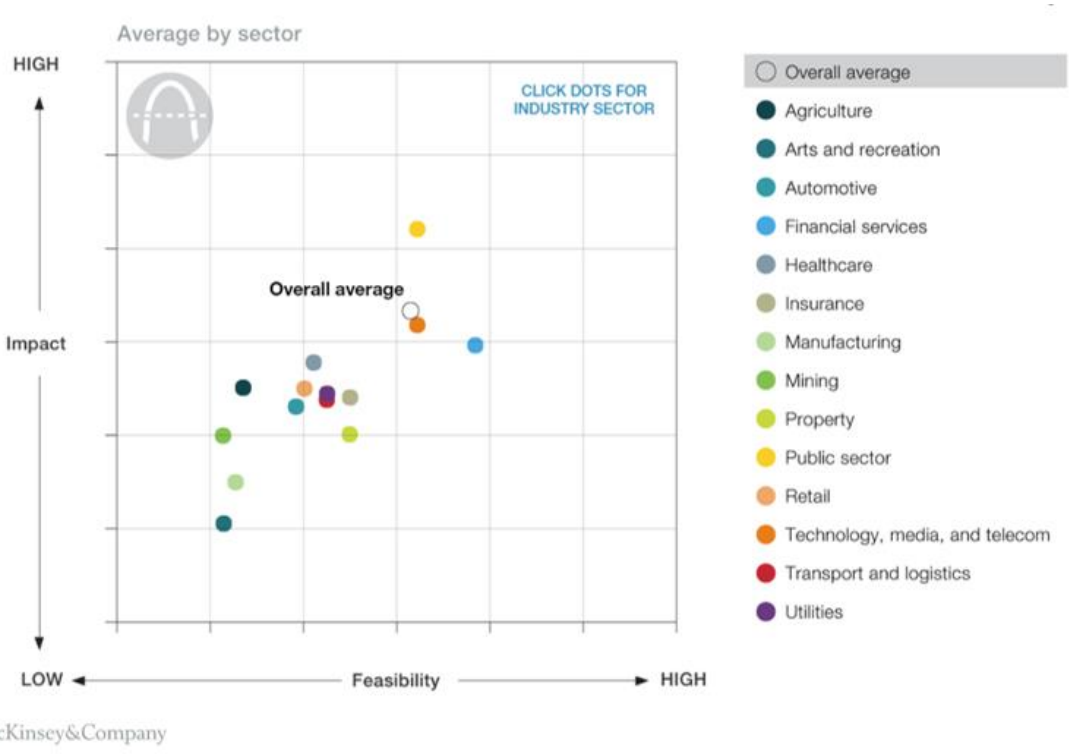
Gartner[iii]

Figure 2 - 2018 Gartner Blockchain Survey of CIOs

The ZDNET article stated that the term "blockchain" is also known as "distributed ledger technology" (many use the terms interchangeably) and that, "Gartner's 2018 CIO Survey suggests that 77 percent of CIOs believe their companies have no interest in the technology at all, and no plans to develop any uses for distributed ledgers."

At roughly the same time (2018), McKinsey Digital also published an article[iv] stating that: "Blockchain is still three to five years from feasibility in scale."

McKinsey bolstered this statement by researching "expected business value" across 90 discrete blockchain use cases. For each use case, the company estimated the difficulty (e.g., feasibility) of implementing a DLT in support of each use case. Figure 3 shows the average "value versus feasibility" results across all sectors.



McKinsey[v]

Figure 3 - 2018 McKinsey Blockchain Opportunities by Industrial Sector

Figure 3 hints at two reasons that caused the lagging of enterprise DLT implementations from 2018-2020.

1. Most of the sectors highlighted in the graph trended towards "low impact" (meaning that the business value is not high enough).
2. Overall feasibility (ease of implementation) across all sectors was also low.

Low business value and high implementation difficulty caused many companies to pass on blockchain/DLT during this time. One of the primary reasons that feasibility was low, according to the authors of the McKinsey article, was "the coopetition paradox." This contributes to coordination complexity:

"Blockchain's major advantage is the network effect, but while the potential benefits increase with the size of the network, so does the coordination complexity. For example, a blockchain solution for digital media, licenses, and royalty payments would require a massive amount of coordination across the various producers and consumers of digital content. Natural competitors need to cooperate, and it is resolving this coopetition paradox that is proving the hardest element to solve in the path to adoption at scale. The issue is not identifying the network – or even getting initial buy-in – but agreeing on the governance decisions around how the system, data, and investment will be led and managed. Overcoming this issue often requires a sponsor, such as a regulator or industry body, to take the lead."

In other words, running an IT department is hard enough, but coordinating the people, processes, and technologies across IT departments at multiple companies has proved to be too high of a bar.

Given this situation in 2018, has the landscape changed five years later, in 2023? Has the business impact of DLT use cases increased during that time?

The answer is “yes.” As highlighted below, one tipping point is edge computing.

But what about increased feasibility? Has anyone solved the coopetition paradox? The answer to this question is also “yes.” As discussed below, DLT governance across companies has made significant headway.

This paper asserts that while the answer to both questions is “yes,” corporations are still in for a bumpy ride as they attempt to bridge the gap from siloed, centralized IT processes to the decentralized requirements of DLTs.

While the paper does briefly discuss the applications that run on a DLT, the primary focus is the implementation of the DLT itself.

Section 2 of this paper describes the increasing business potential of DLT technology; great business value awaits those corporations that can successfully implement enterprise DLTs.

Section 3 outlines why the ride will still be bumpy, enumerating a list of issues that have traditionally limited the feasibility of implementing DLTs across corporations.

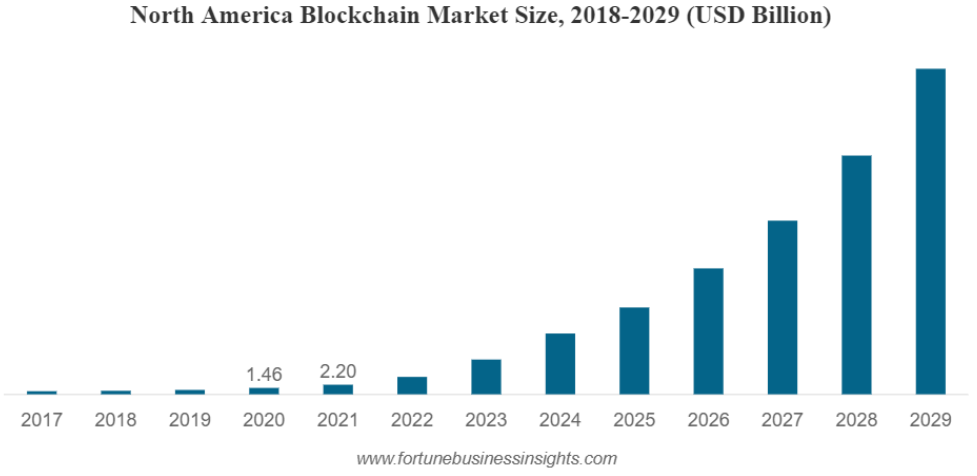
Section 4 describes an organization dedicated to increasing the feasibility of enterprise DLT deployments: the Hedera Governing Council.

Section 5 paints a go-forward vision for capturing long-term business value on the edge by building a DLT bridge across an edge ecosystem.

And finally, Section 6 concludes by stating that while DLT deployment is becoming easier, it won’t be easy. There is still much work to do.

Increasing DLT Business Value

A recent Fortune Business Insights article[vi] validates the stagnant DLT market (in North America) in the 2018 timeframe but predicts significant business growth during the current decade.



Fortune Business Insights[vii]

Figure 4 – DLT/Blockchain Market Projected to Rise to $163.83 B in 2029

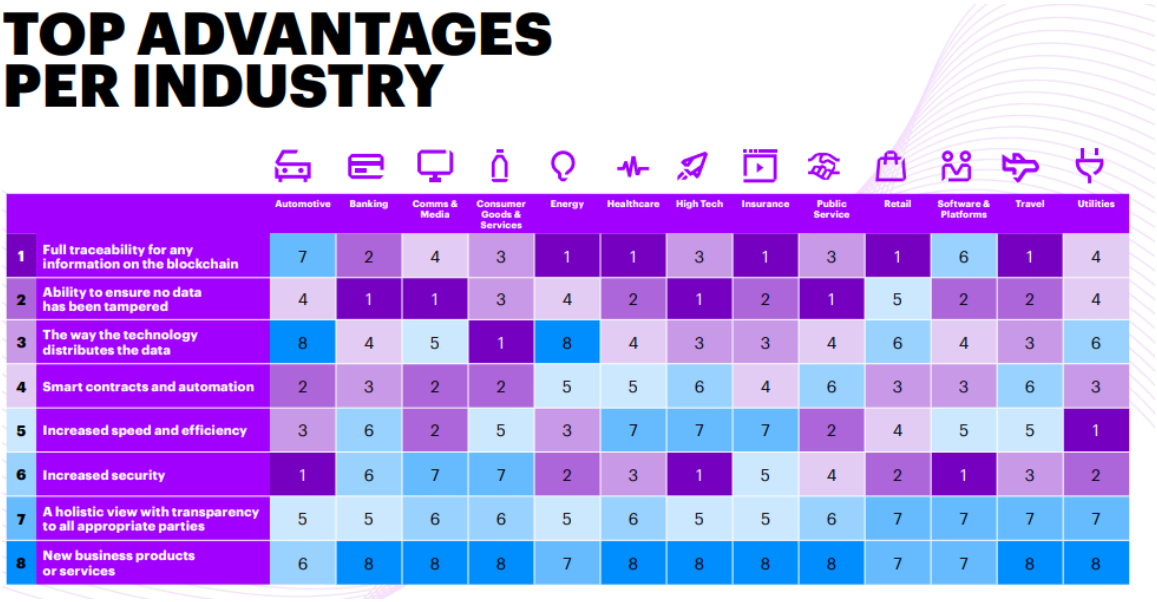
What is the reasoning behind the expanded market share prediction (56.3% CAGR during the forecast period) for DLT? The same Fortune Business Insights article goes on to explain[viii]: "The rising adoption of cloud and Internet of Things [IoT] devices has raised security and privacy concerns across all verticals. The technology offers identity protection, transparency in supply chain operations, and protects health records. Thus, the increasing adoption of digital technologies is expected to expand the market share."

In other words, as data moves from IoT devices on the far edge to centralized environments, there is a significant concern about security and privacy "across all verticals." This concern is largely due to the heterogeneity of vendors, networks, geographies, and policies touching the data as it moves.

A DLT report by Accenture[ix] echoes these concerns by summarizing the top three reasons that different verticals are looking to DLT:

1. Full traceability of any information
2. Ensuring no entity tampered with the data
3. DLT technology focuses on distributed data

Figure 5 highlights an Accenture survey from the same article. The diagram depicts 13 different industries considering DLT and summarizes the primary advantages of doing so. Traceability, tamper-resistance, and decentralization top the list.



		Automotive	Banking	Comms & Media	Consumer Goods & Services	Energy	Healthcare	High Tech	Insurance	Public Service	Retail	Software & Platforms	Travel	Utilities
1	Full traceability for any information on the blockchain	7	2	4	3	1	1	3	1	3	1	6	1	4
2	Ability to ensure no data has been tampered	4	1	1	3	4	2	1	2	1	5	2	2	4
3	The way the technology distributes the data	8	4	5	1	8	4	3	3	4	6	4	3	6
4	Smart contracts and automation	2	3	2	2	5	5	6	4	6	3	3	6	3
5	Increased speed and efficiency	3	6	2	5	3	7	7	7	2	4	5	5	1
6	Increased security	1	6	7	7	2	3	1	5	4	2	1	3	2
7	A holistic view with transparency to all appropriate parties	5	5	6	6	5	6	5	5	6	7	7	7	7
8	New business products or services	6	8	8	8	7	8	8	8	8	7	7	8	8

Accenture[x]

Figure 5 - Transparency, Tamper-proof, and Distributed Advantages of DLT

The travel industry is one example of an industry that places distributed traceability and tamper-proof resistance as top priorities. The second-to-last column lists traceability, tamper-proof, and distributed data as the first, second, and third priorities.

The travel industry is globally distributed (for example, passengers, luggage, planes, etc.), must have traceability (such as the origin and movement of passengers, luggage, and planes), and that data cannot be tampered with (in other words, the identity of passengers).

In addition, multiple parties (travel agents, hotels, airlines, transportation companies, etc.) are globally collaborating to provide distributed travel services.

Therefore, the travel industry must continually create and deploy applications that extend outside the bounds of the enterprise and interact with external data in edge/IoT ecosystems. Systems like this are often called "the distributed enterprise."

In 2022, Gartner made the following prediction[xi] about distributed enterprises. Gartner® predicts that "By 2025, more than 50% of enterprise-managed data will be created and processed outside the data center or cloud."

What are the ramifications of that prediction? According to Gartner,

"The modern data architecture will include the edge, and enterprises need to make plans to capture the opportunities and prepare for the challenges of managing data in edge environments."

Enterprise IT departments have assembled a long list of *centralized* technologies (enterprise storage systems, Active Directory servers, etc.) that allow *data center and cloud* applications to process data in a trustworthy way.

How can these organizations guarantee the same level of transparency and tamper-resistance of data in a distributed, decentralized edge environment?

The answer *does not* involve deploying centralized technologies onto the edge. But it must include integrating legacy technologies with edge computing solutions.

DLTs can provide this integration.

Indeed, in 2018, Dell Technologies anticipated the need for transparency and tamper resistance on the edge by announcing[xii] the creation of a new technology known as a Data Confidence Fabric (DCF). The company also published a paper in 2020[xiii] describing the complex challenges of transparently delivering tamper-resistant data across a distributed "sensor-to-cloud" edge ecosystem. Figure 6 depicts this complexity.

Figure 6 - The Challenge of Trusted Data Delivery on the Edge

Dell's DCF solution proposes that a DLT can provide trustworthy tracking of IoT data from birth to application delivery. As a DLT tracks data's edge journey, it also enables calculating a confidence score. This confidence score provides insight into the trustworthiness of the IT infrastructure that delivered the data.
Figure 7 provides a high-level overview of how a distributed ledger helps annotate and score the trustworthy IT journey of edge data from sensor to gateway to edge server to cloud.

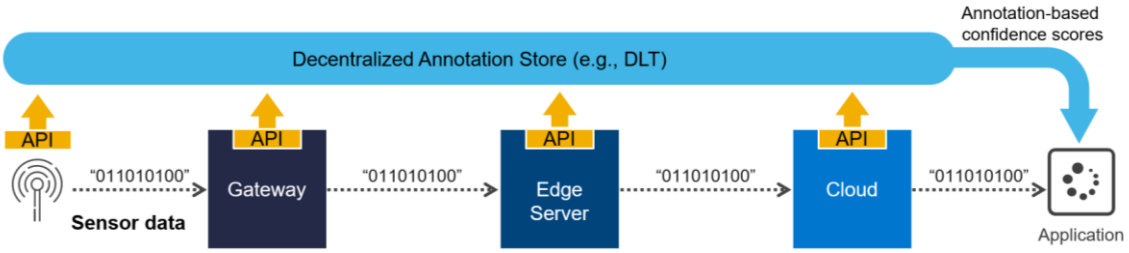


Figure 7 - Annotation of Trustworthy Edge Data Handling via DLT

In 2022 the potential business value enabled by DLT had increased.

What about the feasibility of enterprise DLT implementations? Has it risen?

Before answering that question, Section 3 will explore the baseline problems that IT departments experience when attempting to collaborate on DLT implementations across company lines.

Corporate Obstacles to DLT Feasibility

This paper has identified two reasons enterprise-grade DLTs did not achieve widespread adoption (despite technology readiness).

1. The business value of DLT use cases was too low.
2. The feasibility of DLT implementation was also too low.

In other words, the difficulty of implementing an enterprise DLT has been too costly, and the correspondingly low business value failed to provide a sufficient return on investment.

Section 2 of this paper provided evidence that DLT-enabled business value has risen.

But has feasibility increased? To answer that question, it makes sense to understand why feasibility was low in the first place. In other words, what obstacles prevented the successful deployment of a DLT node in an enterprise context? The answer lies in cross-company collaboration. It is hard enough for a singular IT department to manage its own application infrastructure, never mind collaborate with others.

This section describes the historical challenges that all companies face when deploying a DLT node in partnership with a community of other IT departments.

The first challenge corporations face is not technical but operational. Operating a DLT node within an enterprise means that each corporation formally joins a "node operator community" (e.g., partnering with other IT departments). In addition, to operate a DLT node, each company needs to comply with a "DLT governance agreement" describing how companies will work together to support the DLT. The agreement contains specific operational and technical requirements imposed by the community onto the enterprise.

The governance requirements included in the agreement must undergo a risk analysis to determine how much risk the business or operational requirements introduce. Risk analysis organizations must "fan out" to other corporate organizations to communicate, manage, and minimize these risks.

Figure 8 depicts this process. It highlights the central role that risk analysis organizations must play in an eventual DLT deployment.

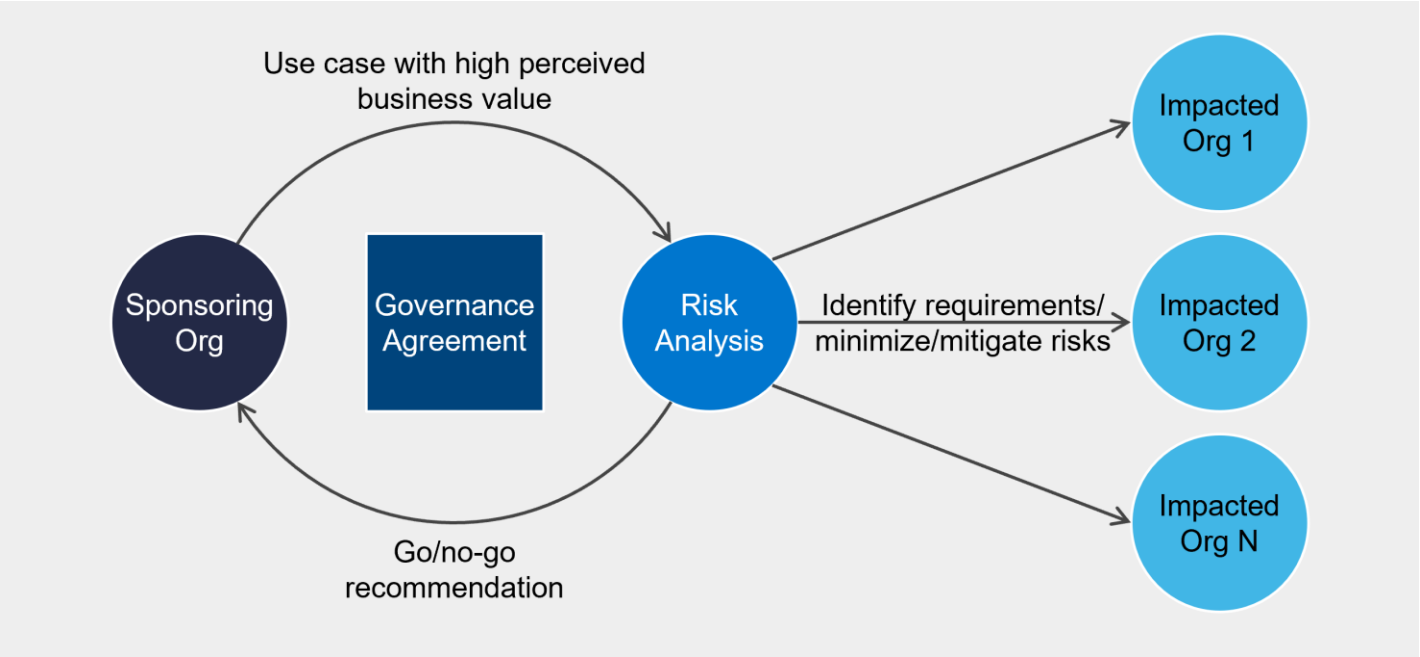


Figure 8 - DLT Governance Requirement Analysis

Figure 8 starts with a sponsoring organization identifying a high-value business opportunity requiring the deployment of a distributed ledger node. One example (as suggested by Figure 5) would be a transportation application that provides traceable, tamper-proof data handling across multiple vendors in distributed environments.

This sponsoring organization could be a corporate line of business (LoB) that would benefit from the deployment. This LoB may determine that a specific type of distributed ledger, with a particular governance model, is the best choice to unlock the perceived business value.

The LoB reaches out to one or more groups that perform risk analysis, explains the business opportunity to them, and requests an analysis.

Review of DLT Governance Requirements

The first obstacle is the risk associated with the requirements of the DLT governance.

To minimize/mitigate risk, the risk analysis teams identify the business and technical requirements. Once identified, these areas typically require a deeper analysis by other organizations. This second obstacle, as described below, can represent the long pole in execution.

The final step is communication back to the sponsoring organization in the form of a go/no-go recommendation. This recommendation will be nuanced; it is difficult to directly compare the potential business value with deployment expenses and potential risk.

How can these obstacles be overcome most efficiently? One approach is to have a checklist describing the potential exposure areas. For DLT governance requirements, the areas of risk/exposure typically fall into the following categories:

- Finance: handling any cryptocurrency-related issues
- Marketing: protecting the corporate brand
- IT departments: provisioning and running a DLT node in alignment with the governance requirements
- Security: managing the risk inherent with DLT applications
- Lines of business: working with a business unit on potential risks related to a new DLT application they wish to deploy

For DLT implementations, the DLT software presents unique considerations, for example, how the ledger joins, operates, and interacts with DLT peer nodes located at other companies/locations.

The sections below describe the ramifications of this uniqueness, or in other words, the obstacles to IT deployment. Each section builds toward the most significant IT obstacle to deployment: security and compliance.

Virtualization / Standard Deployment

Modern enterprise companies strive to operate highly virtualized infrastructure solutions. High levels of virtualization allow these companies to scale application deployment with the following benefits:

- Application deployment is “cloud-like” due to the availability of standard APIs in the virtualization layer.
- Virtualization enables the automation of best practices, often documented in an IT Infrastructure Library (ITIL).
- Virtualization enables workload placement across various IT deployment options, such as customer on premises data centers, co-location, public clouds, etc.
- By placement of mixed-workload types onto the shared infrastructure, virtualization can maximize the allocation and utility of infrastructure resources.

DLT software poses a unique set of infrastructure usage requirements that pose challenges when operating in a virtualized environment. Figure 9 highlights the wide variety of requirements that DLT software can project onto the infrastructure solution/hardware.

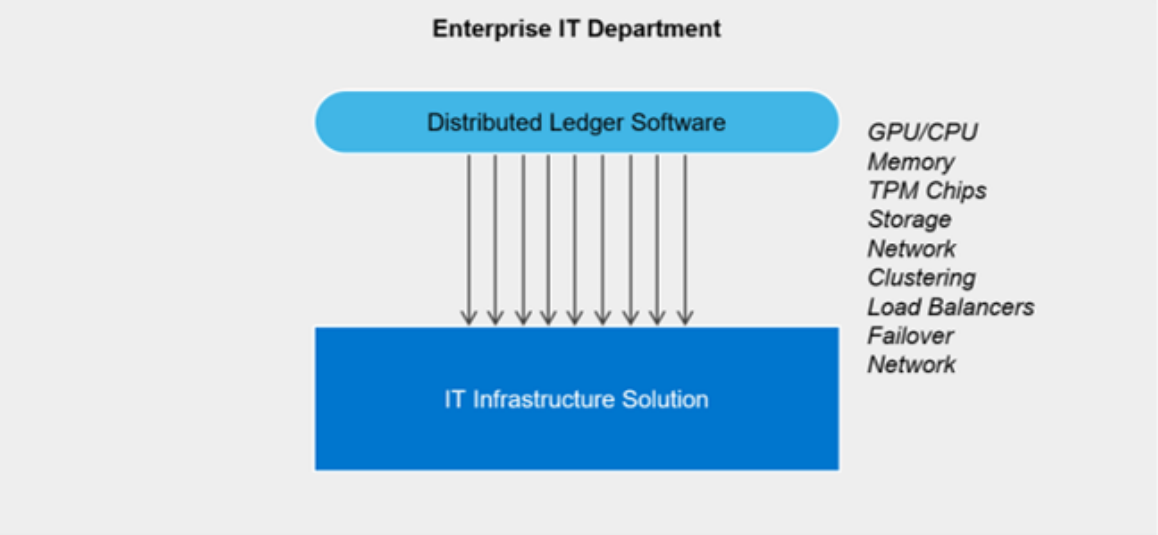


Figure 9 - Unique Infrastructure Requirements for Running DLT Solutions

A virtualized infrastructure should be able to handle these requirements. However, an ‘always-on’ workload impact on infrastructure usage may impact all other workloads operating on the same infrastructure environment. Areas of impact include:

- Storage – high bandwidth requirements for read and write operations and high IOPS requirements for read operations
- Network – high bandwidth requirements, sustained (not burstable)
- Compute – high CPU and memory assignment and persistent utilization

As a result of the usage requirements depicted in Figure 9, DLT software may benefit by having dedicated infrastructure versus a virtualized deployment.

Ensuring that all infrastructure—dedicated or virtualized—adheres to IT and security enterprise policies needs further consideration. The virtualization layer helps ensure that a secure suite of processes is entirely in place, consistent security and vulnerability processes are complied with, and uniform/reliable IT infrastructures adhering to these policies are available for the enterprise.

The need for dedicated DLT infrastructure challenges the desire that all deployed applications adhere to, and are enforced by, these standard policies.

Single Versus Multi-Tenant

In addition to depending on virtualization, many enterprise companies assume application deployment with a single internal tenant as the consumer or provider. DLT software, on the other hand, is an application that provides ledger services to potentially thousands of tenants.

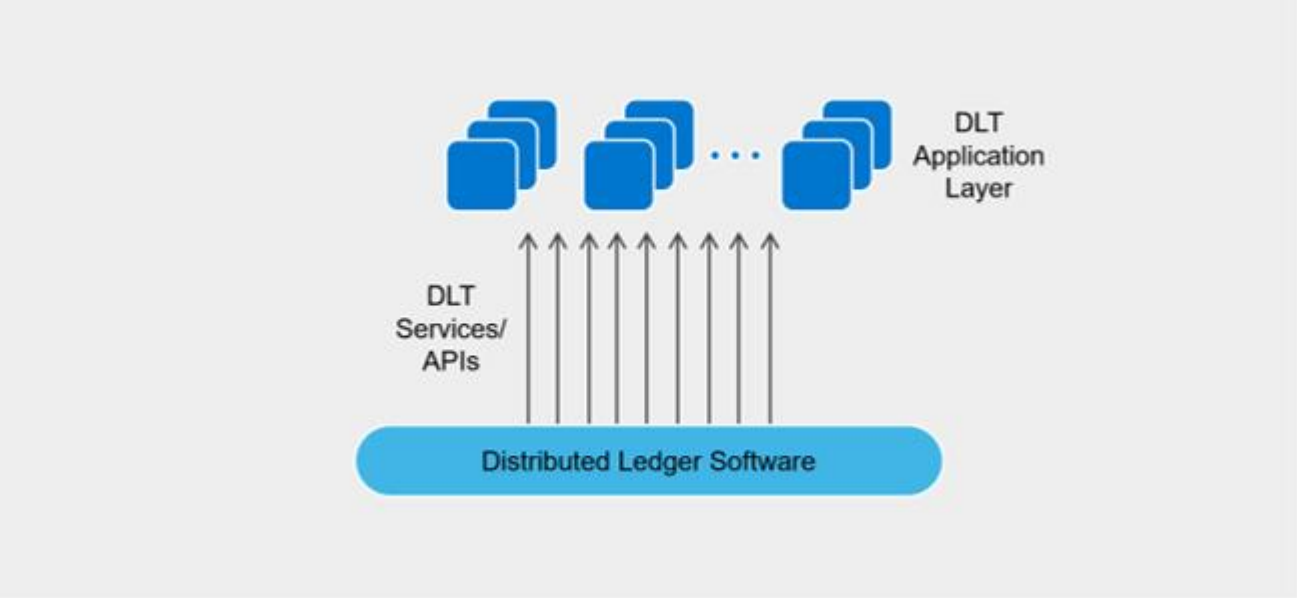


Figure 10 - Multi-Tenant Support to DLT Applications

The scenario depicted in Figure 10 is unique because the applications shown at the DLT application layer may be external, unknown, and dynamic if the DLT is public. An enterprise must understand the challenges of hosting a multi-tenant application and the various additional guardrails required to enable DLT multi-tenant hosting capabilities.

Data Classification and Mapping

The reality of multi-tenant applications leveraging DLT services leads to another unique challenge: the classification and mapping of the data stored within the ledger. Figure 11 highlights this problem.

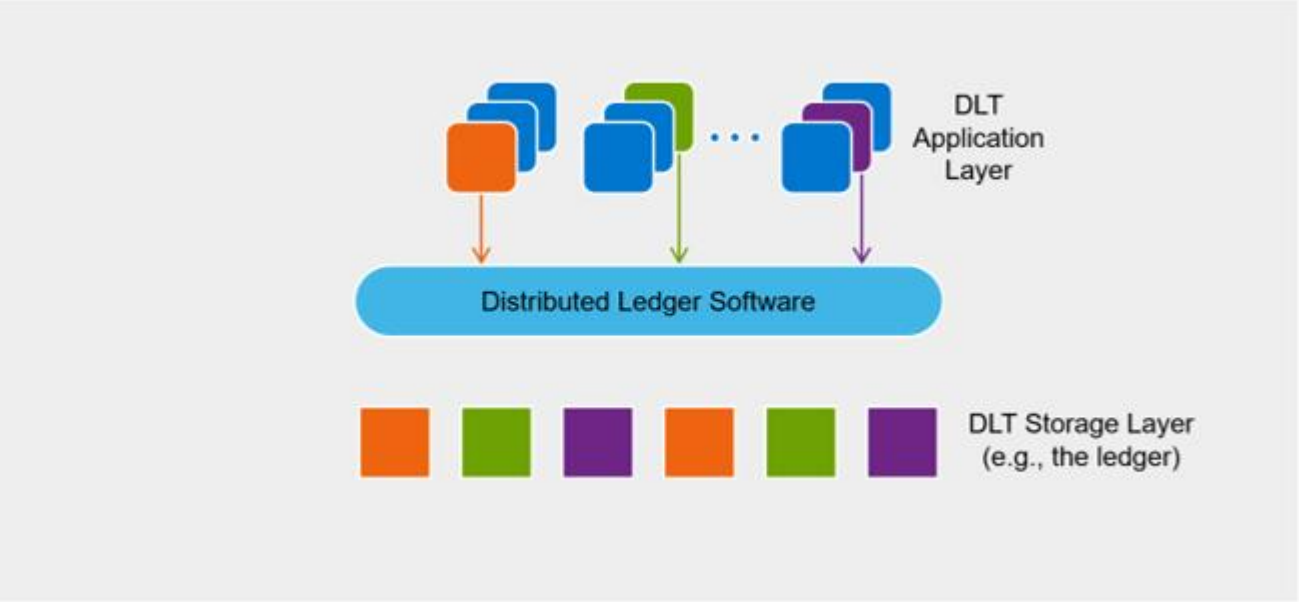


Figure 11 - DLT Storage Layer Storing "Unclassified" Data

Figure 11 shows multiple tenants creating DLT transactions that persist in a DLT storage layer; note that there are various ways to implement this storage layer, for example, as a “chain of blocks” or as a graph. Therefore, data that traverses the solution is multi-tenant/multi-enterprise-based, not solely mapped to any given—or known—single tenant. The challenge, however, is that the enterprise IT department running the application has no visibility into “who” these applications are and “what kind” of data these applications are storing. IT departments are under increasing pressure to classify the data under their care; this becomes impossible, given the uniqueness of the DLT software.

One more concern related to data is the design of the storage layer. Is server-local storage required, or is a more comprehensive, shared-storage solution more appropriate?

Network Connectivity / Application Placement

While the challenges listed above are already quite substantial, the network connectivity required by the DLT software introduces additional new issues.

Figures 9-11 highlighted an application deployed on, for example, a single server. Behind the scenes, however, the application logically enables a highly decentralized set of operations as it participates in the DLT’s distributed network of nodes. These nodes are running in other companies and geographic locations.

Figure 12 sets the scene for these challenges.

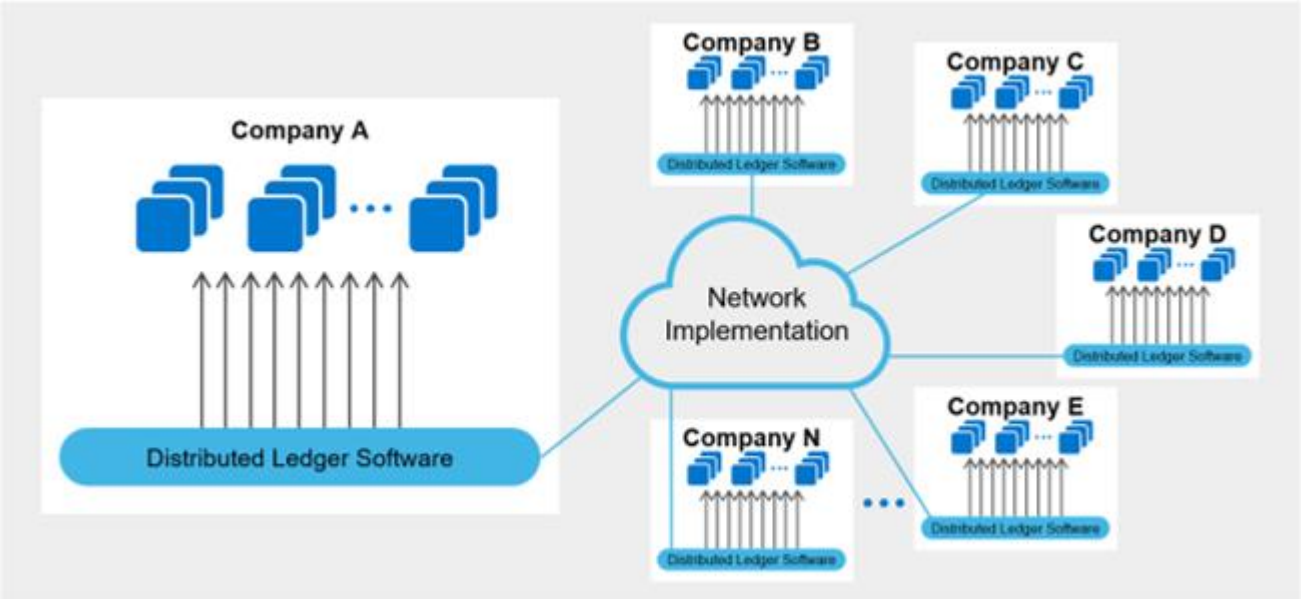


Figure 12 - Network Requirements for Peer DLT Community

The community of companies that make up the DLT Governance Body must agree together—perhaps as part of a governance agreement—on the specifics of the network implementation, for example, the public internet.

The unique requirements of a DLT's connectivity to peer nodes at remote locations result in the following challenges:

- The placement, for example, location, of the DLT software is heavily dependent on the network implementation. For example, if the DLT community plans on providing general—in other words, public— availability, the IT department may have a larger number of geographic deployment choices. These choices may include a public cloud, colocation providers, or a DMZ. But if the computing requirements for the DLT software are highly specialized, a colocation or DMZ may be preferred.
- Sizing the network bandwidth requirements is a challenge. The communication protocols between nodes at different companies may need to be discovered or better understood. The eventual number of applications deployed on top of the DLT may also be unknown, under-estimated, or over-estimated. This can result in congestion—under-estimation—or wasted provisioning—over-estimation.
- Given that network bandwidth sizing is challenging, the network impact on other applications running alongside the DLT—for example, the noisy neighbor problem—is unknown.
- The DLT governance may have availability requirements that impact the design of the network implementation, such as fault tolerance/failover capabilities.

Application Deployment and Operation

Most enterprise companies assume that every application deployment maps to an internal organization. Figure 8 highlights a “Sponsoring Org” that is trying to provide new sources of business value to the company. However, this organization is not responsible for the DLT software. Instead, the creator is an external entity, resulting in new challenges to traditional IT processes. These challenges are best described in a “Day 0” to “Day 2” software lifecycle process.[xiv]

- Day 0 is the planning and design process. There is perhaps no more disruptive phase than this one, starting with the initial engagement of the IT department.
    - The “Sponsoring Org” must engage the IT department. Large IT departments have automated onboarding and out-of-the-box processes that optimize deployment timelines by quickly instantiating the underlying infrastructure.
    - As highlighted above, the uniqueness of the DLT software is not suited for automated onboarding. Each step of the automated process may require a call-out to a manual team, such as the network team or the storage team, to address the unique and new ramifications related to DLT hardware, multi-tenancy, data, network, etc.
    - The call-out to manual teams can result in inter-departmental sprawl. All issues—virtualization, network, data, etc.—are interrelated, requiring multiple conversations across multiple parties. The security organization must also be involved in all discussions.
    - The end of the Day 0 phase results in two recommendations. These two risks will ultimately be balanced against the perceived/potential business value initially proposed by the sponsoring organization.
        - A recommended deployment location and an associated “cost of deployment and operation.”
        - A statement of risk from the security organization.
- Day 1 is the initial deployment phase. This phase results in the installation of the software at the recommended deployment location, which has the following challenges.
    - In the case of a dedicated appliance to run the DLT software, it is unlikely that the internal deployment team can leverage any of its automated installation processes. Therefore, this internal team must interface with the DLT community to get the first instance up and running. The DLT community may wish to perform this step remotely, which raises security concerns.
    - Upon the completion of the first install, there will likely be a “burn-in” period to confirm that the Day 0 design satisfies the community's performance, functionality, and security requirements, which are often listed in the governance agreement or an accompanying document. Issues uncovered during the burn-in period often require configuration changes or upgrades. The local team will not have sufficient knowledge to make these changes independently.
- Day 2 is the daily operations phase. The local deployment team works with the DLT community to continually monitor the health and operational success of the DLT.
    - The local team will likely need new tools or skills to observe the overall health and performance of the DLT software.
    - One of the biggest challenges inherent in this phase is participating in upgrading DLT features or making bug fixes. These upgrades will likely not be able to leverage internal automated upgrade processes.
    - Division of shared roles and responsibilities for the application between the DLT community and the local team will need to be defined.

Security and Compliance

An enterprise Chief Information Security Officer (CISO) should continually revise and enhances security policies to ensure that an enterprise's most valuable assets are adequately guarded and secured from unauthorized access. This includes internal data and business processes/applications impacting primary revenue and profit-generating operations.

CISOs will need to review in detail how DLTs may impact current security and data protection policies, such as:

- DLT governance agreement and terms
  - Hosting requirements, such as SOC2 equivalent
  - DLT and node technical and operational roles and responsibilities
- Security / vulnerability review
  - Software and technology standards review
  - Information and data handling review
  - Information privacy review
- Security and Reliability Office (SRO) validation
  - Adherence to security policies from onboarding and day 2 operations
  - Technical audits
  - Operational audits

This section outlines why DLT feasibility has been so low; there is much to consider.

How can corporations overcome these obstacles? One approach is to leverage a community of experienced DLT deployers. Section 4 describes such a community.

Use Case: Hedera Governance Council

Given the long list of challenges described in Section 3, how can the industry increase the feasibility of DLT implementations and realize business value?

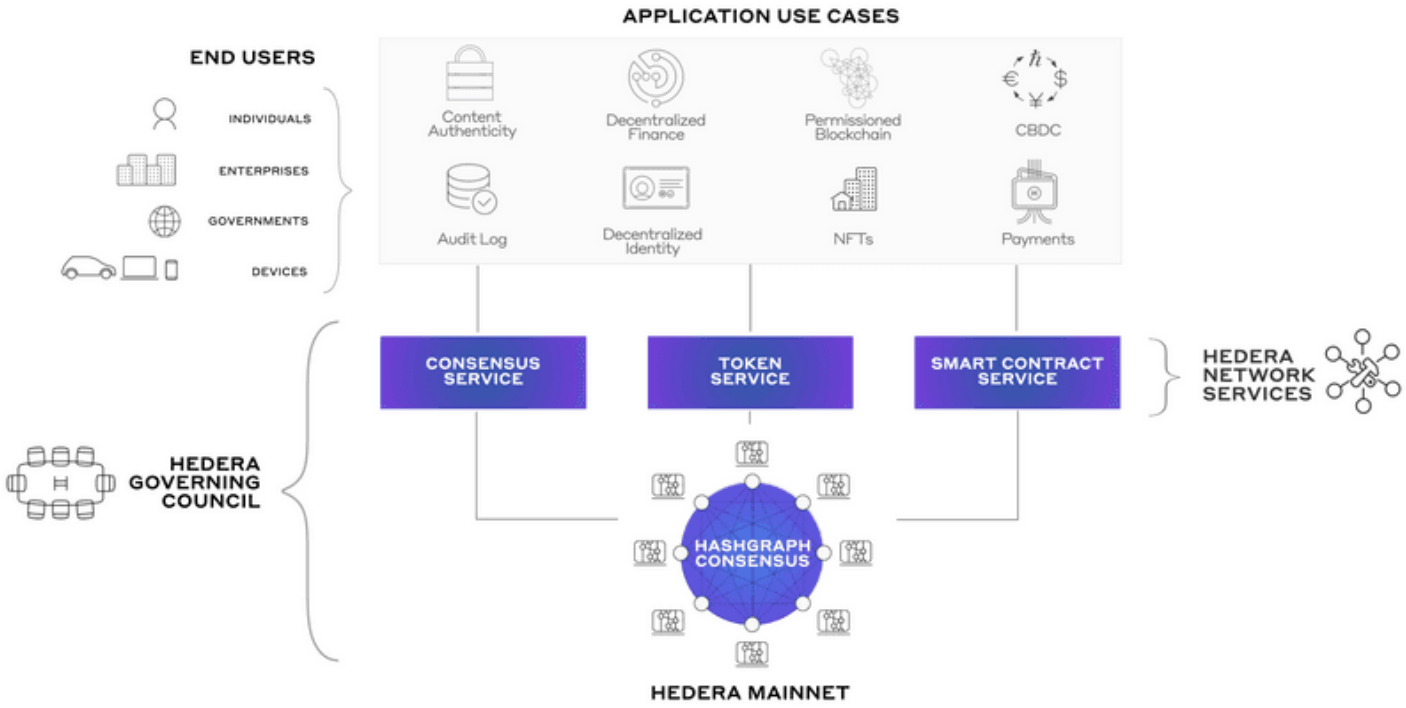
According to the Accenture report[xv] mentioned above, the answer is to join with others effectively. "The whole point of doing blockchain is it's a team sport," Christopher G. McDaniel, President of the Institutes RiskBlock Alliance, explains. "If you're trying to do it on your own, maybe that's OK from a proof-of concept standpoint, but if you ever want to get real production value, you have to join with others. Otherwise there's no point."

This section introduces a DLT community that brings together organizations from across different industries and geographies: the Hedera Governing Council. Its approach eases the feasibility difficulties by providing DLT deployment best practices across disparate companies.

This does not mean that DLT deployment becomes simple. This section outlines that enterprise companies will still have a significant amount of work to do. DLT deployment becomes easier but not easy.

Hedera is:[xvi] "a fully open source, proof-of-stake, public network, and governing body for building and deploying decentralized applications. It offers developers three primary services: Solidity-based smart contracts, consensus, and token services. Hedera is unique in that it is incredibly fast, energy-efficient (carbon negative), and secure – these advantages can be attributed to its underlying hash graph consensus algorithm."

Figure 13 provides a high-level diagram that depicts the Hedera Council overseeing the three DLT services—consensus, token, and smart contract—to various application use cases and users.



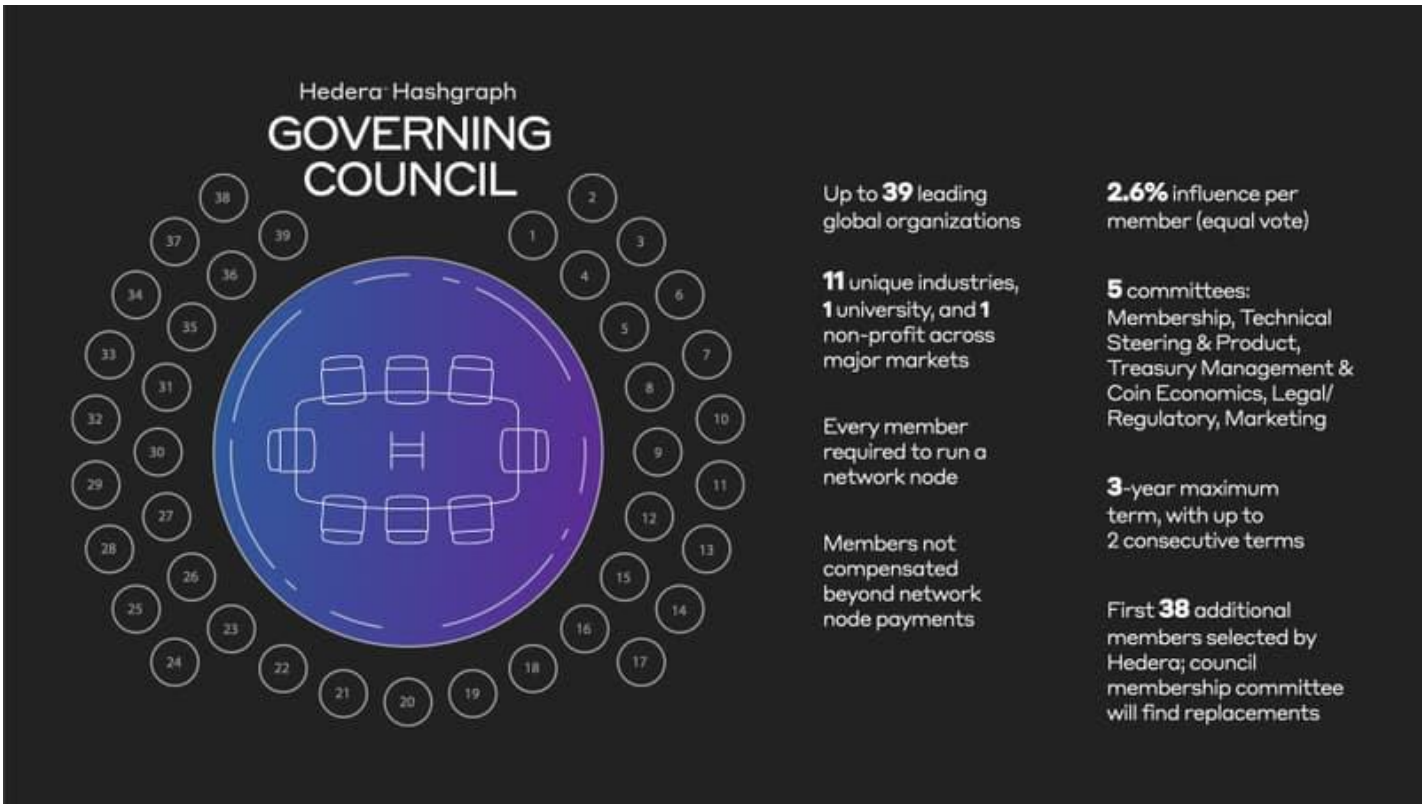
Hedera [xvii]

Figure 13 - Hedera Overview

In this paper, we have explored the challenges inherent in operating a DLT node within an enterprise. Figure 13 depicts a Governance Council setting standards for the decentralized operations of a DLT, known as the Hedera Mainnet.

The Hedera Council is "an expert council consisting of [up to] 39 leading global organizations, distributed across 11 different industries and spanning a wide range of geographies. The Governing Council is completely decentralized – every member has an equal vote over software upgrades, network pricing, treasury management, and more. Governing Council members are term-limited and do not receive any profits from Hedera."[xviii]

Figure 14 depicts the Hedera Governing Council's makeup and each member's responsibilities[xix].



Hedera[xx]

Figure 14 - Hedera Governing Council

The challenges of DLT deployment, as described in Section 3 above, span a variety of departments within a company, including Marketing, Finance, and IT.

Since every member is required to run a network node, the first step is for risk analysis organizations to analyze the operational and business requirements found in the governance agreement. Hedera has created a governance council structure [xxi] acceptable to many corporations, notably those listed in Figure 16, by providing the following terms (found in Hedera's LLC agreement)[xxii]:

- Simple decentralized governance: every member has an equal vote.
- Straightforward member obligations:
  - Participation in meetings and governance activities.
  - Operation of a Hedera node.
  - Compliance with Hedera policies, especially signing network transactions that carry out governance decisions.
- No restrictions on joining other DLT communities.
- Easy ability to exit the Council (can exit for any reason by giving 30 days' notice).
- Strong liability protection under Delaware law and no fiduciary duties.
- Limited financial implications, with no material equity investment or economic interests in the LLC (though subsidies to reimburse a company's node expenses and revenues received as node fees may be taxable).

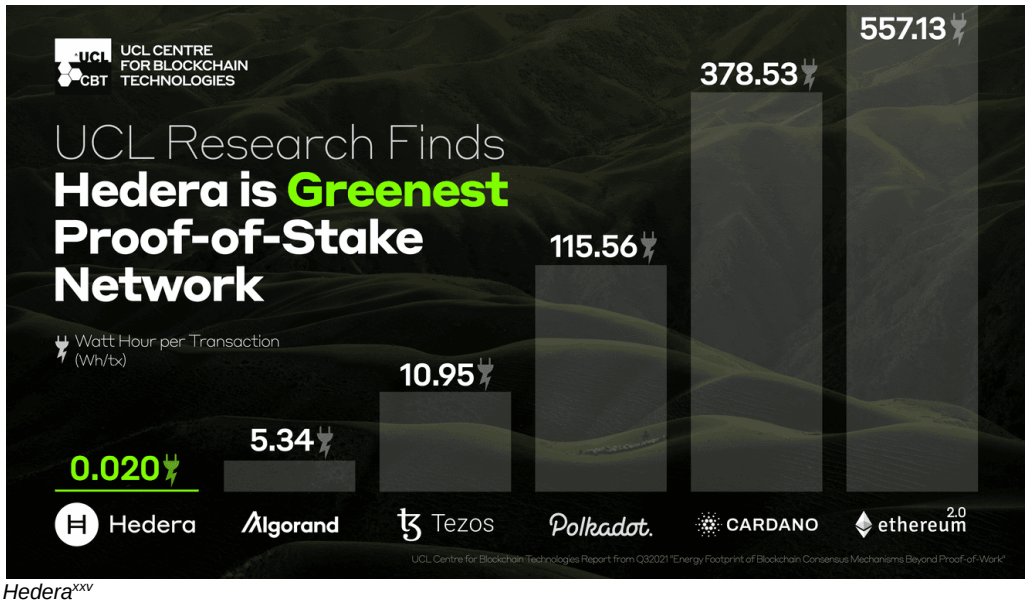
Any risk analysis team may still have concerns related to DLTs— (and cryptocurrency in general). For these concerns, Hedera provides the following guidance[xxiii]:

- The goal is for Hedera to be the standard-bearer for DLTs and be compliant with applicable regulations in the face of existing regulatory uncertainty (existing laws often do not cleanly map to new technologies).
- Hedera has made provision for illegal content; the Hedera Council will remove an illegal file if law enforcement or a valid legal authority notifies Hedera.
- There are tools to delete files related to GDPR compliance. Nodes just process network transactions, and nothing is running in a node that should cause it to violate GDPR.
- Hedera does counterparty due diligence on entities it directly interacts with, such as investors, purchasers, grantees, members, and anyone Hedera sends HBARs (the Hedera cryptocurrency).
- Hedera screens direct counterparties against OFAC-issued sanctions lists.

For a prospective council member, the above concerns may represent a potential risk to the corporate brand. As depicted in Figure 8, a risk analysis team will interface with various internal business units to manage and minimize that risk.

One vital team to consult is the group responsible for the corporate brand. Given the public controversy generated by the terms “blockchain,” “cryptocurrency,” and “mining,” this team must carefully study the Hedera technology itself to learn about potential risks.

One such risk is having DLT nodes associated with wasteful, environmentally unfriendly “proof-of-work” mining operations. A third-party study [xxiv] of the energy usage of different DLT networks shows Hedera’s low environmental impact. Figure 15 highlights the results of this study.



Hedera[xxv]

Figure 15 - Hedera Proof-of-Stake Footprint

This study compared six different DLT implementations and measured overall watt hour per transaction. This type of ESG data should be made public as a corporation manages and minimizes risk, especially to its brand. As an open-source technology and cross-corporate governance council, Hedera provides transparency into the many issues that surface during review of the business and operational requirements. This transparency also extends to assisting an IT department in navigating the risk of deploying a decentralized technology into a heavily centralized environment. Hedera assists companies in navigating questions and issues from Day 0 through Day 2.

Day 0 Operations

Because the lowest-performing node limits Mainnet performance, the Hedera Governing Council endeavors to help its members deploy highly performing nodes.[xxvi] Hedera has published a set of node requirements that will satisfy the operational needs of the Hedera DLT.

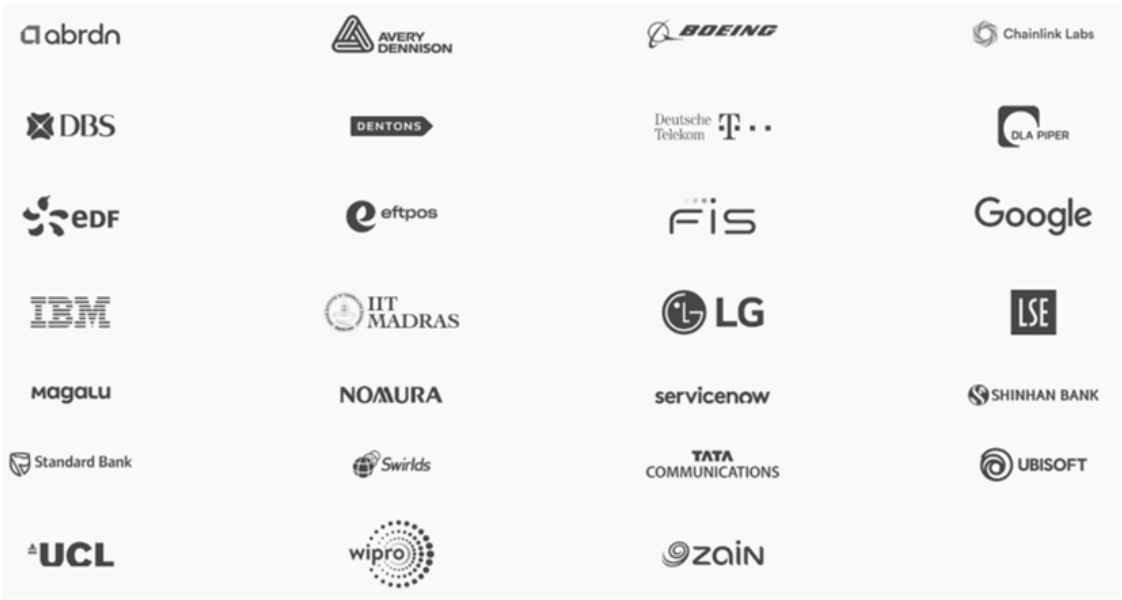
However, each company may have unique marketing, finance, or IT challenges (as described above). This uniqueness means that the Hedera Governing Council must allow different deployment options. As of 2022, the company has demonstrated and run[xxvii] production Mainnet nodes in a variety of configurations:

- Bare metal (e.g., Dell Technologies PowerEdge R740XD Server)
    - Purchased (capital expense)
        - within a member company's private data center
        - in a co-location provider
        - using Intel Xeon or AMD Epyc CPUs
- Leased (short- and long-term operating expenses) among a variety of bare-metal hosting providers worldwide
- Virtual Private Server (VPS) – virtualized machines on dedicated hardware
- Virtualized / Cloud deployments – including major cloud providers such as AWS, GCP, Azure, IBM Cloud, Oracle Cloud

What is the benefit of this flexibility? First, it allows each member organization more options as they deal with internal obstacles to DLT deployment, such as network bandwidth or virtualization difficulties. Second, it will enable each IT department to deliver a Day 0 realizable design.

Some Council members may have concerns about the long-term cost of a cloud deployment. Hedera provides advice[xxviii] in this regard as well: "Hedera and its members have noticed that for the same level of performance, cloud deployments tend to be substantially more expensive than bare-metal (regardless whether privately hosted, in co-location data centers or leased via so-called "bare metal cloud" providers). Showing the cost advantage with members has been a strong motivator towards considering the option."

The Hedera member companies may obtain Day 0 consulting by Hedera employees Council staff. Figure 16 shows[xxix] the current list of member companies—as of December 2022.



Hedera[xxx]

Figure 16 - Hedera Governing Council Member Companies (2022)

As each company attempts to deploy its first Hedera DLT node, it can draw on the collective community experiences of other council members. For example, a new company deploying a new Hedera node can ask other companies about design decisions, such as:

- How they performed security and risk assessments
- How they presented to architecture review boards and other corporate governance bodies
- How to comply with local/international laws and regulations
- How they configured their network, virtualized, firewalled, or isolated their Hedera node
- How they vetted external Hedera users, applications (Dapps), and ledger data against internal policies

The Day 0 planning ends with a final review of the planned hosting solution before purchase to ensure that the solution indeed meets Hedera specifications. This last step is critical because the Hedera team will need to access this solution directly during Day 1 activities.

Day 1 Operations

The installation of the Hedera node requires direct access to the solution by Hedera. For this reason, a company may take steps to isolate its solution, as depicted in Figure 17.

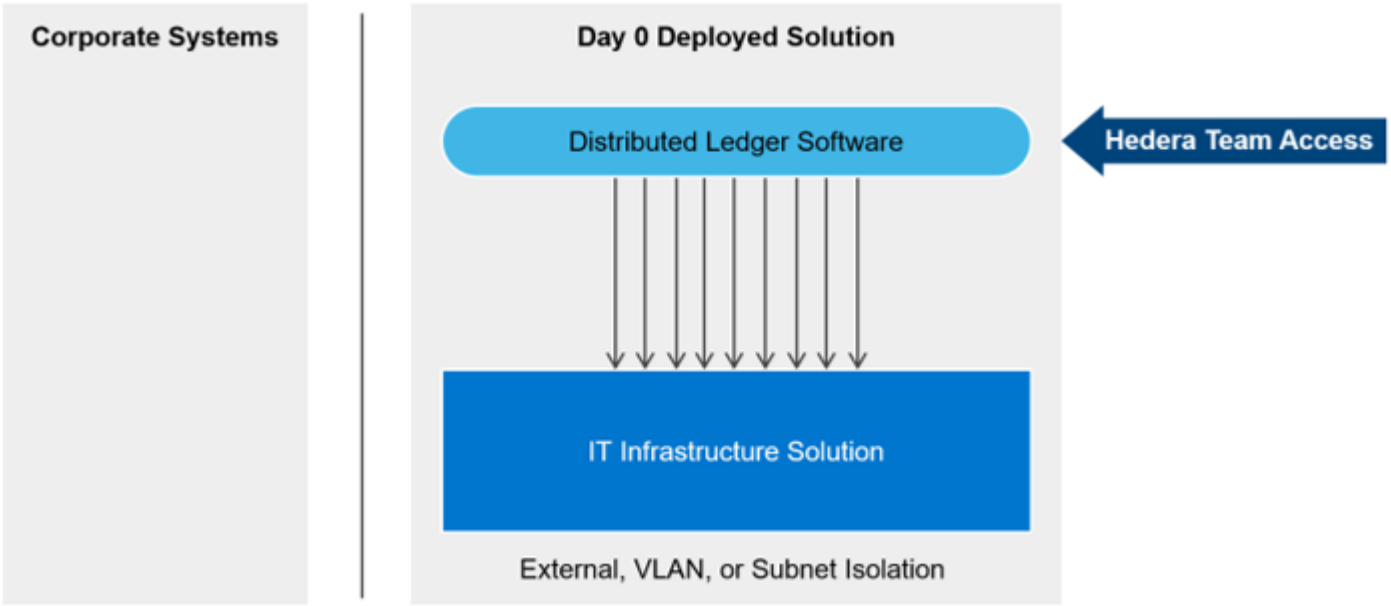


Figure 17 - Segmented Day 1 Access by Hedera

Day 1 activities involve constant communication between the Hedera and local IT teams.

The Hedera team utilizes direct access to the new Hedera node to validate the configuration and deploy the DLT software. This process does not need communication or access to existing corporate systems. The DLT software deploys as a docker container. After installation is complete, the deployed solution is integrated into a Hedera staging area and undergoes functional, performance, and longevity testing.[xxxi]

This burn-in period can last for several weeks and is a teaching experience for the local IT team as they begin to understand the functionality and operation of the Hedera technology. In addition, the local team gains experience monitoring the CPU, memory, storage, and network utilization to understand the eventual needs of the solution and how it might best integrate into a final deployment.

The end of Day 1 activity may result in an IT department leaving the node exactly where it is: firewalled and segmented away from the rest of the corporate infrastructure. However, in the long term, a DLT node must have some integration into corporate systems to maximize business value. Section 5 further explains this integrated vision for maximizing business value.

Day 2 Operations

After the Hedera team completes the burn-in process and the IT team deems the solution ready, the node joins the Hedera Mainnet. The interactions between Hedera and the IT team remain regular until achieving a steady state, and the DLT node becomes a regular contributor.

From that point on, Day 2 operations are best described by the following statement and bullet points[xxxii].Hedera will need to collaborate to coordinate maintenance activities and have established communication protocols for escalation in a bilateral capacity. In other words, Day 2 operations for the Hedera DLT node will still require collaboration, with responsibilities divided across the following lines.

Hedera responsibilities:

- The Hedera DevOps team is flexible in integrating with a member's IT ticketing and operations processes to ensure timely resolution of support as needed.
- Hedera provides operations teams with regular reporting of their node's performance and activity. Later in 2023, Hedera will integrate a real-time dashboard into its monitoring architecture.
- Updates to the Hedera code occur via an automated process conducted by transactions on Hedera's Mainnet (local IT staff involvement is not required). This upgrade process involves two primary transactions, signed by the Hedera Council members:
    - Instruct the node to download and validate the new update code.
    - Schedule the upgrade to the new codebase across all active nodes in a unified manner.

Local IT Staff (Hedera member company) responsibilities:

- The local team must ensure the availability of the host. For bare metal systems, members monitor for potential hardware failures and have an appropriate sparing strategy.
- Members should also monitor for network performance and availability of allocated connectivity to hosts on Hedera's network.
- For planned maintenance or unplanned network disruptions, backups are unnecessary; Hedera has an automated "reconnect" process. However, Hedera recommends taking snapshots of the host minus the data partition during any change events, such as OS patching or Hedera code upgrades, which eases rebuilding in disaster recovery scenarios.
- Currently, Hedera's network still requires Hedera DevOps host access. It is planned for this access to be removed later in 2023 as part of ongoing decentralization activities.

It has been Hedera's experience that day-to-day management of the host is minimal, with several members not being involved other than regular OS patching and integration into their operations centers. System playbooks assist node operators in their monitoring and management responsibilities.[xxxiii]

With a DLT node successfully deployed by their IT department, member companies enable their employees to begin writing new business logic, known as Hedera Dapps, and deploying production-grade applications to bring business value.

Indeed, several Hedera member companies have already deployed production—or near-production—applications generating new forms of business value. Recall that business value is found, per the Accenture article, in building applications that can handle distributed data in a transparent and tamper-proof way.

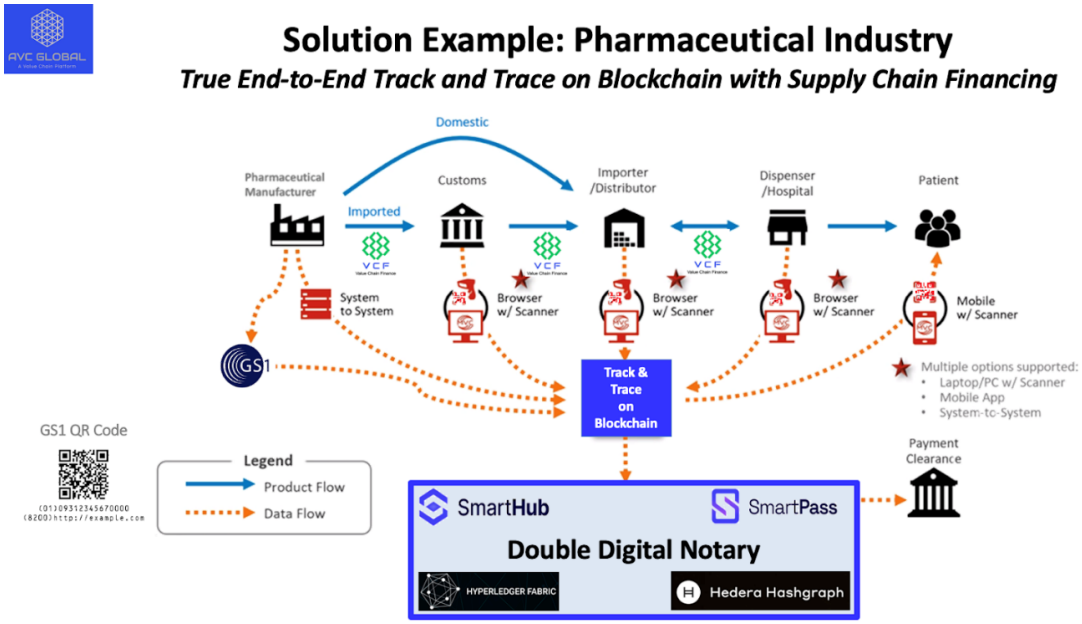
Below are several examples of new applications use the Hedera DLT to handle distributed data in a

transparent and tamper-proof way.

A first example is AVG Global[xxxiv], which uses Hedera to manage threats to pharmaceutical supply chains. These supply chains are increasingly international and decentralized, presenting many opportunities for tampering with the insertion of counterfeit drugs into the supply chain. This DLT use case checks all three boxes for solving the complex combination of distributed data, transparency, and tamper-proof data.

- The pharmaceutical supply chain is highly distributed, involving pharmaceutical manufacturers, customs (for international shipments), importers, dispensers, hospitals, and patients.
- AVG Global uses Hedera as part of a "double digital notary" system for end-to-end transparency. A drug is registered at manufacturing time, and logging occurs throughout the supply chain.
- Drug counterfeiters cannot tamper with any section of the supply chain to insert their drugs.

Figure 18 highlights the Hedera-based solution implemented by AVG Global.



Hedera[xxxv]

Figure 18 - AVG Global's Tamper-proof, Transparent Supply Chain

Other similar use cases leverage the Hedera DLT:

- Everyware[xxxvi] monitors temperature readings of the Pfizer COVID-19 vaccine for the cold storage supply chain, providing transparency and tamper-proof confidence in vaccine delivery.
- EVEC[xxxvii] prevents spoofing of IoT sensor devices, encrypting device data at the point of creation and using a technique similar to zero knowledge proofs to authenticate and authorize device transactions.
- Neuron[xxxviii] performs decentralized drone tracking and management, with tamper-proof data providing proof between parties in a court of law.

This section has documented Hedera's approach to increasing DLT deployment feasibility. It began with a review of governance requirements, whereby multiple departments (finance, IT, etc.) learned about the risks of DLT and devised a plan to manage and minimize those risks through collaboration with Hedera and its member companies.

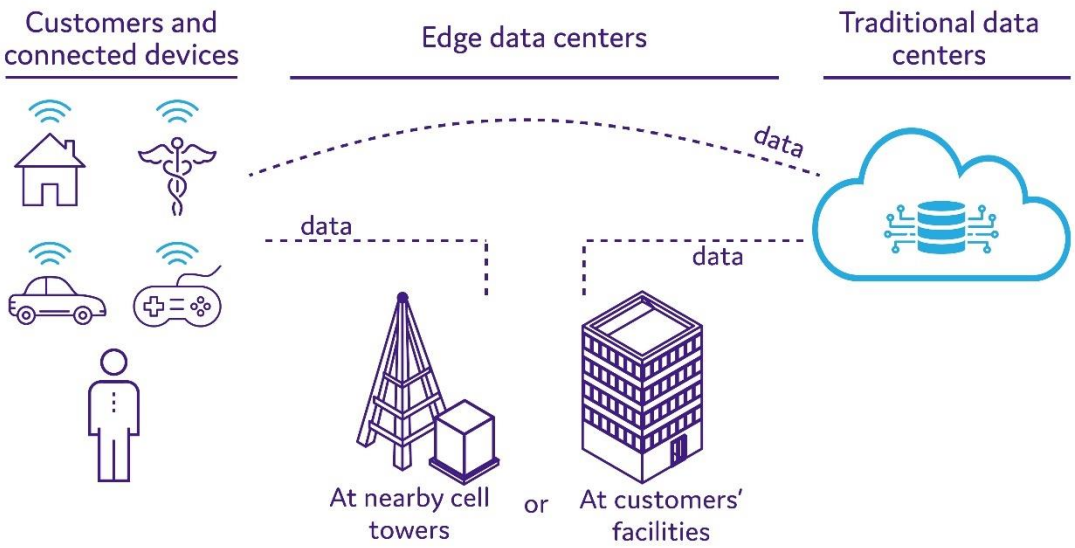
One last step is to raise visibility across the entire corporation before agreeing to join the community. This allows the C-level team to know the plan to deploy a DLT fully and allows each executive to launch DLT application development initiatives.

With increased business value and DLT feasibility, corporations can begin to move forward to find high-value business opportunities.

No business opportunity has more potential than extracting value from edge data.

A Vision for Moving Forward

One definition of edge computing[xxxix] is, "*a distributed IT architecture where client data is processed as close to the originating source as possible.*" In this context, Figure 19 diagrams[xl] an increasingly popular edge architecture for processing data using locations known as edge data centers.



Prolabs[xli]

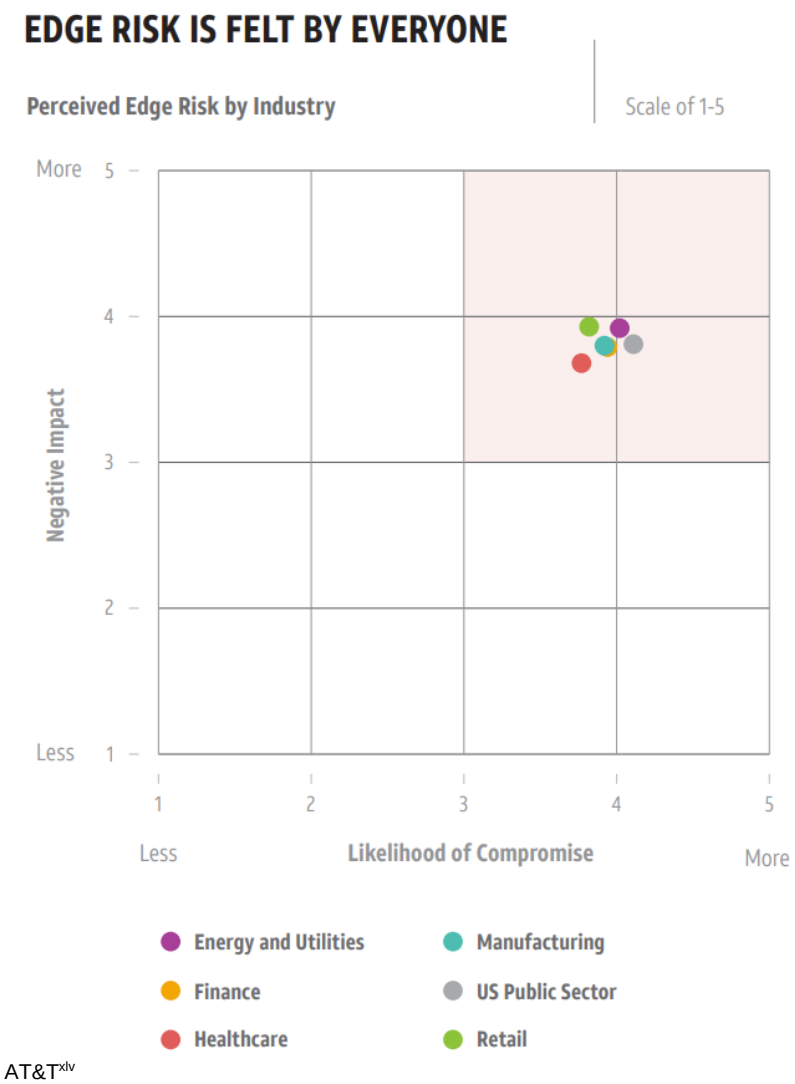
Figure 19 - Data Processing via Edge Data Centers

An edge data center[xlii] has the following definition: "data centers that are located close to the edge of the network… they provide the same devices found in traditional data centers, but are contained in a smaller footprint, closer to end users and devices."

Consider an edge data center's role in providing enterprise access to rich sensor and customer data. And recall Gartner's 2025 prediction[xliii] that "50% of enterprise-managed data will be created and processed outside the data center."

Although the technologies deployed within edge data centers are like that of traditional data centers, there remains a problem: the trusted technologies, policies, processes, and people that allow confident data processing in the data center do not scale to the edge.

As a result, trying to extract business value from this data is fraught with business risk. For example, an AT&T edge cybersecurity report[xliv] concluded that "edge risk is felt by everyone." Figure 20 shows a graphic from that survey describing the risk.



AT&T[xlv]

Figure 20 - Perceived Edge Risk by Industry

The AT&T report asked respondents across several industries to rate their "likelihood of compromise" to their edge systems on a scale of 1-5 and the corresponding negative impact it would have (also on a scale of 1-5). Each risk can have a negative impact[xlvi] on the balance sheet, including "lost value, incident costs, downtime, damaged reputation," etc. Companies also put themselves at risk of heavy fines if they can't prove compliant handling of data.

Many of these risks have already been managed and minimized in data centers using centralized techniques that support strong identity management, access control, compliance, vetted service enablement, etc. But there are gaps between traditional, trusted data center processing versus the edge.

Figure 21 highlights the "data trust gaps" found on either side of edge data centers as they increasingly insert themselves between IoT data generators on the left and traditional, trusted data centers on the right.

Figure 21 - Edge Data Trust Gaps

Distributed ledgers can extend the trusted techniques found in the data center to decentralized environments and close these gaps.

Interestingly, in 2018 a GMSA study[xlvii] identified opportunities for distributed ledgers to address many of the gaps specific to IoT data processing. This study suggested that the following data center strengths could extend to customers and connected devices via a DLT.

- **Identity for IoT devices**: ledgers can store a device's origin, authenticity, and status in a DLT. The DLT can also be used to manage onboarding and upgrades securely.
- **Access control**: DLTs can hold the identities of authorized users to access physical/logical assets.
- **Compliance**: Smart contracts provided by DLTs can contain the "rules of engagement" around data, especially across multiple parties.
- **Data sharing and integrity**: DLT digital signatures and data hashes can help register data at birth and track data movement and distribution.

Figure 22 proposes a "DLT Trusted Data Bridge" as a backbone for trustworthy data transactions from the device layer to the data center.

Figure 22 - DLT Trusted Data Bridge

This DLT vision for moving forward is only possible when the DLT bridge extends from the data source into the data center. As this paper has proven, positioning DLT nodes within the data center is now more feasible.

Consider an enterprise application developer writing a DLT application that runs in a data center environment. Figure 23 highlights how the application business logic can:

1. Access corporate systems
2. Access the local DLT node
3. Influence trusted transaction in the edge ecosystem

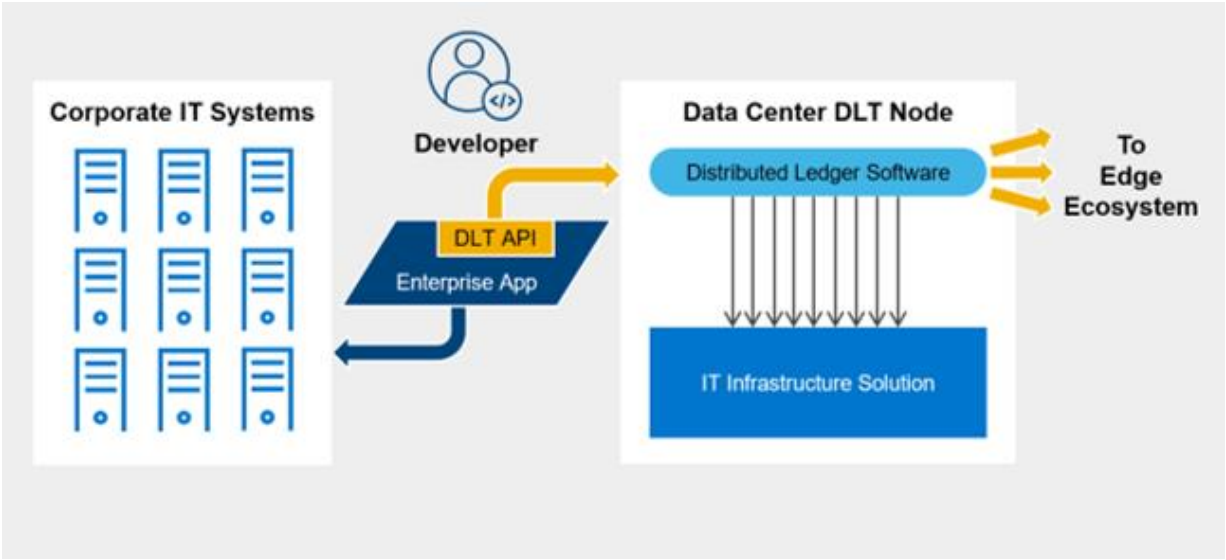


Figure 23 - Application Development That Bridges Enterprise / Edge

This vision extends further when considering new enterprise-class applications that do not access corporate IT systems but operate at the edge data center layer. Figure 24 shows this capability.

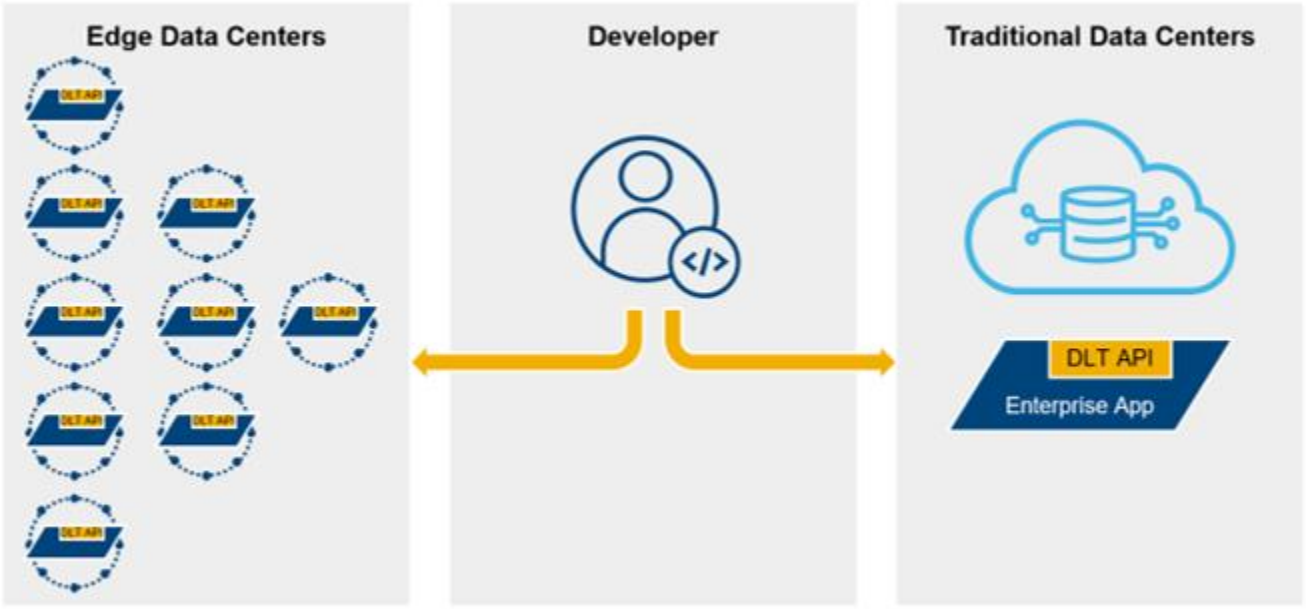


Figure 24 - DLT Applications Extend to Edge Data Centers

Figure 24 highlights the movement of trusted enterprise applications outside the data center, moving closer to the ultimate target: sensor data from the far edge. The applications, whether running inside or outside the data center, leverage the common identity, access control, compliance, and data-sharing primitives provided by the underlying DLT.

This leads to the ultimate vision for conducting business transactions against edge data: a Data Confidence Fabric (DCF). The creation and movement of all data, and every application, are tracked in a DLT. The DCF scores everything that happens. Figure 25 highlights sensor data arriving at a DCF-enabled edge data center node, where a trustworthy business transaction occurs between two “high-confidence” entities.

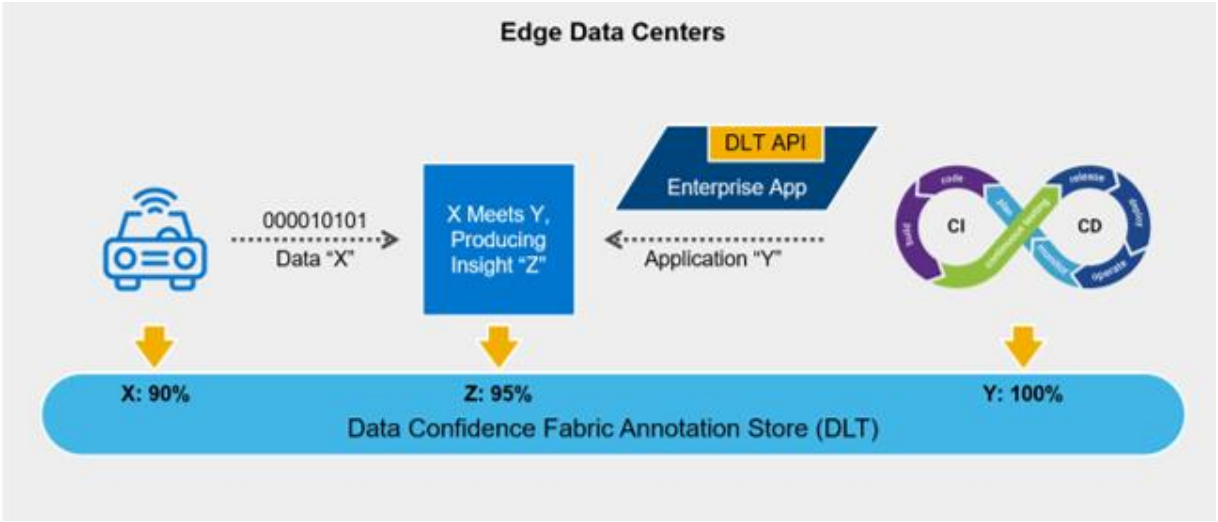


Figure 25 - Edge-based Digital Transactions Conducted with Measurable Confidence

DLTs have the critical characteristic of scale, allowing them to “stretch” from sensors to edge data centers to data centers. This allows edge data sources, such as a connected car, to register newly created, high-confidence data in the DLT and associate a confidence score, such as X: 90%. It also allows enterprise developers to register freshly manufactured, high-confidence applications emerging from trusted CICD pipelines and associate a similar confidence score, like Y: 100%
This paradigm allows edge data centers to perform trusted computing—or not—on well-known edge data.

For the first time, DLTs allow decentralized applications and data to inspect each other's confidence scores and lineage. If the confidence scores are high enough, the transaction occurs, and the resulting business insight, for example, insight "Z" in Figure 25, receives a corresponding confidence score.

If the confidence scores are not high enough, the transaction may either be dropped or handled differently. Either way, an audit trail results, proving to an eventual auditor that the application followed all data policies. For example, Figure 26 highlights an auditor inspecting the tamper-resistant, deletion-resistant components of every step of a digital business transaction.

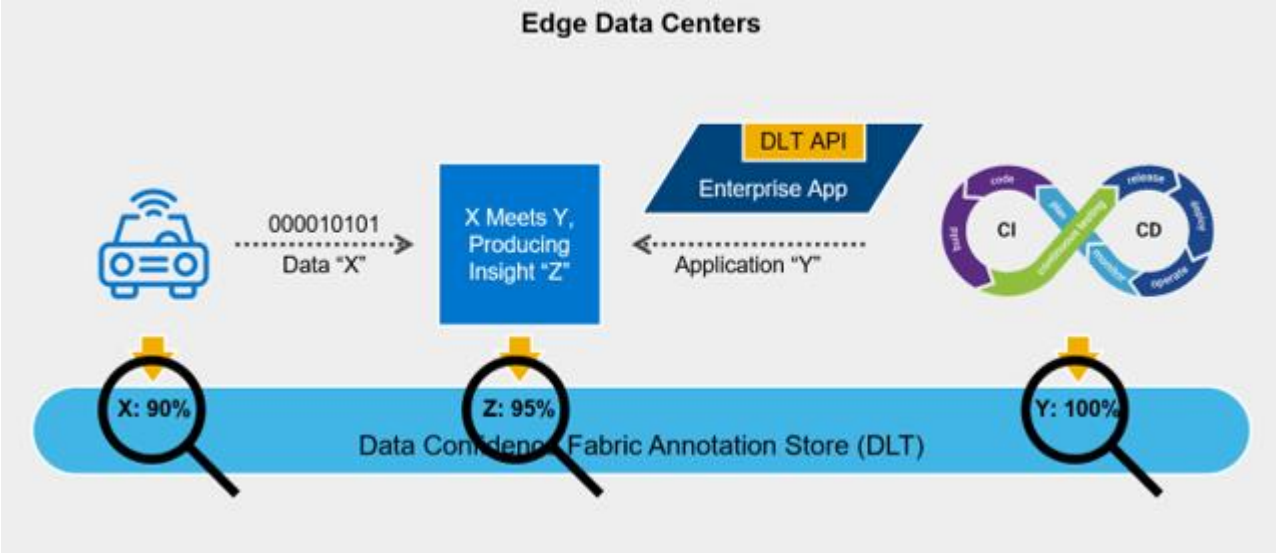


Figure 26 - Audit Enablement of Digital Edge Business Transactions

For many years enterprise companies have known that IoT sensor data has "high potential business value." Distributed ledger technology, when operating as the underlying backbone of a data confidence fabric, unlocks that potential value. Higher confidence scores translate to more valuable data. And more valuable data means more trustworthy and valuable business insights.

Conclusion

This paper has shown that DLTs increasingly provide new business opportunities. It has also shown that the difficulty of implementing a DLT is decreasing.

Removing DLT implementation roadblocks is best accomplished through community; this paper described such a community (the Hedera Governing Council) and how it levels the runway for smoother landings. This does not imply that it will be easy; there is still significant work for enterprise companies to do when deploying a DLT node.

As a result, enterprise developers can aggressively pursue business opportunities in an area that was previously out of reach: transparent and tamper-proof handling of distributed data.

And there is potentially no greater business opportunity than creating a trusted application/data bridge between corporate data centers and the far edge.

Before implementing a trusted DLT node within an enterprise, it must carefully study the governance approach and requirements of a DLT community. A thorough evaluation involves impacted business units before moving forward as a member. Education and buy-off at the executive level should be the final step in this process. This may include driving IT policy and process changes to ease the deployment of the technology.

When a trusted DLT node exists alongside and within a corporate IT infrastructure, it becomes an anchor point for decentralization. That same DLT is now accessible and available to far-edge devices—and everything in between. The fluid, trusted movement of applications and data across edge ecosystems unlocks business opportunities.

And finally, the rise in revenue and decrease in operational complexity is complemented by reduced risk. Moreover, DLTs leave an accountability trail; proof of compliance lives in the ledger, satisfying auditors and regulators.

This paper has sounded a clarion call for global enterprise companies:

- Join a DLT community.
- Implement a DLT node.
- Capture the emerging business opportunities of edge computing.

Bibliography

[i] Todd, Steve. Rock Around the Blockchain With Dell Technologies. June 2018. https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS_Todd-Rock_Around_The_Blockchain_with_Dell_Technologies.pdf
[ii] ZDNET. The enterprise shows little interest in blockchain technology: Gartner. May 2018. https://www.zdnet.com/article/enterprise-shows-little-interest-in-blockchain-technology-gartner/
[iii] Ibid.
[iv] Carson, B, Romanelli, G, Walsh, P, and Zhumaev, A. Blockchain Beyond The Hype: What Is The Strategic Business Value? June 9, 2018. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value
[v] Ibid.
[vi] Fortune Business Insights, Report FBI100072. Blockchain Market Size, Share, and COVID-19 Impact Analysis. March 2022. https://www.fortunebusinessinsights.com/industry-reports/blockchain-market-100072
[vii] Ibid.
[viii] Ibid.
[ix] Accenture. Get the Full Picture: Assessing Blockchain's Business Value.2019. https://www.accenture.com/_acnmedia/pdf-106/accenture-blockchain-value-report.pdf
[x] Ibid.
[xi] Bittman, T, Gill, B, Zimmerman, T, Friedman, T, MacDonald, N, Brown, K. Gartner – Distributed Enterprise Drives Computing to the Edge. 2022. https://www.equinix.com/resources/analyst-reports/gartner-distributed-enterprise-predictions-2022
[xii] Todd, Steve. Building the Industry's First Data Confidence Fabric. October 2019. https://www.dell.com/en-us/blog/building-the-first-data-confidence-fabric/
[xiii] Todd, Steve. Project Alvarium: The Future of Edge Data. October 2020. https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2020KS_Todd_Project_Alvarium-The_Future_of_Edge_Data.pdf
[xiv] Urbanski, Wojciech, and Rusinowicz, Karolina. Day 0 / Day 1 / Day 2: Software Lifeycle in the Cloud Age. November 2021. https://codilime.com/blog/day-0-day-1-day-2-the-software-lifecycle-in-the-cloud-age/
[xv] Accenture. Get the Full Picture: Assessing Blockchain's Business Value.2019. https://www.accenture.com/_acnmedia/pdf-106/accenture-blockchain-value-report.pdf
[xvi] Hedera.com. What Is Hedera? December 2022. https://hedera.com/learning/hedera-hashgraph/what-is-hedera-hashgraph
[xvii] Ibid.
[xviii] Ibid.
[xix] Ibid.
[xx] Ibid.
[xxi] Hedera.com. Hedera Council Overview. October 2022. https://files.hedera.com/Hedera_COUNCIL-OVERVIEW_2022_OCT.pdf
[xxii] Hedera.com. Fourth Amended and Restated Limited Liability Company Agreement of Hedera Hashgraph, LLC. April 2022. https://files.hedera.com/2022-04-06-Hedera-4th-AR-LLC-Agreement-with-exhibitsupdated-2022-10-07.pdf
[xxiii] Sylvester, Tom. General Counsel Hedera. December 2022.
[xxiv] Hedera.com. UCL Centre for Blockchain Technologies Discussion Paper. 2021. https://hedera.com/ucl-blockchain-energy
[xxv] Ibid.
[xxvi] Hedera Documentation. Node Requirements. December 2022. https://docs.hedera.com/guides/mainnet/mainnet-nodes/node-requirements
[xxvii] Popowycz, Alex. CIO Hedera. December 2022.
[xxviii] Ibid.
[xxix] Hedera.com. Hedera Global Governing Council. 2022. https://hedera.com/council
[xxx] Ibid.
[xxxixxxi] Ibid.
[xxxii] Ibid.
[xxxiii] Ibid.
[xxxiv] Hedera.com. AVC Global. A Value Chain Platform. 2022. https://hedera.com/users/avc-global
[xxxv] Ibid.
[xxxvi] Hedera.com. Everyware. Digitally Track and monitor critical or high-value assets. 2022. https://hedera.com/users/everyware

[xxxvii] Hedera.com. EVEC. Distributed Internet of Things Device Management. 2022. https://hedera.com/users/evec
[xxxviii] Hedera.com. Neuron. Enabling Autonomy in Aviation. 2022. https://hedera.com/users/neuron
[xxxix] Gillis, Alexander. Tech Target. Edge Data Center Definition. October 2020. https://www.techtarget.com/searchdatacenter/definition/edge-data-center
[xl] Prolabs.com. Edge Data Centers – Location, Speed, and Connectivity. 2022. https://www.prolabs.com/news/blog/edge-data-centers-location-speed-and-connectivity
[xli] Ibid.
[xlii] Gillis, Ibid.
[xliii] ZDNET, Ibid.
[xliv] AT&T Business. 2022 Securing the Edge. AT&T Cybersecurity Insights Report. Eleventh Edition 2022. https://cdn-cybersecurity.att.com/docs/industry-reports/cybersecurity-insights-report-eleventh-edition.pdf
[xlv] Ibid.
[xlvi] Ibid.
[xlvii] GMSA. Opportunities and Use Cases for Distributed Ledger Technology in IoT. 2018. https://www.gsma.com/iot/wp-content/uploads/2018/09/Opportunities-and-Use-Cases-for-Distributed-Ledgers-in-IoT-f.pdf