

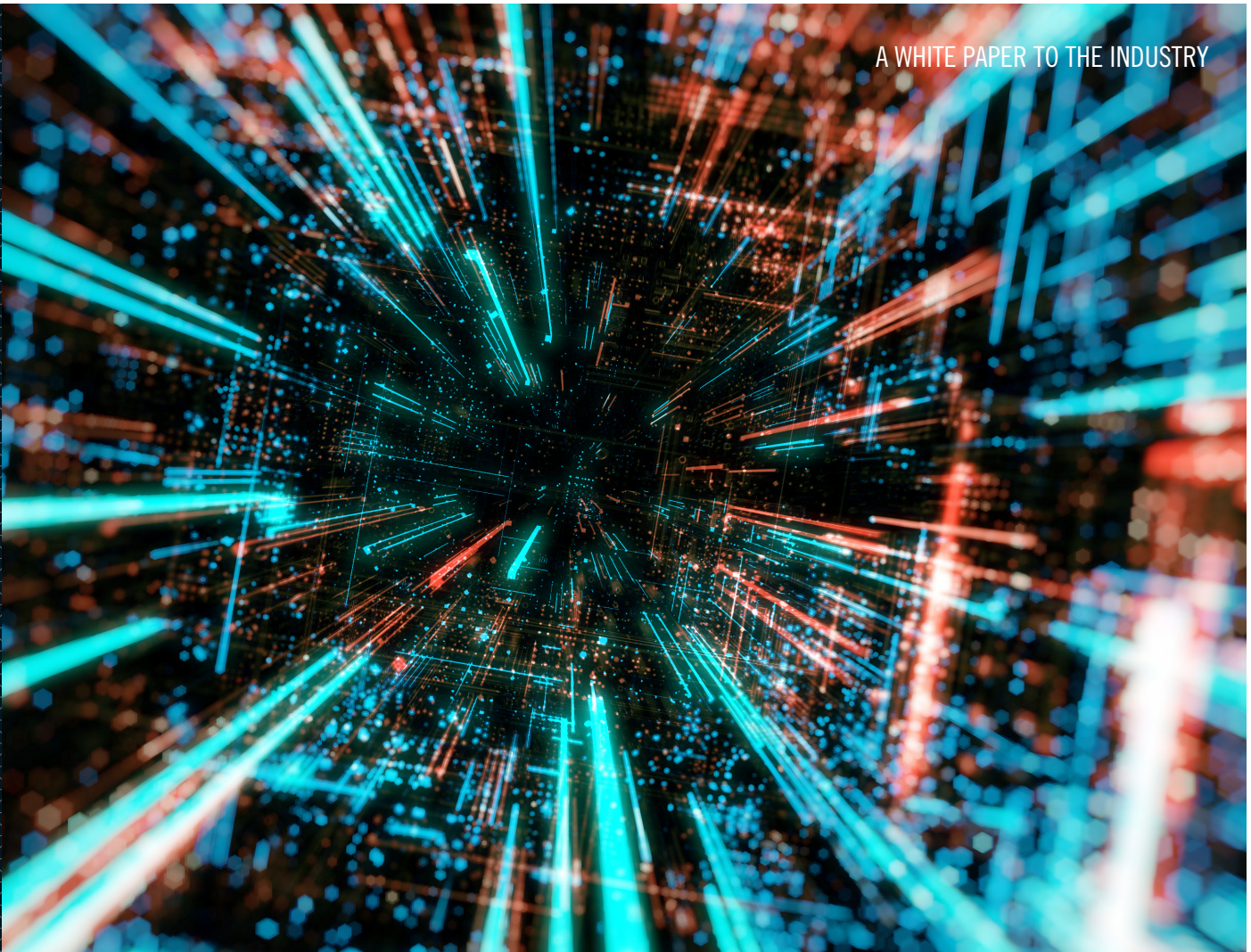


JUNE 2019

# GOVERNING DLT NETWORKS

DISTRIBUTED LEDGER TECHNOLOGY GOVERNANCE FOR PRIVATE PERMISSIONED NETWORKS

A WHITE PAPER TO THE INDUSTRY





## Contents

Executive Summary	2
Governance for Corporate or Enterprise Networks	4
Network governance model	7
Securing transparency and trust	19

---

# EXECUTIVE SUMMARY

Over the past several years, we have seen tremendous innovation in the development of distributed ledger technology (DLT), along with a dizzying number of use cases that reflect the excitement of banks and other firms to leverage this technology to transform the operations of global financial markets.

Blockchain evolution—from a primal description of Bitcoin in a 2008 white paper to the emerging enterprise version of DLT of today, with its built-in consistency, security and privacy—has been nothing less than dramatic. DLT is a powerful platform that may one day modernize corporate and enterprise operations and provide the benefits of transactional security and privacy, as well as verifiable and auditable integrity. It has significant potential to simplify our complex world of opaque siloes of information, including the ability to encode policies, rules, and business logic within the software and mathematical rules of the platform.

Early believers in DLT saw it as way to conduct transactions without banks or financial institutions, but the need for sound, controlled markets has overwhelmed that initial view. The immaturity of the technology, and its nascent ecosystem of vendors and tools, resulted in challenges to meet the expected performance, scale and cost efficiencies. But the disruptive potential of DLT continues to motivate massive investment to improve and mature those missing capabilities. It has become clear that the long-term potential hinges on effective governance to guide the growth of DLT, to meet the highest requirements of the regulated industries, and to bring a risk management perspective to migrating critical processes onto the technology as it becomes ready.


If “a financial system is only as strong as the governing practices and institutions of its participants,”<sup>1</sup> transparent policies and rules, along with accountable and responsible governance are a prerequisite.<sup>2</sup>[2] In short, the need for oversight and governance among the institutions that participate in the regulated financial industry is necessary if DLT is to continue to grow and be successfully adopted.

DTCC, working with Accenture, has developed a governance model to manage the risks and consequences of a distributed ledger landscape. Any enterprise-wide DLT initiative must have an effective governance operating model and supporting management tools. The model and tools are designed to address the responsibilities and critical functions required to operate and maintain a DLT platform. Together they create an orderly system for addressing adoption, security and regulatory compliance.

---

1 Robert E. Litan, Michael Pomerleano and Vasudevan Sundararajan, “Financial Sector Governance: The Roles of the Public and Private Sectors.” Brookings Institution Press (2002).

2 As noted in the *ISSA Report* - Distributed Ledger Technology: Principles for Industry Wide Acceptance, “Establishing Distributed Ledger technology as a widespread, accepted platform for the global financial industry and for managing records of public investments, will require policies, rules, standards, actions, processes, security, risk and operational controls, best practices, rules of conduct, and exception management. All of these requirements are critical to creating and sustaining a financial market network and each of those requirements are ultimately the responsibility of an assigned and accountable governing body...”



Conceptually, this model reflects DTCC’s core mission for nearly 50 years in clearance, settlement and risk management. We believe that existing, regulated and trusted critical infrastructure organizations—such as DTCC—are well-positioned to play a leading role in introducing governance principles and uniform standards. Developing and building on strong governance that leverages expertise and best practices for regulated industry infrastructures will help to ensure the safety and soundness of the network designed for the benefit of all participants. It also will address approaches to managing the activity, connectivity, software changes, contractual agreements and transaction finality for every participant across the entire network.

This paper is the beginning of a critical dialogue. Research, experimentation and learning about the challenges and potential for DLT-based governance processes will continue as these platforms become more widely adopted and challenges emerge. We invite a community of cross-industry leaders to join us in sharing experiences, knowledge and innovation to advance our collective capabilities. With properly implemented and operated governance, DLT can provide additional safety and soundness for the financial markets and the opportunity to enhance the “trust but verify” models for the investing public.



# GOVERNANCE FOR CORPORATE OR ENTERPRISE NETWORKS

The original Bitcoin blockchain innovation was based on a public, permissionless network of untrusted parties. Yet for most industries, particularly financial services, the business rules, performance and scale requirements and most importantly regulatory rules and policies, do not align with the public and permissionless model. This drove an evolution of the original innovation resulting in the creation of “permissioned” DLT networks – private communities with well-defined controls and known members and membership criteria.

As such, the distributed ledger platform has become a catalyst for change. Its emergence is prompting an examination of business workflows across various industries, as well as efforts to reimagine new ways of doing business built on a platform of shared, but secure and private information.

Permissioned DLT networks for corporate and enterprise contexts require the creation of rules and governance over “who” can do “what”. Building a viable DLT network for a community of cooperating but competitive corporations depends upon the realization of a common set of standards and practices. Even more important is establishing who is accountable for the network when unexpected circumstances occur, or workflows and contracts fail. While the continuing evolution of the technology may eventually provide opportunities to leverage public permissionless platforms, the focus of this document is to define a DLT governance operating model for permissioned DLT networks.

---

*Building a viable DLT network for a community of cooperating but competitive corporations depends upon the realization of a common set of standards and practices.*


---

Before we explore the DLT governance operating model, it is useful to explore the scope and context of permissioned DLT network. This includes use cases that leverage the value of DLT, using DLT to strengthen engagement with relevant industry supervisors, and a level set on customer support expectations.

## ENTERPRISE USE CASES

The number of use cases for DLT has grown exponentially as visionary leaders in a wide range of industries, from healthcare to shipping, have gained an understanding of the potential of this new technology. New business workflows are emerging that enable transactional exchanges of assets and payments to be recorded, linked and traced through their entire lifecycle; for example, tracking the lineage of a diamond, from mined stone to its use in a ring for sale in a retail store. The information about the asset—a diamond in this example—and its ownership and all transfers and payments are recorded in a distributed ledger that is shared by all parties involved in the process.

DLT eliminates traditional “data silos” which have persisted for decades, where each party has built separate systems of record with a copy of their version of information. As a result, each party engages in a series of message exchanges, file transfers, or e-mails to send their information to counterparties and other third parties. The multiple redundant exchanges and siloed data sets leads to time delays, unnecessary costs, as well as data quality issues.



The promise of DLT is to build a system once, share data and information across a community and realize tremendous efficiencies and eliminates the different data schemas, different language constructs and individual interpretation of business rules and contracts. DLT is a multi-party workflow platform that validates and stores transactions using a consistent, shared data model and contract language. However, this can only work if strong, accountable and transparent governance is in place to implement and manage the rules, practices and processes for any community of competitive parties.

### **PROACTIVE REGULATORY COMPLIANCE**

The financial industry is accountable to its' clients and regulators globally for adherence to laws and policies designed to protect the public and ensure the safety and soundness of financial markets. These regulations differ in each jurisdiction, but generally include requirements to:

- establish controls and oversight,
- comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) rules in the United States,
- protect privacy (including new General Data Protection Regulation (GDPR) rules in the European Union), and
- ensure system resiliency and controls for securing transactional records from both physical and cyber threats.

The use of DLT for financial transactions provides an opportunity to build security and resilience into the base platform, to encode business logic and regulatory requirements directly into trade contracts and to offer visibility to the regulators through their own “distributed ledger node” to enable them to have immediate and real-time access to the state of ledger transactions that they oversee. The DLT governance operating model will ensure the implementation and operation of a financial industry DLT platform adheres to those rules and regulations in a manner that benefits all members of the community.

Other industries, including healthcare and the global supply chains for the food industry, have similar opportunities to meet the needs of their regulatory supervisors.

### **SUPPORT AND ISSUE RESOLUTION**

For any system, including a DLT network, the most fundamental governance requirement is that there is an accountable party to address unforeseen problems. Examples include code defects, unforeseen behaviors from participants, unintended behaviors from smart contracts and unexpected real-world events. While the most ambitious future promise of the technology suggests that governance can be pre-programmed into the ledger code, a realistic view of the current state of technology suggests that neither technology maturity, nor programmatic quality have reached that capability (arguably no technology has ever reached that state). An equally realistic view of the current legal and regulatory dialogues concerning DLT across global regulatory jurisdictions also suggests that ensuring smart contract code is kept up to date with changing regulations and policies will be a challenge.

Therefore, a DLT governance operating model must include administrative tools to react to idiosyncratic events to serve as a circuit-breaker in the system, transparently and accountably modify the state of the ledger when errors or adverse systemic events occur, improve the business logic and rules if there are flaws or conditions change, and adjust the operating model itself as the needs of the community evolve.



## THE DLT NETWORK OPERATING MODEL

The process for creating a value added network between business partners has followed a consistent pattern over the past few decades. The responsibilities for delivering certain capabilities has changed, with the emergence of service providers, cloud vendors and outsourcing, but the approach has remained consistent. Our DLT network operating model aligns to existing frameworks and is reliant on three key roles:

- **THE GOVERNING ENTITY** represents and is accountable to the interests of the entirety of the network as a priority, with an expectation of complete integrity and continuous reliable operation. The governing entity owns responsibility and accountability for creating the policies, rules of conduct, operating procedures, controls, standards and so on, to establish a shared platform that benefits all members fairly.
- **THE NETWORK OPERATOR** is charged with operating the DLT network fairly and objectively for the benefit of all members in accordance with the policies and procedures of the governing entity. This role ensures operational safety and soundness of the network.
- **THE MEMBERS OF THE NETWORK COMMUNITY** includes direct and indirect network participants and other third parties with interests in the network. Examples include transactional participants, data providers and consumers, regulators, industry associations, software vendors, and so on. Each member of the network has a primary responsibility to their own shareholders and owners.

For the remainder of this white paper, we will focus on a generalized DLT governance operating model. Governance models for enterprise IT, as well as for industry consortiums have existed for decades, so many of the components and functions will be familiar to the reader. We have highlighted discussion of the functions and considerations that are significantly different for DLT networks.

# NETWORK GOVERNANCE MODEL

DTCC, working with Accenture, has developed a DLT governance operating model, as well as an initial set of management tools to manage the rules, policies, standards, membership, processes and controls, and to establish practices for addressing exceptions and other issues that may arise on a DLT platform (see Figure 1).

As illustrated, our model, DLT-GM, is composed of eight high-level functional areas.

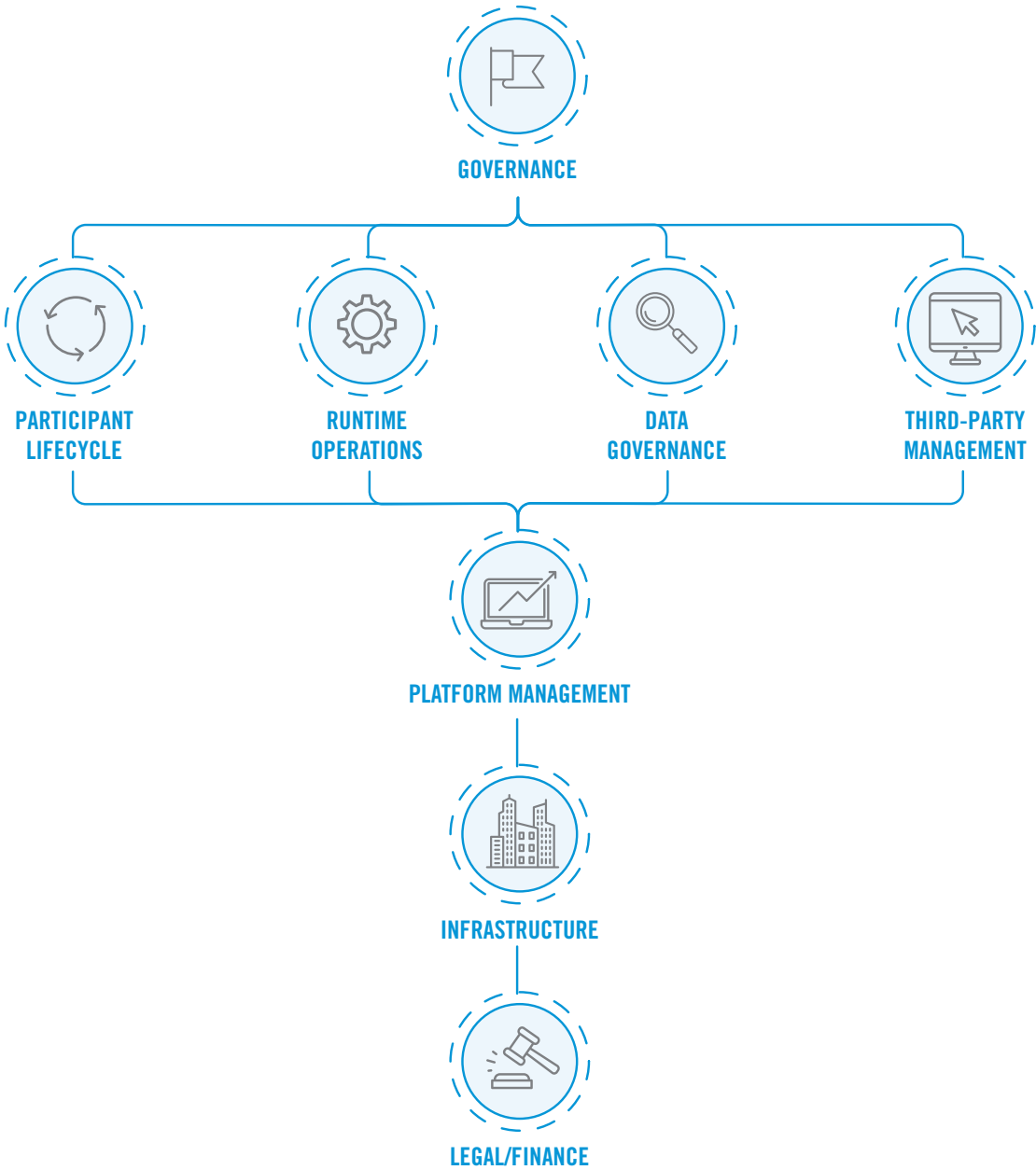


Figure 1. DLT Governance Operating Model (DLT-GM)



## FUNCTIONALITIES AND CONSIDERATIONS

Let us explore each functional area of the DLT-GM, highlighting the key considerations required for DLT platforms.

### 1. Administration

This functional layer has overall responsibility and accountability for the oversight and strategic decision-making for the DLT network community. There are four distinct advisory bodies which together provide the highest level of oversight: Steering Committee, Functional Working Group, Technical Working Group and Change Management. These advisory bodies are long-lived and critical during the start-up phase of a DLT network as they approve the initial business functions and technical designs. They are also important for maintaining the value of the network as business and regulatory requirements change and as technology advances.

<b>STEERING COMMITTEE</b>	<ul style="list-style-type: none"><li>■ <b>Responsible for the overall direction of the platform</b>, including the scope of functionality, the solution it provides, and risk/control oversight</li><li>■ <b>Includes a representative set of all network participants</b> to ensure the network provides benefits for all (or as many as possible) of the network members</li></ul>
<b>FUNCTIONAL WORKING GROUP</b>	<ul style="list-style-type: none"><li>■ <b>Governs the business functions</b> (business process, flows, regulatory compliance, data models) built into the platform and establishes policies for ongoing maintenance</li><li>■ <b>Includes all key stakeholders</b></li></ul>
<b>TECHNICAL WORKING GROUP</b>	<ul style="list-style-type: none"><li>■ <b>Provides oversight of the technical design and architecture decisions</b> for the DLT platform, including DLT designs for security, confidentiality and resiliency</li><li>■ <b>Responsible for the review of the critical usability elements</b> such as technology components, languages, standards and client interface models</li><li>■ <b>Definition of non-functional requirements</b>, such as for scale and performance, as well as operating parameters (e.g., period of operation, time of day for global networks, etc.)</li></ul>
<b>CHANGE MANAGEMENT</b>	<ul style="list-style-type: none"><li>■ <b>Responsible for the strategy and oversight</b> of network-wide change management (business flows, contract rules, network standards, etc.)</li><li>■ <b>Manages the strategy for implementation, versioning of changes and ensuring back-out and contingency plans</b> are tested and ready to be used</li></ul>

Together, these advisory bodies form the essential oversight of the network and must operate with the interests of the whole network as a priority, without any conflicts of interest. The remainder of the governance operating model includes the service responsibilities of a network operator, which may be specifically owned or outsourced by the governing body in line with the business case.

**A Note on Interoperability**

The evolution of DLT and the wide adoption across industries and across different market segments is resulting in many different ledgers networks, but the ultimate promise of DLT can only be realized when all ledger networks can seamlessly interoperate. But at this stage in the DLT’s maturity, there are very limited real-world instances of interoperating ledgers. In this DLT governance operating model, business requirements for interoperability and associated cross-ledger governance issues have not yet been considered. Interoperability involves standards, rules of engagement, decisions on trust and custody business models and the technical requirements to implement those decisions. It includes integration and mapping of data models, reference data and users. It also involves interaction between the governance models and governing entities of the interoperating DLT networks. As a result, it is expected that interoperability will be within the purview of the Steering Committee and associated working groups.

**2. Participant Lifecycle**

The Participant Lifecycle includes the management and operations of every aspect of onboarding a new network member, all the interactions during that member’s participation in the network and the steps to off-board a member.

Earlier, we suggested that most industries and the enterprises within them would consider a “permissioned” model for DLT with known participants. Onboarding new members into the DLT network and enabling them to perform their expected role in the network, is the starting point of the Participant Lifecycle.

A membership request initiates the onboarding process flow (see Figure 2).

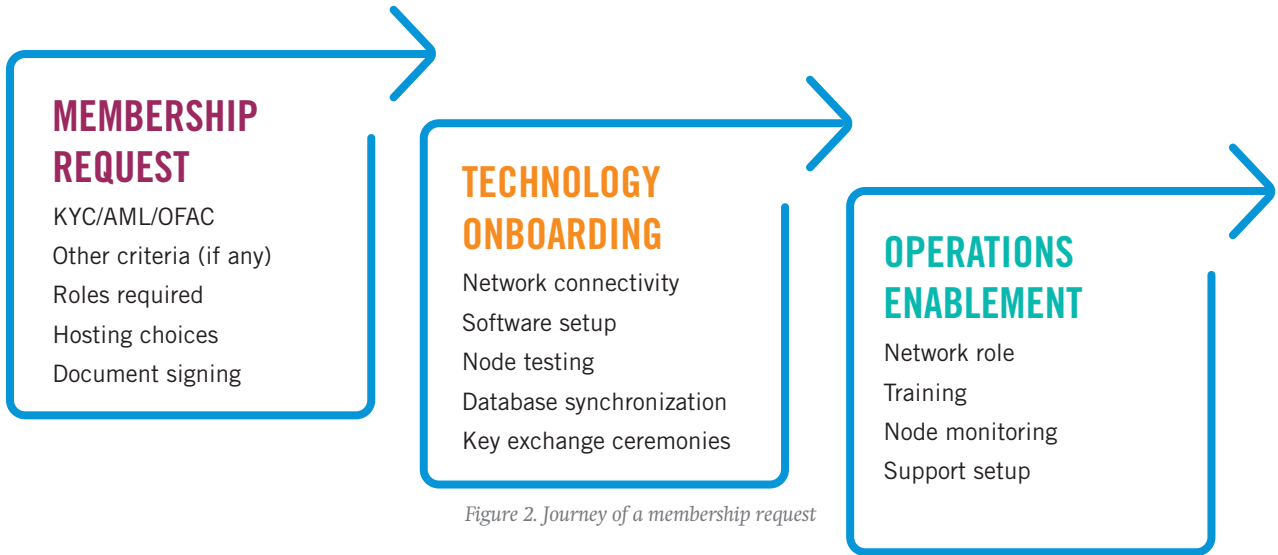


Figure 2. Journey of a membership request

Generally, the onboarding function for a member will have several necessary workstreams:

- Assessment of participant eligibility to meet membership criteria, including KYC/ AML review.
- Document exchange, review and signing, which includes all legal, regulatory and business agreements that must be approved and maintained.
- Business process training for participant's operations team.
- Technical training and information for participant's IT/tech team.
- Building participants DLT network connectivity which will differ based on:
  - If the participant is taking a node on the network (and hosting arrangements).
  - If the participant is outsourcing network node management.
  - If the participant is using a service provider to provide node interface.
  - Note: each of the above scenarios requires different connectivity, software and testing models.
- Establishing the participant's identification, users, entitlements and encryption key exchanges.

If a participant is taking a node on the network, they will have additional steps associated with:

- Participant network node setup: node host registration, DLT software download and installation, software checkout, node configuration and testing and node enablement.
- Participant account setup: account registration, encryption key exchange, privacy enablement.
- Ledger sync: client reference data refresh, ledger history synchronization.
- Participant network and node operations and monitoring.

Once a firm has been on-boarded and established as a network member, there will be various ongoing maintenance functions, including: ongoing network management, functional, technical and vendor updates which involve change notifications and implementations, resiliency testing and other typical system maintenance functions. Additionally, there will be ongoing communications concerning network status, changes, upcoming test cycles, and so on.

The final step of any participant lifecycle is off-boarding and removing all access and network connectivity. This may entail addressing the duration where the participant has been off-boarded and is not active but is still registered in live transactions on the DLT platform, or in transactions archived for data retention purposes.

## CONSIDERATIONS FOR DLT NETWORKS

The description of participant onboarding may seem like traditional client or account management processes, but there is a fundamental difference for a DLT network. A participant may elect to take a network node and every network node is part of a shared, distributed database. Depending on the configuration of the DLT platform, nodes may have a direct influence over transaction processing through consensus rights and/or transaction validation votes (the ability to approve or reject any transaction). In fact, nodes become part of the database replication protocol, the resiliency scheme and the encryption and security scheme. As a result, every node, even those in participant hosted facilities, is governed by and must adhere to the rules of the network operating entity.

There is a linkage in the Participant Lifecycle function to two other business process and related systems:

- Client Relationship Management (CRM)—typically for managing all interactions with a client
- Billing—depending on business relationship

While these are outside the scope of this white paper, they are noted for completeness, as they may be relevant depending on the industry and business use-case.

### 3. Runtime Operations

Runtime Operations covers the day-to-day execution of the DLT. In this area are the major functions focused on DLT runbook operations—monitoring, reporting, support, change and release management. The governing entity for the DLT network has responsibility for ensuring the continuous operation and safety and soundness of the network (even if the governing entity has outsourced the actual operation of the network, the governing entity still owns responsibility). As a result, each of the Runtime Operations functional areas take on a new meaning and a much larger scope and sphere of responsibility in a DLT ecosystem, as compared to a traditional model of single enterprise responsibility. As an example, in a DLT network, if a member's node becomes inoperable, or potentially a source of a Distributed Denial-of-Service (DDoS) attack, the escalation action taken by the operating entity may be to shut down and remove the inoperable node of a network participant.

**RUNBOOK OPERATIONS:** Generally, DLT networks are implemented to operate continuously 24/7/365, so the traditional model of daily application starts and stops and subsequent end-of-day processing is not relevant. Additionally, financial lifecycle processing, which was traditionally driven through batch processing models (for example, dividend payments on a specific date), can now be written as a business rule within a transaction's smart contract code (so the payment can be executed as a transaction when a triggering event occurs, such as a date change). However, there will likely be various housekeeping activities, including daily, weekly, or monthly reporting, database cleaning, DLT pruning (the archiving of older ledger blocks out of the online ledger to improve performance) that will need to be executed as a responsibility of the network operating entity.

**MONITORING:** A primary daily, real-time, responsibility of an operating entity will be to monitor the health of the DLT network. As a decentralized/distributed database, the health of the network will directly impact the ability of network members to do business activities (for example, complete financial transactions). Network monitoring includes: processing exceptions on any node (for example, from errors in smart contract coding), security monitoring for unusual and unexpected behavior, network monitoring for unknown network traffic, network activity indicative of denial-of-service attack, or performance degradation (for example, consensus and/or validation protocol response delays). Network nodes that are newly connected to the network will start a “hydration process” to synchronize their node history to the active ledger, a process that will impact performance, so this activity must be also monitored closely for abuse. The monitoring operation is responsible for tracking healthy, active nodes and escalating an action to address disabled nodes.

The operating entity should have mechanisms to quarantine nodes “behaving badly” and remove them and the related validation and consensus responsibilities, from the main part of the network.

**SUPPORT:** The support function must be able to address the full range of online community needs, from node onboarding support, to basic participant connectivity problems, to suspending and fixing errant smart contract

code. Multiple channels should be available (direct dial, email, online chat) and as much on-line help and frequently asked questions content as possible to enable the network to scale.

A fully staffed support model of client focused Level 1 to 3 teams is the base expectation for any industry-level network. DLT is a real-time platform and the support model must align with client and industry expectations. Establishing escalation thresholds and timing are critical to both the client experience as well as potentially the health of the network itself.

The Exception Management process within the support function is required to support full root-cause analysis, as well as the ability to fix things that are broken, in a manner that aligns with the design of the DLT and maintains the integrity of the ledger. Administrators must be able to stop or suspend smart contracts, change existing smart contracts (potentially through exiting a faulty contract and invoking a new contract), change reference data in a transparent and accountable manner and have the necessary tools to fix things when they are broken.

**CHANGE AND RELEASE MANAGEMENT:** As previously mentioned, the Change Management function is responsible for the strategy and oversight of network-wide change management. This operations function provides the participant-facing management of the process itself, in alignment with the strategy and the specifics of the DLT platform. Here we have another aspect of DLT that is fundamentally different from traditional siloed applications. The traditional model enabled individual firms to change their entire application stack, as the only interface from a client or peer firm was a message or a file exchange. With the DLT platform, every firm should have an identical copy of the node processing environment—the same version of the validation engine, the same smart contract rules and interpretation and the same core processing engine.

DLT platforms inherently exchange and execute “code,” so, in concept, a transaction and contract to update node software can be implemented in many DLT models through

## HOW DTCC IS BUILDING CAPABILITIES TO SUPPORT THE GOVERNANCE MODEL

By way of example, DTCC has leveraged open source code from the Hyperledger Explorer project, to develop a governance tool which provides administrative, monitoring and troubleshooting or investigative tools as an integrated package. Known as DLT AdMon, it provides a view into any node’s ledger activity and performance, enabling remote query and view of: blocks, transactions, smart contracts, entitlements, network information data (name, status, list of nodes) and any other relevant information stored in the ledger. A dashboard provides an overall health check for the DLT in terms of nodes connected, their status, performance or throughput and the smart contracts being invoked. This provides DTCC, as the operating entity for this DLT network, the ability to understand the performance of the DLT and capture issues before they impact network participants.

DTCC has also implemented an administrative framework, which can be leveraged by our support team to stop or restart any network nodes, pause the entire DLT network (stopping blockchain updates), monitor the performance of smart contracts and pause them if issues are identified. This framework provides a real-time ability to manage the network and cancel the processing of a transaction or block if it is causing the system to hang. By suspending a non-performant smart contract, we manage performance of the DLT and reduce the noise from incorrect processing (see Figure 3).



automation by scheduling coordinated deployments to a common time and date. But, the real world implications make the change process more complex. Every participant that has adopted a network node has also likely integrated that version of the node into their own processing environment and is using the provided API's to integrate with their systems. As a result, all changes need to be communicated, coordinated and tested with network participants in a manner that does not impact production transactions. Obviously, it is critical that all parties to a contract interpret and process the contract in the exact same way on every network node, so maintaining compatibility and consistent and synchronized change deployments across the network is a key aspect of change governance and operation. Procedures for emergency changes, that are not part of a planned change process but are necessary to maintain network integrity and operation, must also be established as a key governance responsibility.

Even with the critical need for consistency, a strategy for a large network with multiple validators (where it is impractical to expect hundreds or thousands of nodes to synchronize software upgrades simultaneously) may need to consider methods for rolling change deployments and potential support for multiple versions simultaneously—which implies further provisions to identify inconsistent contract processing.

#### 4. Data governance

At its core, DLT is an enhanced database that integrates data as well as the business rules associated with the data, so the emergent models of Data Governance become a critical, core competency for a DLT network. DLT introduces several aspects that are different from how the industry operates today:

- Participant entitlement and confidentiality models—nodes in a corporate / enterprise DLT network must provide a construct to only contain the data that the participant running the node has legitimate access; encryption alone is insufficient no matter how 'advanced'. The entitlement and confidentiality models including both data segregation and encryption are the main structure protecting and limiting access to transactional data. The public crypto-networks (for example, Bitcoin and Ethereum) and some private DLT networks enable all nodes to validate transactions, but many other DLT platform implementations limit validation to the parties to a transaction and all other parties will not have access. The entitlement and confidentiality models manage this.
- Reference data is critical for transaction processing, leveraged by smart contracts, which are triggered by market events, holiday calendars or corporate actions. Controls need to be in place to prevent unauthorized changes to this critical data.

### CONSIDERATIONS FOR DLT NETWORKS

Every functional aspect of DLT Network Runtime operations has implications for network node participants that are fundamentally different from traditional models. Each participant's DLT network node, even if hosted within a participant-controlled facility, is part of the "fabric" of the entire network and is governed and operated according to the policies, rules and practices of the network. The network operating entity monitors each node, it can be stopped and quarantined if deemed a threat to the network. If a participant's node is down and that participant is also involved in a transaction, the network must have rules to allow processing to continue and be resilient. If a participant's node has not been updated and a new, smart contract executes that is not compatible with that participant's node, the network must have rules to enable processing to continue and be resilient. The change of control from individual ownership to network ownership, with a governing body and a network operator providing oversight and management, is a massive change from current practice.

- Distribution of third-party data and intellectual property (IP) is a critical consideration for DLT networks. As with non-DLT networks, appropriate data and IP licensing rights must be obtained and maintained. Vendors may need to reconsider traditional models that become prohibitively expensive on distributed networks.
- Encryption key management is essentially the gatekeeper for DLT solutions and must be uniquely tied to secure customer/client reference data. Smart contracts are combinations of data, business rules and code. Establishing the right standards and review models for smart contracts and ensuring they are reviewed and scanned for compliance is an essential governance practice.

## 5. Third party management

As noted in the Governance section, most of the operating portions of the governance model are the operating services that must be provided for any network and these may be outsourced. Many of the members of the network are likely to recruit service providers and/or cloud hosting vendors to provide a managed node service on their behalf. It is also likely that any network will include reference data and other third-party data providers. Different networks may accommodate only third parties that provide information to the network, or that can view and monitor information on the network. A DLT network may coordinate with industry associations and other groups that provide standards and operating practices for the specific business model. Finally most DLT will be provided by open source communities and third-party vendors that will be constantly upgrading and modifying their platforms. All these relationships must be coordinated, managed and governed to ensure they are aligned with the best interests of the DLT network.

The third-party management function is assigned to specifically coordinate every significant outside party interest in the DLT network. At the highest level, the following areas must be considered:

- **OPERATING UTILITY OUTSOURCING**—which encompasses any aspect of the Governance Model service functions that are outsourced and must ultimately answer to the Governance steering committee.
- **NETWORK NODE SERVICE PROVIDERS**—including full platform service providers, which provide the full application service to DLT network participants, as well as cloud and hosting service providers. All these firms are likely to be involved in hosting nodes and become part of the critical infrastructure of the DLT network for software changes, testing and so on.

## CONSIDERATIONS FOR DLT NETWORKS

Industry associations and standards organizations already exist and contribute in a significant way to data governance, including standards, taxonomies, conventions and business rules for specific industries. For example, the International Swaps and Derivatives Association (ISDA) stewards the standards for OTC Derivative contracts and has created a new model, known as Common Domain Model (CDM) for standards of data and processing that can be applied to emerging DLT platforms. The real value of DLT networks is the ability to align to industry approved standards and distribute an application, through smart contract code, of the exact standard data schema and the exact standard business rule, to every network node as soon as a change is approved. Participant internal systems will need to align with this new model, through the adoption of API-type interfaces. The current model of standard adoption, which has been in place for many decades, can then be retired.



- **DLT PLATFORM VENDORS**—the provider of the underlying DLT platform. This is likely to be one single firm, but a critical vendor of the software providing the DLT and it will enhance its platform as well as providing the necessary support and critical software fixes.

Regulators and industry associations may impose requirements, standards and other practices on a DLT network, which requires significant communication and coordinated testing.

## 6. Platform management

The Platform Management function is the DLT ecosystem version of the traditional “application development” model, adjusted to support the multiple layers of DLT. Platform strategy, projects to implement the strategy, code development and change-release pipelines and project management office functions all exist in a similar manner to the traditional model. There are many additional considerations:

- DLT vendors will enhance and modify their platforms. The newer languages and decentralized and distributed models require new testing plans and new security or malware code scanning tools.
- A unique attribute of DLT is the “blending” of database, business data, business data rules and business workflow into the vendor provided product. Traditional database vendors provide software and the client or customer adds their own data schema, data rules and processing. DLT vendors typically bundle all of those into the DLT packaged solution, that must be maintained and upgraded. Thus DLT vendor risk, is one of the key risks that the governing function must manage.

## CONSIDERATIONS FOR DLT NETWORKS

In traditional applications, business flows and message standards are a core shared element and the building blocks for interactions between systems. However those workflows and standards are built and maintained individually by each counterparty in its own databases and systems. DLT platforms have the potential to eventually replace a large portion of traditional in-house, custom applications and databases. Therefore, ensuring full transparency into architecture and design decisions as well as alignment with member expectations is critical to the success of the network. This is especially relevant for satisfying critical technical requirements, such as security, privacy, resiliency and other non-functional requirements for all stakeholders. As such, for DLT solutions, complete technical oversight is a key governance component.

An important additional source of change, which is enabled by the DLT ecosystem, is the opportunity for individual parties to collaborate on new, smart contract code. Many DLT platforms support this through new, or updated, contract libraries. This DLT capability should be integrated into the change governance process for testing, malware scanning, prioritization and scheduled release management.

This capability is a key aspect of the value case for DLT as certain regulatory or other types of change can be adopted centrally and consistently on behalf of the participant network. Instead of each participant needing to understand, design, code, test and review regulatory change independently, the operator of the DLT platform could do it once for all and engage in more efficient industry-wide testing with regulators.

- There are multiple technical underpinnings of every DLT model, including: consensus models, encryption models, data distribution, validation, smart contract language execution engines, privacy channels, and so on. Every one of these aspects has a significant impact on the network operation and performance and scale characteristics. As DLT vendors make changes, the impact on processing must be extensively tested.
- Every transaction may be a set of customized code that is executed individually at runtime. This is different from the traditional model of a single set of extensively tested code wherein only data elements are changeable at runtime. DLT enables the business rules themselves to be changeable for every transaction and to respond to external events, along with changeable data elements. As contract complexity increases, the testing scenarios may become unlimited. Contract analysts should define business requirements and business process models to implement rules enforcement within the contract language and testing should conduct extensive validation.
- The implementation of business processing on DLT will involve decisions concerning business rules and logic that will be implemented “on-chain,” meaning in the smart contract and “off-chain,” meaning outside the business validation rules and processing of the DLT. Those decisions may be based on privacy considerations, complexity and what can be digitized considerations, as well DLT performance considerations. Those are very significant governance decisions and must be escalated to the Technical Working Group and designed appropriately.
- Participants on the network may construct their own contracts. Code library models, code logic validation, security malware scanning and other tools should be implemented to ensure the integrity of the network cannot be compromised.
- For the foreseeable future, DLT platforms will require extensive integration with traditional systems, to connect with reference data sets, to connect with enterprise database systems and to connect with other reporting and monitoring systems. The testing environment needs to be evaluated well to enable comprehensive testing for changes to dependent systems.
- It must also be noted that the next five to 10 years will require the management of vendor risk and subject matter expertise risk. Most DLT vendors are small and have small customer bases and limited revenue models. The possibility of vendor failure is high, so committing long-lived ledgers of important transactional data must include active code escrow ensuring current versions are up-to-date and plans to develop platform expertise in the event of the network operator taking on development and core technical support responsibilities.
- DLT security expertise must be engaged and central to the Platform Management team. DLT models are built on a model of the current state of encryption technology. Security and encryption models are continuing to evolve and are likely to be impacted by ongoing developments in quantum computing. There is a need for forward security models to be considered, where an existing immutable ledger must be upgraded to a new encryption model.

## CONSIDERATIONS FOR DLT NETWORKS

The model described in this section is central to the changes brought by DLT. Every participant in a DLT network, even those adopting a node, is essentially a client of a shared business application for critical transactions, including database and processing rules, across the full network of participants in a Software-as-a-Service model.



## 7. Infrastructure

The Infrastructure component of the governance operating model addresses oversight of the core network management functions. This typically involves working with third-party providers but defines ownership responsibility for ongoing infrastructure operations. The key word is ongoing, as the traditional idea of “daily” activity is not relevant in a real-time DLT model. Ownership involves the support of the Runtime Operations function and the development and testing activities of the App Platform function. These centralized responsibilities can be separated as follows:

- **NETWORK MANAGEMENT:** The network operations and monitoring itself, the network routing models and security defenses, adding or updating nodes, testing nodes, removing nodes, performance and bottlenecks, network issues, and so on.
- **CYBERSECURITY OPERATIONS:** Security operations includes defensive monitoring, reacting, responding, proactive testing, and so on. Encryption key administration and management for the network is here. Monitoring for anomalous smart contract behavior and network activity is included. This function includes active escalations to the network participants of current security status and any incidents or elevated threat levels.
- **ENVIRONMENT MANAGEMENT:** Operational management for all production, test and development environments and connectivity across the network.
- **RESILIENCY OR BUSINESS CONTINUITY:** Responsibility for creating strategies for resiliency testing and business continuity testing, managing, organizing and testing business continuity plans internally, coordinating with Participant Lifecycle and Support teams to organize and schedule testing and executing network wide testing.
- **DLT NETWORK COMPLIANCE OR RISK:** This function creates strategies for validating network risks and ensuring compliance with relevant regulatory requirements (for example, KYC, AML, Reg. SCI for the financial industry), provides control and testing validation and documentation for review and supports third-party control reviews.

### CONSIDERATIONS FOR DLT NETWORKS

In the era of cloud infrastructure, it is likely that many participants will outsource node hosting and management, something for which the Governance Model and the network operator must be prepared. There are implications for the technology stack and the public and private cloud models that can support it. There are also implications for the entitlement and DevOps models within a specific infrastructure, and around ensuring the network operator can properly administer misbehaving nodes.


## 8. Legal and Finance

The final component of the governance model is the functional areas of Legal and Finance, and most of the considerations here are specifically for the DLT network.

Several significant legal risks should be addressed and mitigated:

- **VENDOR AND LICENSING RISK:** As mentioned earlier, most current DLT networks are small implementations from new vendors. Multiple rights ownership and licensing models are being created to charge for network nodes, contract libraries and individual ledger transactions that will need to evolve as networks, transaction volume and ledger sizes scale higher. Third parties that provide data are also evolving licensing models as DLT networks distribute reference data that was traditionally licensed to individual firms.



- 
- **PATENT RISK:** Many business and technical patents have been filed in recent years associated with DLT models. While many of the those filing the patents have suggested that these are “defensive patents,” the possibility of lawsuit and injunctive relief, as well as the possibility of different treatments of legal ownership in different jurisdictions, is a risk for the DLT ecosystem. It is important to get strong indemnity from vendors with appropriate insurance.
  - **OPEN SOURCE RISK:** Many DLT implementations leverage open source code, so it is important to implement controls around open source and understand the obligations of the relevant licenses.
  - Finally, many DLT models cross global borders, where tax models and associated reporting have yet to be fully discussed. All these issues suggest a strong need for ongoing legal engagement at the outset.

The financial side is dependent on the specific business model for the DLT. This aspect addresses the funding model of the DLT network itself, including the expense side of implementing, operating and governing the network and the revenue model from billing DLT network participants and ensuring proper collection of vendor and third-party licensing fees—which may be transactional and built into the smart contract models.

---

# SECURING TRANSPARENCY AND TRUST

Distributed Ledger Technology promises a new model for recording multi-party transactions with transparency, security, privacy and self-enforced integrity, all built in. The platform brings together many different technology capabilities to make this happen, as if by magic. But the real-world model of how systems actually run is not magic. It involves people designing models, writing code and implementing systems. In today's world, all public and private, DLT implementations trust people to design it correctly, to write the correct code, to implement the infrastructure and, above all, to do the right thing. Organized governance and operating models that are built for the unconflicted benefit of the full community, with rules of conduct, best practices, transparent accountability and exception management, are the real-world answers to making these systems work as intended. Global policies, regulations and law, intended to ensure the safety and soundness of processing systems, define the operating principles for those models.

This white paper explores the generalized governance model that DTCC is implementing for its TIW-DDL system, a real-world implementation of DLT with the participation of the financial industry. DTCC has nearly 50 years of experience as an industry-owned and governed utility, focused on the governance of securities clearance and settlement and risk management for the global capital markets. Together with Accenture, we believe we have built a DLT governance and operating model that provides unconditional benefits to the entire participating community and enables all our members to operate on a level playing field. And it is not a standalone solution. We believe this model can be leveraged for the benefit of other DLT network use cases and look forward to developing its scope and capabilities in the years to come.

---

*Organized governance and operating models that are built for the unconflicted benefit of the full community, with rules of conduct, best practices, transparent accountability and exception management, are the real-world answers to making these systems work as intended.*

---

## CONTACTS

**Robert Palatnick**, Chief Technology Officer

[rpalatnick@dtcc.com](mailto:rpalatnick@dtcc.com)

**David Treat**, Managing Director

[david.b.treat@accenture.com](mailto:david.b.treat@accenture.com)

**Wynn Davies**, Managing Director

[wynn.davies@accenture.com](mailto:wynn.davies@accenture.com)

**Questions or comments** about this white paper can be addressed to your DTCC Relationship Manager at [DTCCClientCommunications@dtcc.com](mailto:DTCCClientCommunications@dtcc.com)

## ABOUT DTCC

*DTCC is a premier, global, financial markets infrastructure provider, owned and governed by the financial industry, with nearly 50 years of experience providing governance, risk management and operational efficiencies to regulated financial markets around the globe. DTCC has established processes, standards and rules, supported by technology platforms and enforced by control models to promote the safety and soundness of an efficient and accountable financial markets industry. DTCC provides governance services that address the requirements of public and private sector supervisors and regulators in the U.S., Europe (and U.K. post-Brexit) and in the major markets of AsiaPacific.*

## ABOUT ACCENTURE

*Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. A key part of the Accenture blockchain practice is to apply its' independence, expertise and technical capabilities to help operate DLT based ecosystems, applying governance models, performing key operational functions and continuously modernizing the technical platforms. 14889\_PS072019*