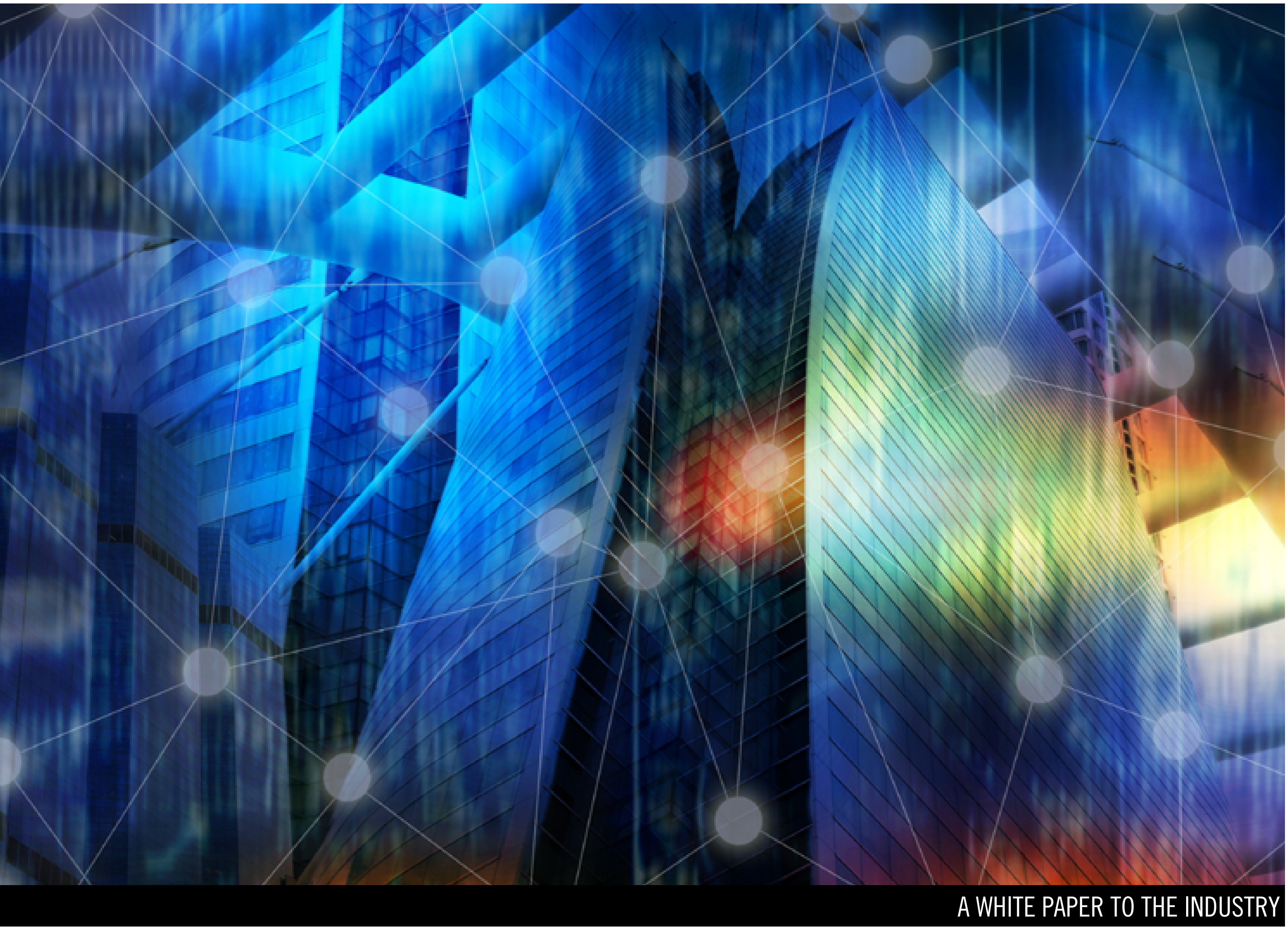
DTCC

FEBRUARY 2020

SECURITY OF DLT NETWORKS

A Distributed Ledger Technology Security Framework for the Financial Services Industry



A WHITE PAPER TO THE INDUSTRY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The distributed ledger technology (DLT) landscape is filled with fragmentary standards and guidance with respect to DLT-specific security considerations. Although numerous standard setting bodies have published industry-leading security standards and guidance for traditional IT environments the adoption of DLT across the financial services industry remains in its infancy. Organizations are still in the process of navigating the DLT landscape in order to develop standards and guidance for DLT-specific security.

DLT provides a variety of value propositions for the financial industry. These include strengthened identity measures, improvements in information preservation and data integrity, processing efficiencies, increased operational capacity, and compliance effectiveness. Consequently, these potential value enhancements come with a variety of security risks.

To address these DLT security risks, the existing IT organizations, along with a plethora of new organizations, are publishing various guides, standards, and best practices to assist with DLT security. This paper illustrates the main areas that these guides are addressing, and highlights where there may be further opportunity in addressing DLT-specific security risks.

To expand on the possible shortcomings of traditional IT security frameworks as applied to DLT, this paper evaluates the intersection between traditional and DLT-specific security considerations. It is evident that many security principles overlap in both traditional and DLT environments; however, gaps in addressing DLT-specific security risks are also widely apparent. To demonstrate the proliferation of these gaps, this paper applies an existing cybersecurity assessment to a DLT-environment. As demonstrated by the standard assessment considerations, there are a multitude of special and additional factors to consider when operating in a DLT environment.

Lastly, this paper explains the importance of standards. Standards allow for DLT interoperability, agreed-upon terminology, streamlined governance, and stronger digital identity management. The paper concludes with a call to action, inviting all financial industry stakeholders to contribute to the best practices that will eventually develop into an agreed-upon, industry-wide DLT security framework that may be used by the financial services sector and leveraged by other industry sectors. To establish a comprehensive and standardized DLT security approach requires collaboration from professional organizations, the financial services sector, and its regulators.

FINANCIAL SERVICES DLT

DLT introduces a multitude of value propositions for the financial sector. The core value propositions include strengthened identity measures, technical components for enhanced information preservation and maintenance of data integrity, processing efficiencies, operational capacity and scalability, and compliance effectiveness.
This white paper highlights and expands on each of these value propositions and how they can be achieved through the DLT adoption. In order for the industry to realize these value propositions, the industry must develop a comprehensive and standardized approach to DLT security to ensure the confidentiality, integrity, and availability of an organization's DLT operations. However, in addition to providing new value to the financial services industry, DLT presents unique risk profiles and security exposures that must be addressed using both traditional and non-traditional methods.

IDENTITY MEASURES

Identity and access management (IAM) encompasses the processes and technologies used by an organization to authenticate and authorize an individual to access systems or services. Traditional IAM processes and technologies are vulnerable to loss, theft, and fraud due to the storage of personal information on centralized servers, which become primary targets for hackers. Since the inception and adoption of DLT networks, multiple organizations and government agencies experienced attacks leading to the theft of customer personal identification information. DLT provides the opportunity to strengthen IAM processes through the application of cryptography and decentralization. This strategy is especially useful when and where the subject entity does not trust the verifying entity but still has to prove to the verifying identity that it knows specific information. In a DLT scenario, this ability allows an entity to prove that its authenticating details fulfill certain requirements without revealing the actual details being requested.

Traditional security guidance published by organizations such as The National Institute of Standards and Technology (NIST), International Organization for Standardization, Center for Internet Security, Control Objectives for Information and Related Technologies, The SysAdmin, Audit, Network and Security Institute, and Internet Security Alliance are useful in addressing security concerns for traditional IAM processes and technologies with DLT, however additional security considerations must be identified and addressed. DLT-specific security concerns respective to IAM generally surround the key management lifecycle, which is critical to the related lifecycle of an identity and its corresponding access privileges in a DLT environment. For example, an IAM-with-DLT scenario would require an organization to evaluate IAM components such as key creation, maintenance, storage, and disposal—each of which may not be considered critical security considerations within traditional IT security publications.

As mentioned above, decentralization also provides additional possibilities to strengthen IAM. In a distributed environment, entities may choose to retain control of their identity, as opposed to permitting their identity to be controlled by a third-party. Assuming the user follows basic security protocols, this can be a more reliable form of identification and authorization than requesting proof of identity from a third-party provider who may have security gaps or vulnerabilities.

DATA INTEGRITY

Digital ledgers provide an inherent level of security through their tamper-evident and tamper-resistant characteristics, which is a reason they are trusted for financial transactions. With DLT, tamper evident represents the ability to identify modifications, malicious or otherwise, to transaction records in the validation or post-validation processes. Tamper resistance is the difficulty of modifying past transaction records that have been validated and appended to a digital ledger. Tamper evident and tamper resistant characteristics are established through the use of cryptographic hash functions. Cryptographic hash functions are critical to the security and preservation of information being processed, stored, and transferred in a DLT environment as they encrypt sensitive transaction information such as timestamps, which preserve the order, or history, in which transactions are appended to a digital ledger. Cryptographic hash functions also encrypt digital signatures, which identify the parties involved in a transaction, as well as other sensitive information such as digital asset quantities and amounts.

There are a number of recommended, standardized cryptographic hash functions used across DLT environments. These standardized functions possess inherent security properties that are expected to function correctly to allow for a secure DLT environment. However, these generally accepted hash functions do not come without process difficulties and increased security risks.

For example, larger hash functions take up more space on a computer, and therefore lead to slower processing and validation speeds. Unreliable validation can lead to security vulnerabilities and distrust in the network. Furthermore, as computers increase in processing power, standard cryptographic hash functions are subject to functional obsolescence. For this reason, it is important that organizations ensure that their cryptographic hashing mechanisms are flexible to changes in the marketplace.

Use Case:

In 2019, approximately $2M worth of digital assets were stolen from an emerging technology investment fund using the private key stored on an officer's mobile device. The breach allowed the hackers to gain access to the officer's hot wallet, or digital asset storage platform connected to the internet—in this case via mobile device—in order to compromise the wallet and gain unauthorized access to the digital assets. This use case highlights the need for a comprehensive DLT security approach to address all aspects of the DLT key management lifecycle including the DLT-specific security considerations associated with the creation, maintenance, storage, and disposal of sensitive key information.

Traditional guidance for standardized cryptographic hash functions has been published by organizations such as NIST, ISO, Open Web Application Security Project (OWASP), and The Institute of Electrical and Electronics Engineers Standards Association (IEEE), with respect to traditional IT environments. However, there are a multitude of DLT-specific security considerations related to cryptographic hash functions which have not been formally addressed by professional organizations. Such DLT-specific security considerations include comprehensive code review for DLT protocols and smart contracts, monitoring of transaction processing volumes and times, scalability of computational resources, the key management lifecycle as it pertains to DLT and cryptography, and authenticating users and transactions via cryptographic hash functions on a distributed ledger.

CONSENSUS MECHANISMS

Unlike traditional distributed databases, DLT incorporates the functionality of consensus mechanisms. Consensus mechanisms are mathematical algorithms which consist of validation rules that provide independent participants the ability to verify the validity and integrity of transaction records being proposed to a DLT environment's digital ledger. The ability for independent participants to reach consensus on the current state of a digital ledger supports the maintenance of data integrity within an adversarial environment.

Consensus mechanisms are primary targets for the exploitation of DLT environments. When successfully exploited, consensus mechanisms may function inappropriately, leading to unauthorized transfers of digital assets, unauthorized censorship of transactions, double-spending, or operational disruption to the transaction validation process. Security must be considered at all stages of the DLT lifecycle including the design, development, implementation, and production. DLT-specific security considerations related to consensus mechanisms include consensus rule design, access management, separation of duties, deployment of consensus modifications, monitoring of consensus performance and prevention of attacks.

> ### Use Case:
>
> **In 2019, a global digital asset exchange discovered a large-scale security breach where hackers stole $40M worth of digital assets in one transaction via the compromise of a large number of application programming interface (API) keys, two-factor authentication (2FA) passcodes, and other sensitive user account information. To obtain sensitive information, the hackers bypassed the 2FA security algorithm, which had been used by the exchange to generate passcodes to access user accounts. If the exchange had been aware that the 2FA security algorithm did not support the custom hash function leveraged by the exchange to encrypt the API keys, the hackers would not have been able to bypass the 2FA without having access to both the application and user devices. Using a 2FA security algorithm that supports a custom hash function would have forced the hackers to obtain access to both the application and the user devices in order to successfully breach the accounts in which the stolen digital assets had been stored. This use case highlights the need for a comprehensive DLT security approach to provide guidance and practices respective to securing account access with the use of cryptographic hash functions, standard authentication methods, and bridging the security gap between DLT and traditional IT environments.**

There are a range of consensus mechanisms that may be leveraged for DLT, each of which possess common and unique security considerations and weaknesses. One consensus mechanism often used by permissioned DLT environments is the federated byzantine agreement (FBA), or distributed quorum. The FBA is a consensus mechanism where DLT environment participants assign trust to other participants who have been identified as trusted by the greater DLT environment. However, no matter the degree of trust assigned to participants, the environment is constantly at risk of rogue actors. It is imperative that organizations operating with the FBA consensus mechanism take into account appropriate DLT-specific security considerations including KYC/AML procedures, participant lifecycle management, participant activity monitoring and reporting, and operational capacity and scalability monitoring to ascertain whether the DLT environment may support, or require, additional participants to adequately process transactions.

TRANSACTION EFFICIENCIES

DLT is often promoted for enabling faster transaction settlement times, lower costs associated with transaction processing, enhanced transparency between transacting entities, potentially higher scaling capabilities than traditional databases and currencies, and the use of smart contracts for automation.

Key finance operations that may be subject to the identified processing efficiencies are procure-to-pay, intercompany transactions, order-to-cash, and acquire-to-retire.

For example, DLT may provide the order-to-cash process for customer billing the opportunity to achieve real-time visibility to involved entities and allow for external inputs to trigger faster settlement of balances with customers. In order to achieve the identified processing efficiencies, organizations need to evaluate a multitude of security considerations to ensure that the implementation of DLT does not result in operational disruption.

Use Case:

To counteract wide-spread or evolving security vulnerabilities, Hyperledger Sawtooth, created via the open source, collaborative effort of the Hyperledger ecosystem, employs the ability to toggle between various consensus mechanisms. Hyperledger Sawtooth is one example of how this flexibility allows organizations using DLT to adjust to emerging risks and vulnerabilities in consensus mechanisms, and can serve as a form of security. To avoid the risk of stagnation in the face of evolving technology, this idea of functional flexibility could be employed in other DLT components, such as smart contracts.

There are efficiencies to be obtained with the adoption of DLT, however, security considerations related to governance structure, DLT integration, operational capacity and scalability, legal risk, and data protection and privacy must be adequately addressed in order to achieve these efficiencies. A wide range of resources exists to assist organizations with the previously mentioned security considerations for traditional IT environments, however, there is no one-size-fits-all approach to addressing the considerations for DLT environments. For example, to ensure operational resilience, organizations need to consider how their DLT environments' transaction throughput and processing volumes are monitored to guarantee the environment maintains adequate capacity to process transactions during peak volume periods. Several factors must be considered when evaluating transaction processing, including the scalability of the environment, the number of active nodes, and the consensus mechanism used to process the transactions.

Use Case:

In 2016, a decentralized autonomous organization developed on the open-source Ethereum protocol was victim to a successful Reentry Attack, which ultimately led to a hard fork of the Ethereum protocol and the theft of approximately $50M in Ether from the organization. The attack exploited a smart contract vulnerability wherein attackers were able to write a piece of malicious code referred to as a "recursive call bug."

The "recursive call bug" was executed against the decentralized autonomous organization's code to repeatedly withdraw Ether funds from the single wallet where the decentralized autonomous organization stored its initial coin offering (ICO) proceeds. Once withdrawn from the organization, the attacker anonymously transferred the funds to its own wallet.

COMPLIANCE

Compliance leaders in the financial industry are focused on assessing and enhancing their compliance effectiveness in response to the continuously evolving DLT and digital asset regulatory environment. DLT provides an opportunity to enhance the compliance function by providing more accessible, transparent, and secure data processing, increased transaction processing efficiency, multi-party transaction validation, and continuous monitoring of assurance capabilities.

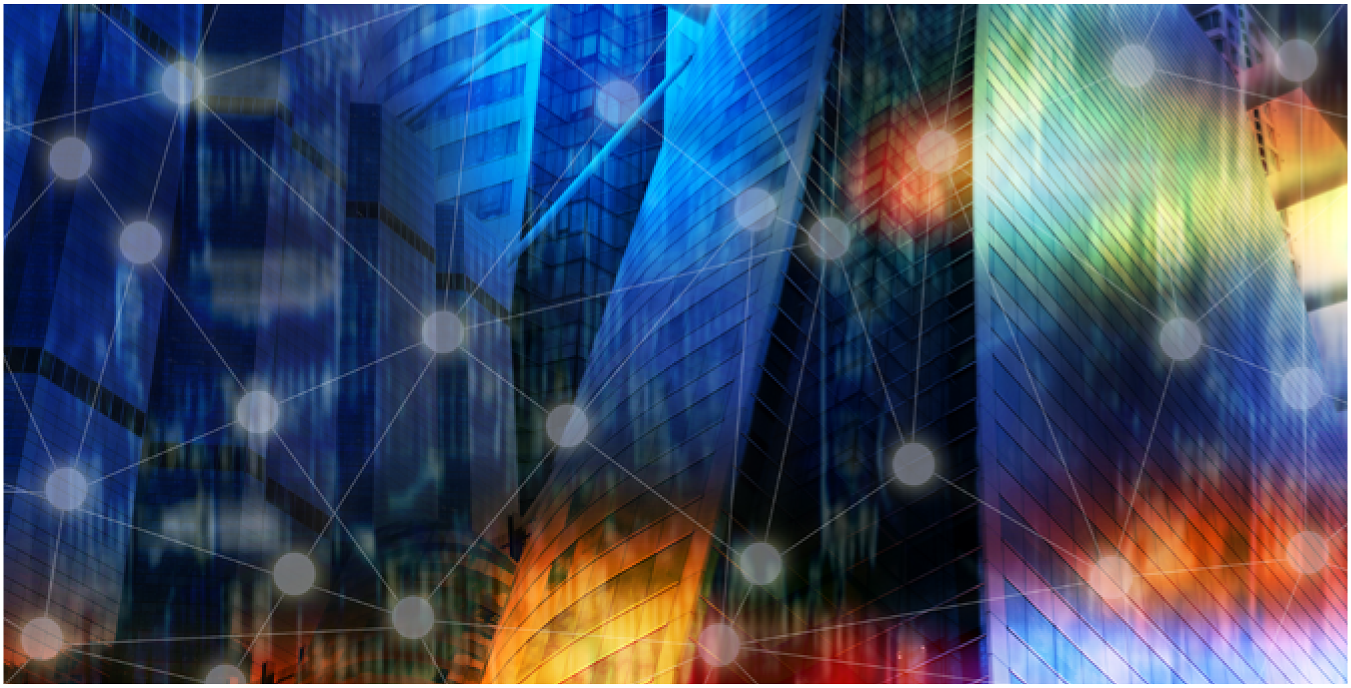
Security considerations include design and execution strategy, timely response to issues, and readiness for regulatory change.

DLT plays host to a variety of value propositions for the financial services sector. This section identifies gaps that currently exist between security standards and guidance published for traditional IT environments and DLT environments, specific to the value propositions identified. In the subsequent section, the paper will explore the gaps in greater detail and present the need for collaboration from the financial services sector to produce a comprehensive and standardized approach to DLT-security.

Use Case:

In 2018, a major Canadian bank explored a number of use cases for DLT. The objective of the bank's technology function was to validate the benefits of DLT, to enable greater efficiency in the intercompany sharing of client know-your-customer (KYC) data. With the engagement of a consulting firm, the bank was able to develop a KYC data proof-of-concept using the Hyperledger Fabric DLT platform. The platform was selected for its ability to provide features respective to privacy and its ability to restrict sharing of sensitive intercompany client data through the implementation of smart contracts.

Ultimately, the bank transformed their KYC data process from a siloed, line of business process, into a distributed operation wherein KYC data could be aggregated and stored in a distributed manner, yet accessed by any authorized participant with access to the DLT environment.



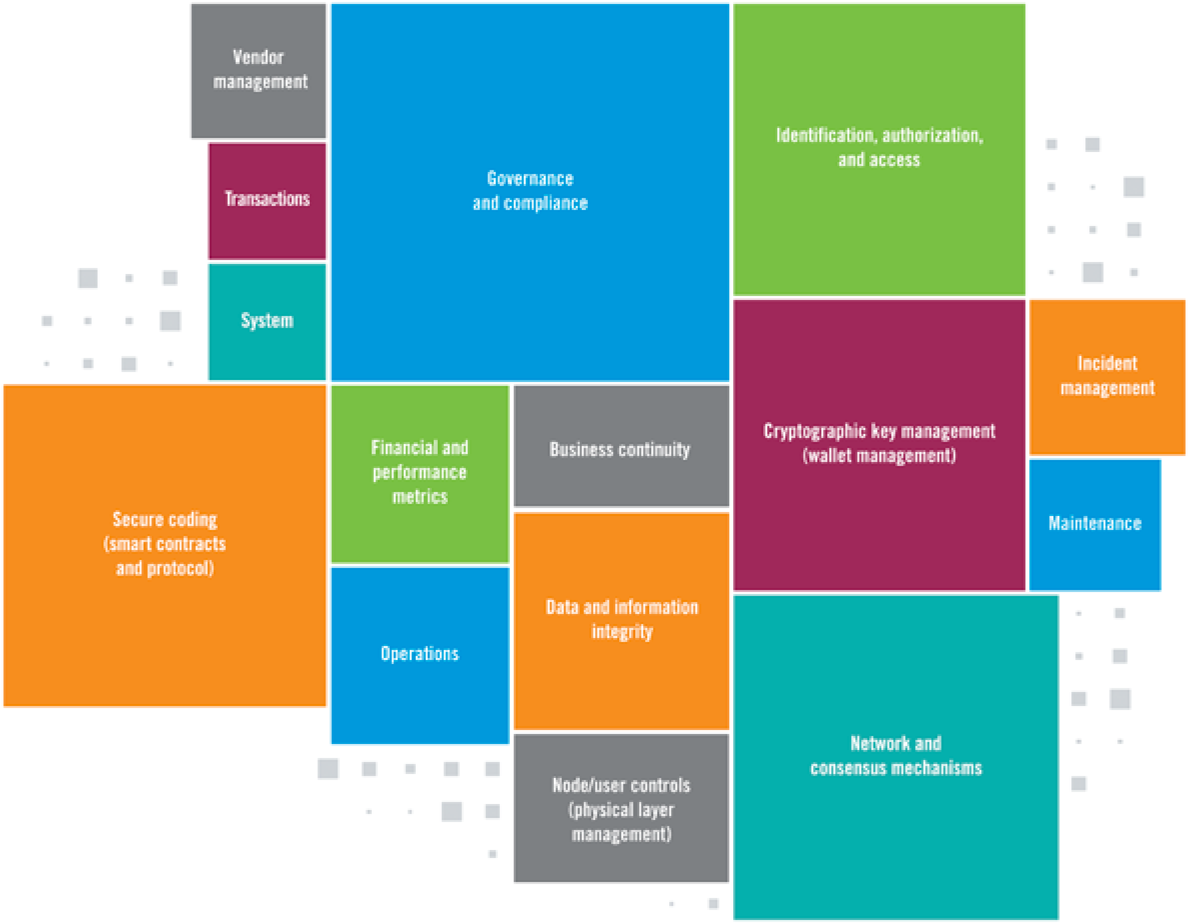
SECURITY ASSURANCE CONSIDERATIONS FOR DLTs

There are a range of DLT security-related frameworks, guides, standards, and practices available to organizations. While maturity levels may vary, it is important to consider how DLT may impact organizations at all levels by developing a comprehensive understanding of DLT current security threat vectors. The chart below illustrates fifteen categories of the DLT security landscape. Data was collected from 20+ guides, frameworks, assessments, and other methodologies published by professional organizations.

The chart categorizes the most frequently mentioned DLT security and general IT-security categories, comprised of 150+ subcategories. Larger blocks in the chart indicate that a greater count of organizations mentioned that category as a part of their DLT security considerations.

While this chart does not comprise an exhaustive search of all possible DLT security publications and related security considerations, it does provide high-level insight into the most commonly researched and utilized security considerations. It is clear that organizations have thought carefully about how their DLT environments will be impacted by identification, authentication, access controls, secure coding, governance and compliance, network security, and consensus mechanisms. These security "themes" comprise a majority of the literature surrounding how to protect an organization's operating environment.

Three areas which have received less collective thought include incident management, transactions, and business continuity related to DLT. Some of these categories clearly overlap—as such, it is not imperative that organizations categorize their security protocols in the manner presented above. However, it is important that each of these categories are considered in the implementation and continuous maintenance of a secure DLT environment.



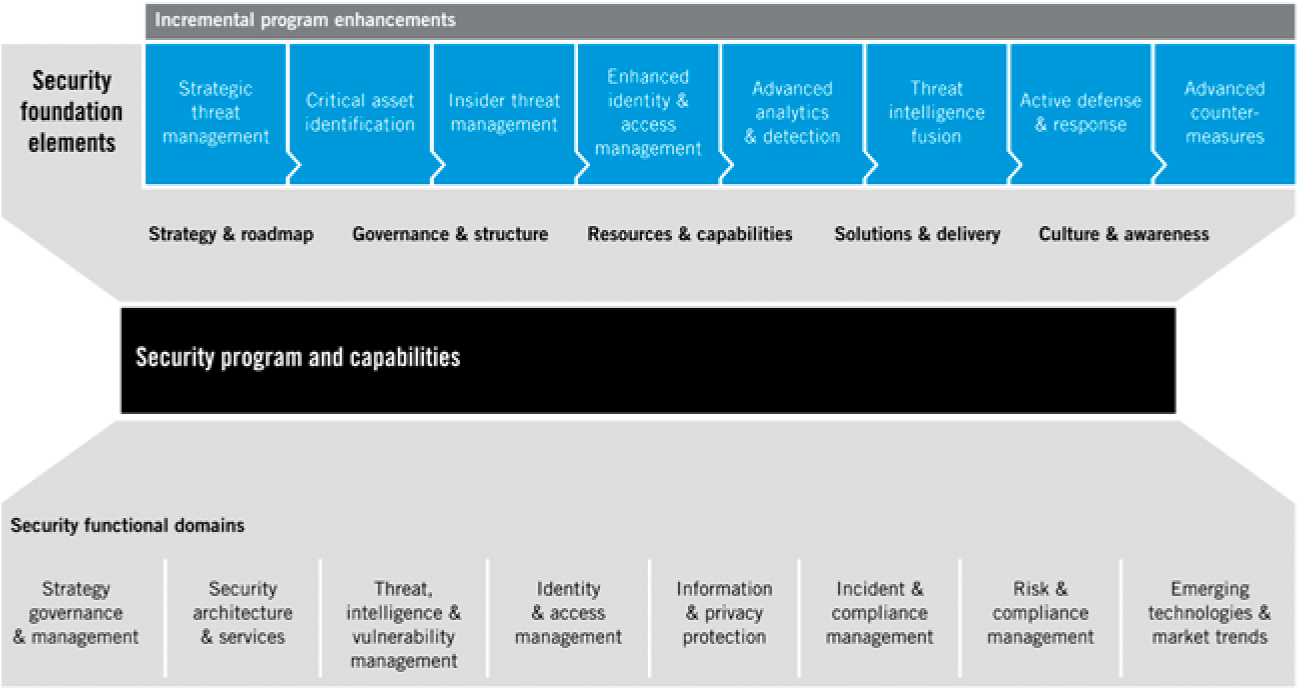
SECURITY BASELINE CONSIDERATIONS FOR DLTs

As DLT evolves, it is apparent that DLT-specific security considerations exist and require analysis from industry experts. The block chart in the previous section includes both traditional IT security considerations and DLT-specific security considerations. It is important to illustrate the difference between traditional IT security considerations and the new developments surrounding DLT-specific security considerations. For example, smart contracts, or programmatically-executable code, can perform legally binding requests on behalf of multiple entities within a DLT environment. To add to the complexity, smart contracts are irreversible. The security consequences related to this functionality are novel, and worth considering in more detail.

The illustration below demonstrates foundational elements for a security function, its functional domains, and areas for incremental program enhancements. In understanding what was uncovered in the previous section, many of the functional domains still have opportunity to be described, vetted, and published against DLT–specific requirements. Until these actions occur, it will be difficult to extend to areas of enhancements (e.g., strategic threat management, or advance analytics and detection).

Some traditional IT security considerations may help users gain comfort with the strength of DLT-specific security; however, additional coverage may be needed to ensure that DLT-specific security considerations are addressed in their entirety. Although traditional IT security may assist in addressing DLT security, there are various DLT-specific nuances and risks which may require additional security controls above and beyond the standard employed for traditional IT environments. It is promising to note that the block chart above illustrates that some key security domains are commonly addressed across DLT-specific and traditional IT security literature.

Security domains such as incident management, business continuity, and threat/vulnerability management should be considered for DLT. For example, business continuity planning for a centralized database has one set of characteristics and related controls, and a completely different set for a decentralized database. Given the irreversibility of DLT transactions, policies and procedures must also account for DLT-specific considerations such as immutability. These DLT-specific concerns can be extrapolated across all traditional IT security domains; therefore, it would be prudent for organizations to keep these differences in mind while evaluating the DLT-specific security domains such as wallets and smart contracts.


Incremental program enhancements
Security foundation elements
Strategic threat management
Critical asset identification
Insider threat management
Enhanced identity & access management
Advanced analytics & detection
Threat intelligence fusion
Active defense & response
Advanced counter-measures
Strategy & roadmap
Governance & structure
Resources & capabilities
Solutions & delivery
Culture & awareness
Security program and capabilities
Security functional domains
Strategy governance & management
Security architecture & services
Threat, intelligence & vulnerability management
Identity & access management
Information & privacy protection
Incident & compliance management
Risk & compliance management
Emerging technologies & market trends

DLT SECURITY ASSESSMENTS

At this point, several DLT-specific and several traditional IT security considerations have been described. An example of how these risks overlap with a real-world use case can be useful in determining where potential strengths and areas for improvement exist in a traditional framework when applied to a DLT use case.

In the table below, slightly modified versions of each of the five domains of a popular security assessments are evaluated for their impact on traditional IT and DLT environments. Areas where there are similarities or overlap between processes for a traditional IT environment and a DLT environment are identified in the middle column.

In the right column, gaps in the security assessment in regard to DLT environments are noted.

The following table discusses all the sub-components of the assessment. This is not an exhaustive list of all overlapping controls. It is intended to illustrate areas for improvement in current standard financial services security frameworks when applied to DLT environments, as well as to provide an example of how an organization can apply current industry frameworks to a DLT environment in order to find overlapping controls or new areas of improvement.

> **Behavioral Analysis:**
>
> **Tests and assessments of security do not need to pinpoint every transaction, node, and account balance. In 2019, a security analytics company prevented a large DDoS attack by comprehensively analyzing the behavior and network connections, instead of pinpointing specific IP addresses as the culprit. This "behavioral analysis" to prevent network attacks and analyze performance can be extrapolated to a DLT environment. Verification of all transactions on a network can be extraordinarily burdensome compared to gaining assurance of a network's security by looking at its general behavioral patterns.**

ASSESSMENT CRITERIA	TRADITIONAL AND DLT ENVIRONMENT SIMILARITIES	ADDITIONAL CONSIDERATIONS FOR DLT ENVIRONMENTS
Risk Management and Oversight	• **Strategy/Policies:** Policies and procedures are commensurate with risk and are communicated enterprise-wide. • **IT Asset Management:** An IT asset inventory is maintained. • **Risk Management Program:** A risk management function exists within the organization. • **Training:** Training is implemented as new issues emerge. • **Culture:** Employees are held accountable for compliance with security program.	• **Decentralization:** While decentralization is a major advantage of blockchain, it is also a main security concern as it limits the amount of control any single participating node on the blockchain can exercise. • **Distributed infrastructure:** The main risk of distributed infrastructure is a decreased level of oversight. • **Data Immutability:** Immutability of a distributed ledger means that changes to information stored on a blockchain compromised maliciously or by error often require a non-trivial amount of time and resources to correct. • **Consensus:** Consensus can be a major threat vector across all blockchains regardless of algorithm choice. Consensus based attacks have many access entry points across code, networks, users and nodes. • **Smart contracts:** Smart contracts allow organizations to run programmable logic on blockchains. However, their autonomous operations, without human oversight, make them more difficult to monitor and expose a greater risk of exploitation.

Vulnerability Management	• **Threat Intelligence and Information:** The organization monitors new threats and vulnerabilities. • **Information Sharing:** Security threats are gathered and shared with employees and law enforcement. • **Malware:** While blockchain core technology, with its cryptographic protections, is generally resistant to direct exploitation by malware, the ancillary supporting systems in a blockchain ecosystem such as wallets and browsers are subject to the same malware attacks as non-blockchain systems.	• **Cryptography:** Cryptographic public key algorithms and hash functions are fundamental components of blockchain security. These critical security functions are used for identities, transaction and block signing, and form the foundation of blockchain's integrity and immutability guarantees. Theft or loss of cryptographic private keys may result in identity theft, user obfuscation, and loss of cryptocurrency and assets. • **Code vulnerabilities:** Smart contracts are executable code designed to run distributed and autonomously on blockchains. Their distributed nature make smart contracts difficult to maintain due to their immutability and without human interaction can lead to exploitations resulting in direct financial loss. • **Malware:** Blockchain core technology, with its cryptographic protections, is resistant to direct exploitation by malware. • **Peer-to-Peer:** Blockchain's peer-to-peer design makes it difficult and complicated to keep distributed code, such as smart contracts, synchronized across different organizations' security and change control rules and procedures
Cybersecurity Controls	• **Secure Coding:** DLT introduces nuance to coding languages and execution styles. However, secure SDLC practices remain generally the same. • **Anomalous Activity:** Anomalous activities should be monitored where possible. • **Event Detection:** Mechanisms to alert management of potential attacks should be used in all environments.	• **Event Detection:** Event detection can be more difficult with blockchain technologies due to the autonomous execution of code such as smart contracts. Often transactions are conducted anonymously at high velocity and are only observed after they have occurred, making recovery difficult. • **Nascent technology:** Since the blockchain technologies are relatively new, the same level of expertise and security as in traditional cybersecurity does not yet exist.
Third Party Management	• **Due Diligence:** The due diligence process for permissioned DLT environments should include the same elements as in traditional environments. • **Ongoing Monitoring:** Monitoring of malicious third parties should continue.	• **Developer skills:** Most smart contract languages and technologies, when compared to existing traditional programming languages, are immature and lack widely accepted secure development practices and guidance. • **End point security:** Blockchains themselves, are by design inherently secure. It is the third party supporting systems and the APIs that allow external systems to interact with the blockchain network that introduce security vulnerabilities.
Incident and Event Management	• **Testing:** Testing should continue to include collaboration with critical third parties and routine tests of systems, applications, and data recovery. • **Detection:** Organizations should continue to utilize alert parameters and system performance reports.	• **Contract management:** Smart contracts can be considered as legally binding, although common and internationally recognized legal standards for "code as law" do not yet exist. • **Business continuity and disaster recovery strategy:** Blockchain, due to it properties of immutability and distributed code and data features provide inherent business continuity and disaster recovery capabilities.

It is apparent from the above illustration that a variety of additional considerations exist when applying a traditional IT security assessment to a DLT environment. This may also make obvious the need for a comprehensive DLT security framework. There are often too many nuances and technology limitations to apply existing frameworks to entirely new problems; especially ones as complex as DLT.

A DLT SECURITY FRAMEWORK FOR THE FINANCIAL SERVICES INDUSTRY

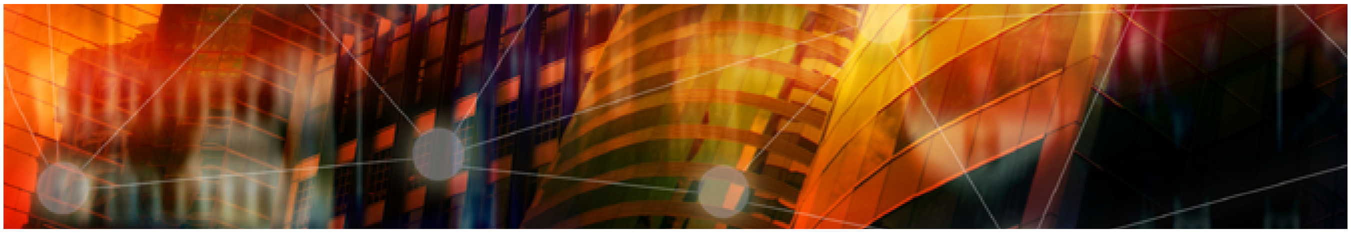
Given the variety of use cases, there is no one-size-fits-all approach to DLT security. However, there is the possibility of a reliable and comprehensive framework to follow when approaching DLT security, regardless of the use case. Agreed-upon standards will prove invaluable to making such a framework possible. Standards perform several vital functions in regard to providing strong DLT security for all participants in the financial industry.

Standards can play an important role in ensuring interoperability between multiple DLT implementations, which can reduce the risk of a fragmented ecosystem within the industry. As the technology develops and the number of DLT participants increases, many stakeholders will want to interact with and use other blockchain platforms that operate independently from their own. If each industry participant lays its respective DLT foundations in a silo, this synergistic result will be difficult to achieve. Standards can be the guiding light for organizations to ensure that they will be able to work with others and build on top of their previous infrastructure investments in a controlled and modular manner.

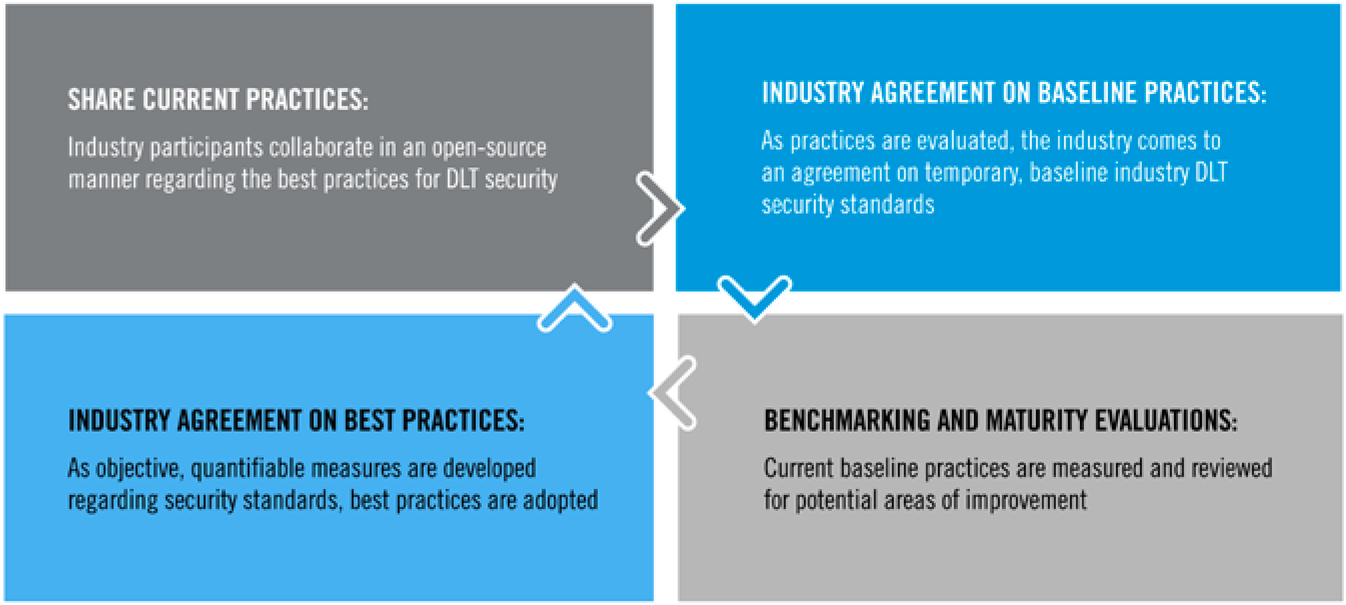
Standards also can result in shared vernacular, which will in turn provide for an improved understanding of the technology. This increased understanding will expedite adoption by the industry, as decision makers will be able to more quickly understand some of the risks and opportunities associated with DLT. Standardized terminology can also assist with the development of robust, easy-to-understand DLT security standards.

Governance, and specifically data governance, is a critical security issue that often delays the adoption of new technologies like DLT. Standards can also help alleviate this concern. By establishing a principles-based framework, firms have the flexibility to identify potential security weaknesses in their DLT implementations. A principles-based framework will also increase the likelihood that disparate DLT implementations from different organizations could be linked or otherwise exchange information. In addition, supervisors and regulators will have a consistent measure for understanding potential strengths and weaknesses in different DLT implementations.

Lastly, standards play a role in digital identity management and can foster end-user trust in the technology. Digital identity is the compilation of an individual's collective actions performed online. The collection of actions can be corroborated to provide a very comprehensive view of that individual's reliability, interests, and general personality. DLT can enable users to retain more control of this identity, allowing them to have greater privacy and trust in the actions they perform online.



In creating this standardized approach, the financial industry has the opportunity to develop, share, reuse, and continuously improve upon an approach to DLT security. This effort will require the collaboration of the financial industry at large. Further, it will benefit from continuous innovation and iteration. An example of the DLT security collaboration and coordination life-cycle will likely resemble this format:



SHARE CURRENT PRACTICES:

Industry participants collaborate in an open-source manner regarding the best practices for DLT security

INDUSTRY AGREEMENT ON BASELINE PRACTICES:

As practices are evaluated, the industry comes to an agreement on temporary, baseline industry DLT security standards

BENCHMARKING AND MATURITY EVALUATIONS:

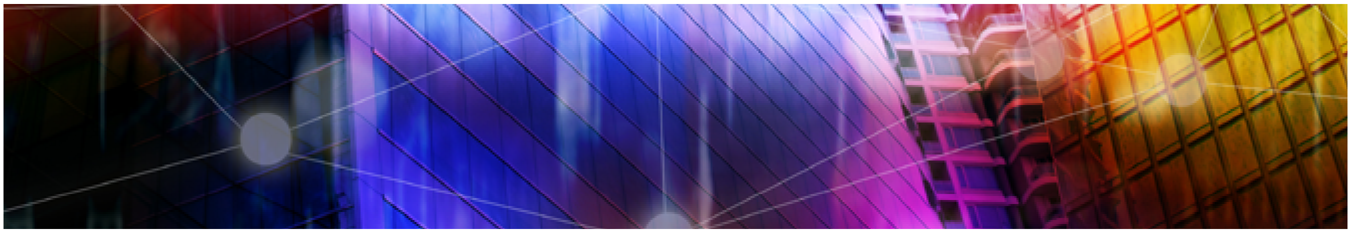
Current baseline practices are measured and reviewed for potential areas of improvement

INDUSTRY AGREEMENT ON BEST PRACTICES:

As objective, quantifiable measures are developed regarding security standards, best practices are adopted

As is common in IT security communities, frameworks must be widely available, generally agreed upon, and commonly adopted. As best practices mature, they can be adopted into a formal framework and used for financial industry participants and regulators alike.

In light of the speed of digital transformation within the financial services sector, DTCC calls for a coordinated strategy for the development of a principles-based framework to identify and address DLT specific security risks. Because these risks may cross multiple critical infrastructure sectors, the coordinated strategy should be a cross-sector effort beginning with a conversation between the financial services sector, DLT providers and consumers. As a first step, we will leverage our unique role within the financial services sector to begin the conversation, and we encourage interested parties to contact one of the individuals in the Contacts section of this white paper to participate.



CONTACTS

Stephen Scharf
Chief Security Officer
sscharf@dtcc.com

Chris Koutras
Executive Director Security Architecture and Technology
ckoutras@dtcc.com

William Izzo
Director Security Technology
wizzo@dtcc.com

Questions or comments about this white paper can be addressed to your DTCC Relationship Manager at 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 Asia Pacific.

25452TC020620