Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives - Guidance Notes Series

Note 1: Collateral Registry, Secured Transactions Law and Practice

May, 2020
ACKNOWLEDGMENTS

The publication of this Guidance Note was made possible due to the generous support of the Swiss State Secretariat for Economic Affairs (SECO). The preparation of this Guidance Note was led by the Secured Transactions and Collateral Registries Team (Pratibha Chhabra, Murat Sultanov, John M. Wilson, Elaine MacEachern, and Luz Maria Salamina) within the World Bank, under the guidance of Mahesh Uttamchandani. The primary technical content of the Guidance Note was developed by Dr. Marek Dubovec under the aegis of Kozolchyk National Law Center (NatLaw).

Special thanks to Charles W. Mooney, Jr., Giuliano G. Castellano, Andrea Tosato, Bob Trojan, and Simon Stanley for their contributions to this report. The authors are indebted to the following peer reviewers for their excellent suggestions and thoughtful contributions to improve the content of the Guidance Note:

Jae Sung Lee, United Nations Commission on International Trade Law
Ivor Istuk, World Bank Group
Prema Shrikrishna, World Bank Group
Harish Natarajan, World Bank Group
# TABLE OF CONTENT

**EXECUTIVE SUMMARY**

**INTRODUCTION**

1. **EFFECT OF DISTRIBUTED LEDGER TECHNOLOGY ON THE COLLATERAL REGISTRY**
   - 1.1 Functions and Operation of Collateral Registries
   - 1.2 Sufficiency and Completeness of Information
   - 1.3 Authentication of Users and Participants
   - 1.4 Authorization
   - 1.5 Integrity and Security of Stored Data
   - 1.6 Searches - Ease of Access, Search Logic, and Real-Time Availability of Information
   - 1.7 Interoperability with Third-Party Systems - Payment Systems and Other Registries
   - 1.8 DLT-STCR Registry Versus Other DLT Registries
   - 1.9 Some Proposed Applications

2. **DLT AND SECURED-TRANSACTIONS LAW AND PRACTICE**
   - 2.1 Nature of the Grantor’s Right in Digital Assets
   - 2.2 Collateral Types under Secured Transactions Laws
   - 2.3 Creation
   - 2.4 Methods of Perfection - Registration and Possible Alternatives
   - 2.5 Perfection as to Original Collateral
   - 2.6 Perfection as to Proceeds
   - 2.7 Priority Considerations
   - 2.8 Enforcement
   - 2.9 DLT as a Facilitator of Enforcement
   - 2.10 Conflict-of-Laws Regime
   - 2.11 Role of Intermediaries
   - 2.12 Effect on Lenders’ Procedures and Practices
   - 2.13 Security Rights in Insolvency

3. **FINAL OBSERVATIONS**

**REFERENCES**
Secured transactions frameworks, including substantive laws, collateral registries, and their underpinning regulations, influence practices of lenders. These practices include due diligence, monitoring of the collateral and its eventual disposal in secondary markets as well as registering notices in collateral registries. Many aspects of secured transactions frameworks already utilize electronic technology supported by substantive laws and regulations. Distributed ledger technology (DLT), especially blockchain, promises to transform some of these aspects, functions, and practices.

This Guidance Note examines the potential of DLT within the context of the UNCITRAL Model Law on Secured Transactions. While this model is the primary reference, the Guidance Note also provides examples from domestic secured transactions frameworks, especially where the analysis leads to a different result. It examines these issues from different perspectives, including those of policy makers and legislators but also secured creditors and borrowers. It should be a useful tool not only for stakeholders in economies that contemplate undertaking secured transactions but also for those engaged in secured transactions where DLT plays some role, such as a loan applicant proposing to use as collateral her digital asset for which the secured transactions law does not contain any specific provisions.

The traditional roles and functions of collateral registries are examined from the perspective of DLT. These roles and functions include perfecting security rights, establishing their priority, and facilitating due diligence of prospective buyers and secured creditors. Given the structure of collateral registries as centralized institutions, permissioned (rather than permissionless) blockchain would more closely replicate the functions of non-DLT technology without significantly changing the nature of the collateral registry. This model would not necessitate changes to the legal framework underpinning the registry.

Modern collateral registries already provide all or most of their services electronically and in an automated fashion. Accordingly, the potential application of DLT is examined from the perspective of superior technological features. Non-DLT technology already ensures that i) notices are not registered with incomplete information; ii) registrants are properly authenticated before being able to register notices; iii) processes are implemented to minimize the risk of unauthorized registrations, especially amendments and cancellations; iv) registrations are timestamped and stored in a chronological order; v) the data stored in centralized databases maintained by the registries is secure and does not become compromised; and vi) searchers have electronic access to efficiently retrieve records from the databases or obtain confirmation that no registration exists against a particular identifier of the grantor.

Both “non-DLT” technology and DLT have similar limitations in terms of addressing some challenges of collateral registries. Foremost, neither is able to eliminate or reduce the risk of “garbage in, garbage out,” where the registrant remains responsible for accuracy and legality of information entered in a notice. Similarly, neither is capable of effectively establishing gateways to other systems – the problem of interoperability. A DLT system minimizes but does not entirely eliminate the risk of “single point of failure” characteristic of non-DLT supported registries. In both, a software vulnerability may be exploited. These limitations and challenges may be addressed in the future as technology matures.

DLT may be superior technology for systems with certain characteristics. This is especially the case for those systems with a high risk of tampering with the registry records, ensuring that information in registered notices remains immutable. While it ensures the integrity of data, DLT’s inherent limitation is its ability to store hashes of data rather than the data itself that a searcher needs to conduct due diligence. As DLT matures, this limitation is expected to be eliminated.

Overall, DLT does not provide readily identifiable benefits for the administrator of the registry to consider replacing “non-DLT” technology with DLT. The benefits that would induce a collateral registry administrator to replace the
existing system with DLT are yet to materialize. Several applications have been proposed for collateral registries, including a complementary DLT database, a facility to constantly update the collateral description in a registration as individual receivables are financed and collected, to tokenizing the registration itself. The commercial utility of some of these proposals is questionable, while non-DLT technology already enables other proposed applications. DLT has been more promising in installations of land registries.

Various digital assets of different types, native and non-native tokens, and different functions, payment, security, utility, and hybrid tokens are held and transferred through distributed ledgers. The second part of this Guidance Note examines various aspects of the substantive secured transactions framework and related laws that affect processes of secured lenders when digital assets of different types are or may be used as collateral. These aspects include the creation, perfection, priority, and enforcement of security rights in different types of tokens as well as the effect of laws governing custodians of digital assets, their insolvency, and transfers of digital assets through distributed ledgers.

Classification of digital assets, first as either property or personal claims and then under a particular collateral type defined in the secured transactions law, is critical. The rights of holders of digital assets, and by extension their secured creditors, will depend on whether the relevant law classifies the digital asset as property or personal claims, whether some statutory restrictions preclude its transfer, and the type of collateral under the applicable secured transactions law. These classifications are typically limited to the purpose of the particular law and may vary. Of significant importance is the classification under insolvency law that will determine the recovery of the holder, or its secured creditor, from an insolvent custodian.

Classification as a type of collateral is essential to the application of the secured transactions law, particularly the perfection, priority, and conflict-of-laws provisions that are asset specific. This classification may be established through the definitional section of the secured transactions law, by other laws to which the secured transactions law defers (e.g., the securities law that defines security), or by an action of the parties, such as crediting a digital asset into a securities account. The application of the relevant creation, perfection, priority, and conflict-of-laws provisions depends on that classification. For instance, classification of a token as a receivable would render any anti-assignment clause ineffective as against the secured creditor. Classification as a deposit account would enable the use of control to perfect a security right. Some enforcement provisions also apply in specific contexts, such as exempting the secured creditor from providing a notification of disposition if the collateral is sold on a recognized market, which may necessitate an assessment of whether a “crypto exchange” is such a market.

While DLT emerged as a system to disintermediate relationships, various implementations have necessitated services of custodians of digital assets. Conceived as a disintermediated system, the practices have led to deposits of digital assets with custodians. The profile of the custodian industry has been raised by a number of insolvencies resulting in significant losses for investors. Several, primarily regulatory, measures are being contemplated to provide for protection of holders of digital assets, comparable to that available to investors in securities and other financial products.

The most profound advances have been made in processes of lenders. The assessment of creditworthiness of loan applicants, valuing and monitoring the collateral, but also its disposal in secondary markets have been impacted by DLT, smart contracts, and artificial intelligence. The developments in these processes thus far have not necessitated any legal changes, though some aspects, especially regarding smart contracts, such as their automated enforcement, raise policy questions.

Finally, insolvency highlights a number of important aspects affecting transactions with digital assets. The classification of digital assets determines the nature of recovery of the holders of those assets and their creditors in insolvency of grantors and custodians, exemptions from the automatic stay, the power of the trustee to use cash proceeds, as well as rights to participate in proceedings in various groups of creditors. Several recent high-profile insolvencies shed light on some peculiar features of digital assets, such as their high price volatility between the time of filing for insolvency and distribution to creditors.
INTRODUCTION

Secured transactions laws underpinned by electronic collateral registries facilitate access to credit secured with movable assets, such as equipment, inventory, or receivables. A number of elements of secured transactions and collateral registry (STCR) regimes rely on technology, such as providing digital assets as collateral, disposing of collateral on an electronic platform after default, or designing the search function of a collateral registry. Blockchain, as a type of distributed ledger technology (DLT), provides an alternative form of storing records, enables the issuance and transfer of different types of digital assets, and facilitates lending processes, such as monitoring collateral. Existing legal frameworks are flexible enough to permit the deployment of DLT for the generation and transfer of digital assets, its use in various collateral registry functions, as well as in lending processes. However, challenges may arise in the absence of asset-specific rules that, for instance, provide for a perfection mechanism specific to security rights in digital assets.

This Guidance Note does not compare the efficiency of manual processes with those that could be accomplished using DLT. Rather, it assesses advantages and disadvantages of DLT vis-à-vis non-DLT technology, particularly in the context of electronic collateral registries. The core functions of collateral registries and features of the substantive legal framework are identified and examined primarily in the context of the UNCITRAL Model Law on Secured Transactions (UNCITRAL Model Law). Even though the UNCITRAL Model Law is just that – a model for States to adapt – the Guidance Note assumes that it has been implemented as adopted, thereby establishing a baseline from which to contemplate and analyze the variations that States could incorporate into their domestic regimes.

As further discussed in this Guidance Note, all the functions of modern collateral registries may be already performed electronically. Collateral registries allow secured creditors to register notices, also referred to as financing statements or registrations, relating to security rights, and in some cases non-consensual interests. The time of registration establishes the priority of a security right. Third parties, such as prospective lenders and buyers, are able to discover potentially existing encumbrances as part of their due diligence process. The objective is not to advocate for or against DLT as a platform for collateral registry implementations; it is rather to draw attention to specific elements of DLT, and especially blockchain, that warrant caution in the context of collateral registries.

The increase in the rate of adoption of DLT raises a number of questions in relation to all aspects of secured transactions and collateral registries. The emergence of various types of digital assets and their use in different contexts put secured transactions laws to the test when digital assets are used as collateral to secure the performance of an obligation. As secured transactions laws are closely intertwined with other areas of the law, especially property and insolvency laws, affected parties must assess several aspects of the relevant legal framework. These include the application of general laws that impact the classification of digital assets as property or personal claims under property laws, and the ability to re-claim a digital asset from an insolvent custodian.

This Guidance Note consists of two parts. The first part focuses on the applicability of the integration of private permissioned DLT systems in collateral registries because of their advantages over public and permissionless DLT implementations in the context of collateral registries. It examines various aspects of operations of a collateral registry, including the different types of registrations and the manner in which they are added and held in the registry record, the sufficiency and completeness of information submitted by registrants (filers) for registration, authentication of users and other participants in the registration process, the necessary authorizations for an effective registration, the measures taken to store registrations and ensure the integrity of stored data, various aspects of searches, interactions of the collateral registry with other registries and systems, and, finally, an overview of the application of DLT in land registration systems. The second part focuses on the legal framework governing transactions secured with various types of digital assets, including the classification of digital assets as a specific type of collateral, the creation and perfection of security rights, their priority and enforcement, and the rules that determine the applicable law in cross-border transactions. This part examines these issues, both from the perspective of
the legislator as well as a prospective secured creditor.⁸

The broad focus of this Guidance Note and its analysis, which assumes certain hypothetical transactions, is intended to interest readers who design reforms and implement secured transactions frameworks, including donors, policy makers, legislators, and registry operators, as well as those affected by transactions with digital assets, especially borrowers, lenders, and transferees of those assets.

### Key Takeaways

<table>
<thead>
<tr>
<th>Implementation of DLT in collateral registries</th>
<th>while dlt is inherently more resilient to a single point of failure as it does not rely on a centralized database that stores registrations, non-dlt databases can be protected against inadvertent and malicious attacks, and no known event of loss has been reported.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>while dlt ledgers are inherently tamper resistant, dlt installations are nonetheless susceptible to tampering of data, such as through exploiting vulnerabilities in the software. no tampering of data in non-dlt databases resulting in losses for secured creditors is known.</td>
</tr>
<tr>
<td></td>
<td>for efficiency, blockchain ledgers hold hashes of information. while hashes are sufficient to confirm data integrity, an additional search of a non-dlt database is necessary to obtain transaction details.</td>
</tr>
<tr>
<td></td>
<td>though efficiencies may be gained by enhancing interoperability of collateral registries with other registries, such as motor vehicle registries, this remains a challenge that dlt has not alleviated.</td>
</tr>
<tr>
<td></td>
<td>the commercial utility of some proposed features that may be implemented through dlt, such as tokenized registrations, is questionable or can already be achieved under the current law using non-dlt technology.</td>
</tr>
<tr>
<td></td>
<td>some proposed processes that may be implemented through dlt using smart contracts, such as triggering starter interrupt devices to disable a vehicle, have been achieved using non-dlt technology under the current law for years. it is unclear whether some proposals may be executed only through dlt, whether dlt enhances their efficiency, makes them more available, or simply provides an equally viable alternative.</td>
</tr>
<tr>
<td></td>
<td>there have not been any actual dlt installations of collateral registries that would allow further analysis. for the most part, non-dlt technology has been successfully implemented to design and operate collateral registries.</td>
</tr>
<tr>
<td>Application of secured transactions law pertaining to digital assets</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Digital assets may be used as collateral, but laws and regulations that dictate the nature of digital assets and the rights of their holders may limit or preclude the creation of security rights.</td>
<td></td>
</tr>
<tr>
<td>A transfer of digital assets may not have any proprietary legal effect, including the perfection of a security right. Where A provides financing to B to acquire a motor vehicle, an entry in a ledger that is not maintained by the relevant government agency will not be dispositive of rights to the motor vehicle. Similarly, control of a token covering a car held in the inventory of a dealer would not have the effect of perfecting a security right.</td>
<td></td>
</tr>
<tr>
<td>The UNCITRAL Model Law and other modern secured transactions laws do not provide specific collateral types for digital assets. Accordingly, the rules that generally apply to residual intangible assets would likely apply to security rights in digital assets.</td>
<td></td>
</tr>
<tr>
<td>The classification of digital assets as general intangible assets, subject to some exceptions such as security tokens, determines the applicable perfection mechanism, which is limited to registration in the collateral registry.</td>
<td></td>
</tr>
<tr>
<td>The classification as intangible assets affects the rights not only of secured creditors but also of transferees. As a result, unlike transferees of money or funds, the ability of a transferee to acquire cryptocurrency free of a security right would be much more limited.</td>
<td></td>
</tr>
<tr>
<td>Some of the touted benefits, such as automated and immediate enforcement of a security right upon default, must be balanced against the requirements of proceeding in a commercially reasonable manner and protecting affected parties.</td>
<td></td>
</tr>
<tr>
<td>DLT facilitates some aspects of secured lending practice, including valuation and monitoring of the collateral, which, if performed efficiently, may satisfy regulatory requirements applicable to banks and other regulated lenders.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Effect of DLT outside the secured transactions framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLT promised to disintermediate various transactions and relationships. Instead, custodians of digital assets and private keys play an increasingly important role generating new types of risks.</td>
</tr>
<tr>
<td>Existing custodial legal frameworks may not be suitable for custody of digital assets. Technology risks must be taken into account in light of the losses sustained by investors when their digital assets were stolen from the custody.</td>
</tr>
<tr>
<td>Depending on the classification of digital assets, different provisions of the insolvency law may be applicable to the right of a holder or secured creditor. Recent insolvency cases of custodians of digital assets revealed a number of legal issues.</td>
</tr>
<tr>
<td>The application of the traditional tools of insolvency law, such as to unwind a transaction as a preferential transfer, may be complicated by the anonymity of transactions with digital assets and the ease of their transferability.</td>
</tr>
</tbody>
</table>
## Comparison of Registry Functions in DLT versus Non-DLT Implementations

<table>
<thead>
<tr>
<th>Registry function</th>
<th>Non-DLT implementation</th>
<th>DLT implementation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrant authentication</td>
<td>To submit notices, a user would first create an account and submit credentials for verification by the Registry (either automatically or by Registry personnel). For example, via a digital certificate issued by a certification authority using Public Key Infrastructure (PKI) technology. This authentication process applies continuously as amendments and cancellations are registered.</td>
<td>Consensus rules could require that authentication would be performed by multiple nodes (entities) on the DLT network. Cryptographic signing of blocks authenticates registrants by proving that each person signing the registration had access to that person’s private key.</td>
<td>For any consent mechanisms to authenticate users to be designed into collateral registries, the law must provide for them. Delay caused by the consensus process can be limited by limiting the number of nodes required for consensus.</td>
</tr>
<tr>
<td>Authorization to register</td>
<td>The Registry does not verify whether the registrant has the necessary authority to effectuate a registration, whether from the grantor for initial registration or from the secured creditor for an amendment.</td>
<td>Smart contracts may be deployed to require consent of the parties to a particular type of registration, such as all secured creditors named in a single registration, before it is amended or cancelled.</td>
<td>For any authorization mechanisms to be designed into collateral registries, the law must provide for them.</td>
</tr>
<tr>
<td>Submission of the notice</td>
<td>A new notice is added to the registry record only when certain requirements have been met, such as confirming that no mandatory field is blank.</td>
<td>Consensus rules could require that multiple nodes (entities) on the DLT network must ensure that information has been entered in all mandatory fields.</td>
<td>Neither non-DLT nor DLT systems can eliminate or reduce the risk of “garbage in, garbage out,” where the registrant is responsible for accuracy and legality of information entered in a notice.</td>
</tr>
<tr>
<td>Security of storage</td>
<td>Multiple redundant database servers are configured to include real-time database replication to remote locations and periodic backups stored offsite, with multiple servers in several locations and automatic failover capabilities.</td>
<td>Inherent DLT features include i) tamper resistance; ii) a tamper-detection process of independent data verification; iii) a distributed and redundant system architecture; and iv) a network of heterogeneous nodes.</td>
<td>Non-DLT systems, though geographically dispersed, tend to lack heterogeneity and remain vulnerable to errors. DLT systems attacks that leverage administrative weaknesses, such as access controls, or exploit vulnerabilities may propagate across an entire network.</td>
</tr>
</tbody>
</table>

Note 1: Collateral Registry, Secured Transactions Law and Practice
<table>
<thead>
<tr>
<th><strong>Storage of records</strong></th>
<th>All information provided in notices, whether or not in mandatory fields, is stored in a registry database.</th>
<th>Presently, DLT is limited by its ability to store hashes of data rather than the data itself.</th>
<th>A current solution is to store notice data in a non-DLT database that can be indexed and store the hash of each notice in the DLT ledger. This adds cost to the design and operation of the registry.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Search and retrieval of notices</strong></td>
<td>Indexes, such as for grantor identifiers, allow rapid searches of millions of records.</td>
<td>Presently, because only a limited amount of discrete data is stored within a DLT ledger, an index cannot be created for a data field that does not exist within the ledger.</td>
<td>A current solution is to store notice data in a non-DLT database that can be indexed and efficiently searched. A notice retrieved from the non-DLT database can be hashed and a second search conducted to determine whether the hash exists in a corresponding DLT ledger.</td>
</tr>
</tbody>
</table>
1. EFFECT OF DISTRIBUTED LEDGER TECHNOLOGY ON THE COLLATERAL REGISTRY

1.1 FUNCTIONS AND OPERATION OF COLLATERAL REGISTRIES

Collateral registries are notice-based systems in which registrations contain only the information necessary to alert searchers about the potential existence of an encumbrance. Generally, required information to be entered into designated fields in a notice includes i) the identifier of the grantor (e.g., an individual’s name or a unique ID number) and its address; ii) the identifier and address of the secured creditor or its representative; and iii) a description of the collateral. Any details relating to a security right, such as how much the borrower owes at a particular point in time to the secured creditor, may be discovered through off-the-record inquiries. Human intervention is precluded or minimal in accepting or rejecting a registration, or responding to a search request. Provided that required fields are populated, the registration should be immediately and automatically processed by a software application and made available to searchers.

Registrations integral to secured transactions include initial, amendment, and cancellation notices. Secured creditors may register amendments to their registrations for a number of reasons, including a grantor’s change of its identifier. Secured creditors may need to register a cancellation upon full satisfaction of the secured obligation and when they no longer owe any commitment to extend credit in the future. In order to maintain an auditable record of the priority and history of registrations, collateral registries follow an “add-only” policy under which records are added but never modified or deleted. On the registration of a cancellation notice or on expiration of the period of effectiveness, the initial notice and any associated notices will be archived and cease to be available to searchers. DLT is well suited to implement the “add-only” policy in a registry installation and may be designed to allow only certain records to be publicly “visible.”

Collateral registries are typically controlled by a central authority, such as a governmental body or a central bank. Within this context, permissioned DLT systems are more appropriate platforms for collateral registries than public (permissionless) DLT systems. A permissioned DLT system is more appropriate for collateral registries because a permissioned system enables the registry operator to determine which nodes can read the ledger and submit and validate registrations, thus ensuring the integrity of the data. A number of technical considerations also make permissioned systems more favorable for collateral registries. Most importantly, permissioned DLT systems can implement an efficient consensus algorithm because only a limited number of nodes are authorized to submit and validate new data entries or blocks, and the rules of the consensus algorithm can be designed to ensure that registrations are always added in the sequence submitted, with minimal delay. Moreover, because the identity of the persons responsible for these nodes is known, malicious actors can be identified, their permissions revoked, and legal action taken if appropriate. By contrast, in a typical permissionless DLT system, the persons responsible for a node are not generally known, though in some implementations it is possible to establish identity. Additionally, in a permissionless DLT system, such as Bitcoin, the collection of a new data entry, its addition into a block, distribution to the network and validation are energy intensive, time consuming, and subject to delays. For a collateral registry, a time lag between the moment when data is submitted and the time when it becomes accessible through a search is problematic as it would delay the time of perfection of a security right. Finally, in order to minimize the time and resources required to reach consensus, permissionless systems generally only store a limited amount of data for each transaction, such as the timestamp and a hash representing the digital address of the recipient.

1.2 SUFFICIENCY AND COMPLETENESS OF INFORMATION

A collateral registry cannot fulfill its core functions in a trustworthy and reliable manner unless the information in a notice that is displayed in a search result is sufficient and complete. This enables the searcher to continue its due diligence. Sufficiency of information determines the effectiveness of a registration, which is important particularly for identifiers of grantors according to which the registry record is indexed and searchable.
In order to facilitate an efficient registration process, without delay, and at minimal expense, legal frameworks governing the functioning of collateral registries place the obligation to ensure sufficiency and completeness on the registrant. The task of the collateral registry to ensure the sufficiency and completeness of information in a registration is limited to i) ensuring that required fields are populated; ii) recording the information in a notice as provided by the registrant; iii) timestamping the registration to record its effective time (the time that the registration became searchable and thereby established its priority) and reflect the sequence in which registrations are registered; and iv) storing the registration in a manner that preserves data integrity.\footnote{Note 1: Collateral Registry, Secured Transactions Law and Practice}

Validation processes to ensure sufficiency and completeness of data should be automated and limited to objective criteria, such as verifying that required fields are not blank and that data conforms to the expected format (e.g., the required number of letters and digits for a national ID of the grantor has been entered). Interoperability with other systems\footnote{Validation processes to ensure sufficiency and completeness of data should be automated and limited to objective criteria, such as verifying that required fields are not blank and that data conforms to the expected format (e.g., the required number of letters and digits for a national ID of the grantor has been entered). Interoperability with other systems} can improve the accuracy of information by providing functionality to assist the registrant. For example, in those systems that provide for serial-number indexing, the collateral registry may be connected to the motor vehicle registry to verify the accuracy of a vehicle identification number. In the future, one may envisage interconnections with other registry systems that maintain a record of owners/holders of digital assets. Interoperability may not require any specific provision in the substantive legal framework if it operates as a service to the registrant. This would be the case if verification of the grantor’s ID turns out to be incorrect as entered, but the registrant is nonetheless able to proceed with the registration if it wishes.

As mentioned above, ensuring sufficiency and completeness is a task for registrants. DLT does not eliminate the problem of “garbage in, garbage out” and thus would not ensure that any information submitted by the registrant is sufficient or even accurate. Collateral registry nodes would not verify the sufficiency or accuracy of the information entered. Completeness is already addressed by existing systems that are designed to automatically reject registrations with incomplete mandatory fields (e.g., missing grantor identifier) and could be easily implemented in a DLT system. Accordingly, DLT would not enhance the sufficiency of registered information and would ensure completeness in a manner similar to what is already achieved by electronic collateral registries using the existing technology.

\subsection*{1.3 AUTHENTICATION OF USERS AND PARTICIPANTS}

Most electronic collateral registries implement some processes to authenticate the prospective registrant.\footnote{As mentioned above, ensuring sufficiency and completeness is a task for registrants. DLT does not eliminate the problem of “garbage in, garbage out” and thus would not ensure that any information submitted by the registrant is sufficient or even accurate. Collateral registry nodes would not verify the sufficiency or accuracy of the information entered. Completeness is already addressed by existing systems that are designed to automatically reject registrations with incomplete mandatory fields (e.g., missing grantor identifier) and could be easily implemented in a DLT system. Accordingly, DLT would not enhance the sufficiency of registered information and would ensure completeness in a manner similar to what is already achieved by electronic collateral registries using the existing technology.} Authentication of the registrant reduces the risk of unauthorized or fraudulent registrations, but the process should not be such as to impose an undue burden on the prospective registrant. Modern collateral registries employ various authentication mechanisms, such as conditioning the establishment of user accounts to submit registrations electronically on providing information proving the identity of the prospective registrant. For example, the International Registry established pursuant to the Protocol to the Convention on International Interests in Mobile Equipment on Matters Specific to Aircraft Equipment verifies the user’s identity via a digital certificate issued by a certification authority using Public Key Infrastructure (PKI) technology.\footnote{Some nodes may be limited to the read-only permissions necessary to perform searches, other nodes may be authorized to validate registrations to be added to the ledger. The nodes with a permission to validate registrations may include the registry office and any other authorized intermediaries.}

This authentication process applies continuously as amendments and cancellations are registered and efficiently prevents a person from making changes to registrations submitted by other persons.

DLT incorporates cryptographic signing of transactions to authenticate registrants. As with non-DLT technology, permissioned blockchains may require users to be authenticated before being able to submit registrations to the collateral registry. In this design, the PKI technology inherent to the DLT ensures that the person submitting a registration can be identified.\footnote{Identification and authentication also enable the DLT system administrator to authorize different permissions for each node depending on the identity of the user and the established system policies.} Cryptographic signing of blocks authenticates registrants by proving that each person signing the registration had access to that person’s private key.\footnote{Identification and authentication also enable the DLT system administrator to authorize different permissions for each node depending on the identity of the user and the established system policies.}
In a DLT system, validation of registrations does not refer to the substantive accuracy or legality of the data entries that have been submitted by the registrant, but rather to their consistency and compliance with the relevant cryptographic rules. Each node with the necessary permission to participate in the consensus process independently verifies that each new data entry is cryptographically accurate regarding its originator and its consistency with entire ledger. A new data entry is added in the ledger only when the requirements established by the consensus protocol have been satisfied.

For collateral registries, the consensus rules would also ensure that registrations are added in sequential order. Secure timestamps recorded within each block when it is added to the ledger would establish the time of effectiveness of each registration. The sequential and append-only nature of DLT systems ensures that registrations are permanently recorded in chronological order. Non-DLT technology already ensures that registrations are i) added to the record only when submitted from an authorized user account; ii) timestamped; and iii) stored in a chronological order. The process of validation of the registration by authorized nodes would not differ from the non-DLT systems.

### 1.4 AUTHORIZATION

While registrations may be submitted without any required authorization, this risk may be reduced if secured transactions laws or regulations impose some design requirements. The International Registry requires electronic consent of the debtor, while the UNCITRAL Model Law contemplates the submission of amendments and cancellations through an authorized user account. In a DLT system, the consensus process can include validation of the identity of the registering entity by multiple (or even the majority of) nodes, thus reducing the risk of access to the system by unauthorized entities. Smart contracts may also be deployed to require consent of the parties to a particular type of registration, such as all secured creditors named in a single registration, before it is amended or cancelled. Any request by one of the secured creditors to cancel a registration would automatically alert the other persons named as secured creditors in the same registration whose consent would be required. Similarly, smart contracts can enforce the requirement for the grantor to confirm the registration, which would be the case in the International Registry. Such consent mechanisms might not be practicable to authorize an initial registration in a domestic registry because grantors, especially natural persons, might not have access to such technology or might not understand how it functions.

For any consent mechanisms to be designed into collateral registries, the law must provide for them. Presently, under the UNCITRAL Model Law, the collateral registry would have no authority to reject a cancellation submitted by one of the secured creditors, inquire as to whether the secured creditor obtained an authorization from the other secured creditors named in the same registration, or whether the grantor has authorized the registration. Regardless of the technology and design, the law should determine the effect of an unauthorized registration, or the effect of an amendment/cancellation submitted by one of the multiple secured creditors named in the same registration.

### 1.5 INTEGRITY AND SECURITY OF STORED DATA

Integrity of registry data rests on the administrator’s ability to ensure that stored data is not altered or destroyed in an unauthorized manner. The registry administrator must be able to preserve and restore data, despite natural or human-caused accidents and disasters, including technical failures of software or hardware. This requires a highly redundant registry system in which no single point of failure of a component, or entire datacenter, would result in the data being lost entirely.

The architecture of a collateral registry implemented on a non-DLT database platform is centralized. In the simplest design, only a single database is maintained. Even when multiple redundant database servers are configured, each server generally runs the same version of the software on the same platform using similar, if not identical, hardware. Recommended practices to mitigate the impact of an attack or disaster affecting a centralized system include real-time database replication to remote locations and periodic backups stored offsite, with multiple servers in several locations and automatic failover capabilities. The overall system, though geographically dispersed, lacks heterogeneity and remains vulnerable to errors and attacks that are able to propagate across the system.
DLT has several inherent features that align well with the requirements for security and integrity of stored data. These include i) tamper resistance; ii) a tamper-detection process of independent data verification; iii) a distributed and redundant system architecture; and iv) a network of heterogeneous nodes. Blockchains are often described as immutable, and while this is not accurate in the strictest sense, they are tamper resistant and tamper evident. The header of each block contains the hash of its own block data and the hash of the previous block’s header. Therefore, if the data contained in any block is altered, the resulting new hash changes the hash of all subsequent block headers. This enables tamper detection and rejection of blocks that have been tampered with. Any change in a stored block will be detected when the header of a block is verified before another block is added to it. Moreover, the integrity of every block can be independently verified by any of the network’s users.

The distributed nature of blockchain intrinsically creates redundant copies of data stored in multiple locations on independent systems with independent administration and security implementations. In the context of a collateral registry, a limited number of authorized nodes would fulfill this role. Thus a disaster affecting any single site has limited impact on the resilience of the overall network’s data-storage ability. The more spatially dispersed the authorized nodes are, the more robust the system will be in terms of protecting data from natural or human-caused disasters. Similarly, because the nodes may be independently owned and administered, the network is more resilient to internal or external attacks, human errors, and technical failures. This is because independent administrations may maintain data using different types of hardware, software, access control, and security measures. As a result, an attack that exploits a vulnerability of one administration may not succeed against another administration in the same distributed network.

Replication of new blocks to all nodes that maintain a copy of the ledger is integral to the consensus process and ensures that all ledgers are consistently synchronized. In this way, each participating node in the DLT network preserves its own continuously updated copy of the ledger, which it can audit independently of the registry administrator. In contrast to the central repository architecture of non-DLT collateral registries, DLT architecture is inherently more resilient and gives the participants the means to ensure the integrity of its data. However, non-DLT electronic databases underpinning modern collateral registries have proven to be resilient against tampering and efficiently preserve the data integrity.

Requiring the consensus of multiple nodes, in addition to the node that is the registry administrator, strengthens the validation process and facilitates transparency by enabling independent control of duplicate copies of the ledger. However, as compared to non-DLT registries, the time required to reach consensus and publish a new block delays the effectiveness of registration(s) contained in the new block.

Whereas the records stored in a DLT ledger are essentially immutable due to cryptographic links connecting each record to previous ledger entries, this is not the case in a non-DLT database. An inadvertent or malicious edit or deletion of a record in a non-DLT database, like any update to the data, is replicated from one server to another so that all copies of the data reflect the change. A DLT ledger reduces the risk that the entire system is compromised due to a failure of the centralized database, a phenomenon known as “single point of failure.” Yet such a risk cannot be completely averted; attacks that leverage administrative weaknesses, such as access controls, or exploit vulnerabilities of the particular software used by the system may propagate across an entire network.

### 1.6 SEARCHES - EASE OF ACCESS, SEARCH LOGIC, AND REAL-TIME AVAILABILITY OF INFORMATION

Ease of access and use of the search function, as well as the reliability of the search results are key to encouraging secured lending. A collateral registry’s search function should be easily accessible by all users without the need for special technical equipment, skills, or knowledge. Searches of a collateral registry are conducted according to a grantor’s identifier, which may be a name or some unique number as specified in the law. The law should also determine the official search logic applied to an identifier provided by the searcher to conduct a search; such logic may be either strict, returning only exact matches, or flexible, returning both close and exact matches. These legal rules dictate how the system is designed.
The searcher’s confidence in the search result rests on the integrity of the registry search function and the retrieved data. A search reveals records as they currently exist in the non-DLT database, with no guarantee of their integrity, other than the registry’s reputation for reliability and trustworthiness.

Because a registration is not effective until searchable, it should be searchable almost immediately after submission. Otherwise, the secured creditor may be exposed to a number of risks, such as losing its priority to another secured creditor or an insolvency trustee. Likewise, a collateral registry should return the results of a search almost immediately.

DLT can address some concerns about the reliability of the search results, the ability to maintain data, and trustworthiness of the registry administrator. For purposes of validating records, the DLT ledger need only store the hash of the data contained in the record. A positive result from a search of the DLT ledger verifies that the data in question is identical to the record hashed and stored in the DLT ledger. The searcher’s confidence in this search result rests on the intrinsic tamper-resistant nature of the DLT ledger rather than the integrity of the registry administration. The result of such searches may provide definitive information without the necessity to engage in further inquiry.

Blockchain is currently the most widely used type of DLT, largely due to its ability to securely store transaction data and transparently maintain their integrity. However, one of its weaknesses has been the inefficiency of searches to retrieve registrations. This is because a blockchain generally contains hashes of transaction data but not the raw data itself. This design minimizes the amount of data that must be transmitted to every node and stored therein. Searching a blockchain registry system to determine whether its DLT ledger contains a particular hash is very efficient. Thus, when the entire contents of a transaction are known, the corresponding hash for that transaction can be calculated and the blockchain can be easily searched for this hash – if the hash is found, the existence of the transaction data is confirmed. However, this feature is not helpful when searching for transactions involving a prospective borrower without knowing the hash of a pre-existing registration. By contrast, presently, data held in non-DLT databases can be indexed to optimize the legally required search logic, greatly increasing the speed and efficiency of searches in large datasets.

The solution generally suggested to resolve this issue is to store the metadata of the hashed transaction in a non-DLT collateral registry database with efficient search capabilities (e.g., using SQL queries). For example, when a transaction is hashed for storage on the blockchain, the resulting hash is also stored in a non-DLT database with transaction data such as the identifiers of the secured creditor and the grantor, description of the collateral, and time of the registration. Searches for registrations are then performed in this database, which also provides the hash (or pointer) required to confirm the integrity of the transaction data by pointing to the location of the hashed transaction in the blockchain. However, this type of solution leaves the searcher dependent on the integrity of the non-DLT database to discover the existence of any registrations, thus eliminating the benefit of addressing the risk of the single point of failure.

From the above it emerges that, in the context of searching collateral registries, though blockchain would offer benefits over non-DLT databases for ensuring the integrity of retrieved data, it does not enhance the integrity of the data that is actually searched since the search is conducted on a non-DLT database. Consequently, blockchain does not address potential errors or tampering in the non-DLT database that might prevent the retrieval of registrations when applying the search logic to the criteria entered by the searcher. This architecture entails the added costs of maintaining both a non-DLT database and a DLT ledger. Furthermore, if this architecture were to be implemented, the law is expected to provide that a search result in a non-DLT database determines the effectiveness of the registration. So any searches and results in a blockchain database would not have a legal effect, and that database would merely attempt to enhance the integrity of the data rather than affect its validity. Therefore, such an architecture may be designed already under the UNCITRAL Model Law. It may be useful especially in environments where the reliability or the ability of the registry administrator is questionable. If it were to be implemented, the legislator may need to clarify that searches in the non-DLT collateral registry database only would have a legal effect.

As DLT development advances, search capabilities are improving, and it should be possible to store larger quantities of data...
on-chain, enabling searches of the blockchain ledger by key fields, such as grantor identifier and a serial number. In this way, an initial search could be conducted against data stored within the blockchain and additional details of the registration retrieved from a non-DLT database.

1.7 INTEROPERABILITY WITH THIRD-PARTY SYSTEMS - PAYMENT SYSTEMS AND OTHER REGISTRIES

Interoperability enables registries and other systems to communicate with or transfer data directly between each other in an automated manner. As explained above, interoperability with other registries can assist registrants by providing correlating information that may alert them to an error in a registration before it is submitted, thereby improving the accuracy of the information. Examples include interoperability with i) a national ID registry or a business registry, to verify the ID of the grantor identified in a notice; or ii) a motor vehicle registry, to verify the serial number entered; or iii) an intellectual property registry, to verify ownership to a particular intellectual property right. Interoperability with a motor vehicle registry could also include automatically forwarding notice of a registration against a motor vehicle to that registry, which would associate it with the vehicle’s record of ownership. A similar gateway may be established between the collateral registry and a credit bureau. Federal, regional, and international collateral registries can be designed for interoperability with state collateral registries, enabling the federal, regional, or international collateral registry to immediately receive registrations accepted by state collateral registries. While this may be technologically feasible, a supporting legal framework is necessary to establish the legal effect for such registrations at these levels.

Interoperability has been a challenge for non-DLT systems, and it is also expected to remain a technological hurdle for DLT systems. Until the technology matures and common protocols are agreed, including between Ethereum and Hyperledger, it is unlikely that a DLT registry would be interoperable with other separately developed DLT registries or non-DLT systems without an off-chain interface. Future interfaces with registries for rights to digital assets may also enhance certainty of commercial transactions, but in the absence of such digital assets registries, it is challenging to visualize the actual operation of those interfaces and the legal framework that would give legal effect to such registrations.

Most collateral registries enable on-line payment of registry fees, which may include some level of interoperability with on-line payment systems. For example, for credit card payments, the user may enter credit card information that the collateral registry captures to collect payment. A collateral registry could also accept fees in cryptocurrency. In this scenario, the registry webpage may provide the customer with a unique cryptocurrency address to which the customer sends a payment from their cryptocurrency wallet. However, the law might need to be adjusted to allow the collateral registry to accept fees in such a form, which would also expose the administrator to the risk of value fluctuations if a significant majority of fees are paid in cryptocurrency presenting a high degree of volatility.

1.8 DLT-STCR REGISTRY VERSUS OTHER DLT REGISTRIES

Registrations and searches of motor-vehicle, land, business, and national ID registries have a different purpose than registrations and searches of collateral registries. For instance, the purpose of a search against a prospective borrower in a collateral registry is to discover whether any matching records exist, and then conduct further due diligence off the record, including whether the prospective borrower has rights in the collateral. A search of the land registry will reveal the titleholder as well as the actual document that was used to create an encumbrance. As explained above, the DLT ledger need only store the hash of the data, which, for instance, could relate to the proof of ownership to the land. The prospective creditor may then use the hash to conduct a search of the DLT ledger to verify whether the registry operator created that hash and then conduct a corresponding search of the land registry. The matching of the hash ensures that the land registry record has not been tampered with.
Blockchain-based land registry projects in Fiji, Georgia, and Sweden illustrate the benefits and desirable prerequisites of such efforts. Two key prerequisites that must be in place before integrating blockchain into a registry are i) a digital ID system to identify the parties to transactions; and ii) digitalized records. Both Sweden and Georgia had fully digitalized land registries before developing a blockchain solution. However, it appears that the “old process” continues in parallel and the blockchain data is not used in a meaningful way.

Sweden’s land registry authority, the Lantmäteriet, began developing a blockchain-based land registry in 2016 and two years later demonstrated a transaction on the blockchain pilot. Sweden’s pre-existing digital land registry and an existing digital ID solution enabled the relatively rapid development of the pilot project. Results demonstrated that the three- to six-month delay between contract signing and transfer of ownership could be reduced to hours. Lantmäteriet stores hashes of digital transaction records on a private blockchain. Unlike collateral registries, high speed and low latency are not high priorities for land registries. But, similar to collateral registries, security and transparency are. To this end, third parties affected by land transfer transactions, such as banks, buyers, sellers, and real estate agents, will be able to verify the hashes on the blockchain.

As in Sweden, Georgia’s land registry, administered by the National Agency of Public Registry (NAPR), was already digitalized before it began development of a blockchain-based application in 2016. NAPR converted its registry to a blockchain-based system in two phases. First, the existing non-DLT digital registry was anchored to the Bitcoin public blockchain through a third-party-distributed timestamping service that publishes the hashes of the land title records on the Bitcoin blockchain. This provides cryptographic proof of the date that each hash was stored and enables verification of the documents stored in the land registry, independent of any government agency or official, and establishes their provenance. This was important to alleviate any mistrust of government institutions or fears of internal tampering or external cyberattacks. In the second phase, initiated in 2017, a private (permissioned) blockchain registry was developed to store the digital land records. Again, as in phase one, hashes of the land title records are stored on the Bitcoin blockchain for independent verification of each record’s validity and provenance.

Fiji’s iTaukei Land Trust Board (TLTB) manages 92% of Fiji’s land, but unlike Sweden and Georgia, when TLTB began exploring a blockchain pilot for land records management in 2018, it did not have a digital registry or even a centralized land registry – records were kept at different offices and administered differently. Thus, initial efforts centered on digitalizing land records. The project’s primary goals were to reduce the risk of fraud and provide assurance to stakeholders through the transparency and security of a blockchain-based land registry. Transactions will be executed through smart contracts on a private (permissioned) blockchain. Permissioned users will include i) core public agencies (TLTB, Fiji Revenue & Customs Service, and Registrar of Titles); ii) auxiliary public agencies (Ministry of Land & Mineral Resources, Department of Agriculture, and Department of Town & Country Planning); and iii) private entities (e.g., banks and insurance companies).

1.9 SOME PROPOSED APPLICATIONS

Pilot programs have attempted to replicate certain features of collateral registries using DLT and smart contracts. These pilots focused both on the use of DLT for a database that stores registrations, as well as registry applications that can be accessed by registrants through smart contracts that define their terms of use. In Delaware, a permissioned blockchain database was envisaged to store immutable records of financing statements that would be additional to the UCC Filing Office record. This storage would be optional, and the users expected to pay a premium. Accordingly, the system was designed not to replace the traditional collateral registry database but to supplement it. However, Delaware has not yet implemented any blockchain applications for UCC filings.

Other external applications have been designed to keep track of individual receivables in a multi-lender scenario. The
participating lenders take a security right over the same package of receivables, but each finances only some. The application is designed for connection to the collateral registry to automatically update the collateral description in the relevant registrations as receivables are financed and collected. This allows for accurate allocation of the financed receivables among the multiple lenders, a task previously achieved by negotiating and effecting releases for individual receivables. Accordingly, a search of the collateral registry would reveal that receivables A, B, and C are subject to a security right of Bank 1, while receivables D, E, and F are subject to a security right of Bank 2. While this would enhance accuracy of the public record, its commercial value is questionable as interested searchers should in any case inquire with the banks (through the borrowers) as to whether the receivables are still owing and about other details of the secured transaction(s). The main function of collateral registries is to alert third parties rather than reveal accurate information. Such details are thus unnecessary to the searcher and, in any case, would quickly become obsolete, such as when the receivables A, B, and C are paid, they would be deleted from the public registry record, and new receivables G, H, and I added.

Another design contemplates tokenization of registrations, where the registration itself becomes an asset. The main value of this asset would be its priority, which may or may not relate to a particular security right. For instance, Banks 1, 2, and 3 have all taken a security right in assets of the same grantor. Bank 1’s security right has been extinguished, but its registration remains on record. A token representing that registration could be transferred to another secured creditor who would thus acquire the priority position of Bank 1 after it extends its own loan and satisfies the requirements for the perfection of a security right. It is questionable whether this functionality would be commercially desirable, and, in any case, it is likely that the relationship among the three banks would be governed by a subordination agreement. A diligent party should inquire with Banks 2 and 3 as to the existence and terms of such an agreement that might have altered the priorities reflected in the registry record where Bank 1’s token appears to be first in time, while in fact the subordination agreement gives the priority to Bank 2’s token. Furthermore, this effect may also be achieved under the current laws and using existing functionalities of electronic collateral registries when Bank 1 registers an amendment notice effectuating an assignment of its priority to another bank.
2. DLT AND SECURED TRANSACTIONS LAW AND PRACTICE

Different types of digital assets, including native tokens (e.g., Bitcoin) and non-native tokens (e.g., a token that purports to represent a right in an underlying tangible asset, such as a motor vehicle), are held in distributed ledgers. These may take the form of payment tokens (cryptocurrencies), fiat-backed or deposit-backed tokens, utility, security, or hybrid tokens. Digital assets are issued and used for a variety of purposes. While utility tokens are typically issued and traded for the purpose of granting access to goods and services, asset/security tokens are issued as an investment. A digital asset may also be hybrid, serving both as utility and security token; moreover, a digital asset originally designed as a utility token may evolve into either an asset or a payment token because of its market uses. The analysis in this part of the Guidance Note is generally agnostic as to the different types of digital assets, unless stated otherwise, but various additional legal aspects relevant to those particular digital assets should be taken into account when they are to be used as collateral.

Different considerations may also apply depending on the type of secured transaction, which could be i) an “all assets” deal; ii) financing of digital assets that frequently turn over similarly to inventory; or iii) a loan secured with one or a few identifiable digital assets held for investment purposes, whether the loan is provided to acquire the assets or secured with existing assets of the grantor. While in the first transaction digital assets may not even be included in the borrowing base against which the amount of the loan will be determined, in the latter two cases they could be the sole, or a significant, asset that the secured creditor relies on for repayment of the loan. However, in the first case the value of digital assets subject to a security right will increase recovery of the secured creditor in insolvency. The nature of the transaction may also have effects beyond the secured transactions law. For example, digital tokens sold on credit, or requiring purchasers to post collateral, may qualify as instruments regulated by the relevant authority, such as the Commodity Futures Trading Commission in the United States.

This part of the Guidance Note does not deal with “traditional assets” such as bills of lading and warehouse receipts that may be issued electronically, with the use of DLT or other technology. Neither is this part concerned with the provision of collateral in the form of digital assets in sophisticated financial transactions such as various forms of derivatives. The UNCITRAL Model Law, the provisions of which are examined below in the context of its application to digital assets used as collateral, neither provides for specific rules applicable to electronic negotiable documents nor applies to the use of collateral in derivatives.

This part of the Guidance Note examines various aspects of the substantive secured transactions framework and related laws that affect processes of secured lenders. These include the general property law and regulation of the classification of digital assets as objects of property or personal claims, statutes that may preclude the creation or transfer of a security right in a digital asset, and custody frameworks that may impose certain duties on intermediaries that hold digital assets for their customers. It also assesses the impact of insolvency law, particularly on the classification of rights of parties in insolvency of a custodian. The focus of this part is on the fundamental elements of a modern secured transactions framework, namely its scope, and the creation, perfection, priority, and enforcement of security rights, as well as conflict-of-laws aspects. In addition to analyzing the provisions of existing laws and identifying areas that may require modification of approach to facilitate the use of digital assets as collateral, this part also examines the impact of DLT on various processes of secured creditors, particularly in the context of enforcement, valuation, and monitoring of the collateral.

2.1 NATURE OF THE GRANTOR’S RIGHT IN DIGITAL ASSETS

A security right may be created in any right (or power) the grantor has in the collateral. The secured transactions law defers to other laws that determine the nature of the prospective grantor’s rights in the collateral and any restrictions that may be imposed on its transfer, including the ability to create a security right. Various laws and regulations may preclude the use of certain assets as collateral for a loan or affect the ability of the secured creditor to enforce its right upon default.
The UNCITRAL Model Law recognizes the existence and effect of those laws and regulations but does not modify their application.\textsuperscript{48} They may, for instance, treat what is the most valuable asset of a prospective grantor as some kind of privilege, rather than property (e.g., a restaurant liquor license), precluding the creation of a security right.\textsuperscript{49}

A digital asset may become the subject of a property right, including a security right, when the law recognizes it as an object of property. The grantor may be owner, co-owner, or have some other proprietary right in the digital asset. In both common law and civil law regimes, the specificity or identification of an asset is essential to its characterization as an object of property.\textsuperscript{50} In the absence of specific statutory guidance and where case law in this area is at its infancy, depending on the legal system and tradition, different aspects may be considered by courts to determine whether property rights could be established. Furthermore, different considerations may apply to different types of tokens. Where digital assets are recognized as objects of property rights, transfers of rights to those assets must be completed in accordance with the requirements of the applicable legal regime.

Different types of rights may be created upon deposit of a digital asset with a custodian. If the relationship between the depositor and its custodian is considered a regular deposit, the depositor retains property rights to the deposited object, such as corn in a warehouse. In contrast, if the relationship is considered an irregular deposit, the property right passes to the custodian, such as with respect to cash deposited to a bank account. If laws do not recognize that a digital asset may be the subject of a property right, the holder may have a personal claim to the digital asset. A security right would then be created in this personal claim to the digital asset. This claim may, for instance, be enforceable against an intermediary that may however be insolvent.\textsuperscript{51} As compared to the digital asset that is susceptible to being the subject of a property right, the secured creditor would be exposed to a higher risk when the right of the grantor is merely a personal claim to the return of digital assets from an insolvent intermediary. The consequences of this classification have far-reaching consequences, especially in insolvency of the intermediary (e.g., in the BitGrail Italian insolvency case).\textsuperscript{52}

In those legal systems where a statutory classification for digital assets is provided, that classification is generally applicable to that particular regime. For instance, under the U.S. laws, virtual currencies that are convertible into fiat currency are treated as property for tax purposes, whereas for regulatory purposes they may be treated as commodities.\textsuperscript{53} In the absence of a specific classification that would extend to the secured transactions law, secured creditors would take the risk of a judicial interpretation regarding whether a particular digital asset may be subject of a property right.

The recognition of a given asset as an object of property, nonetheless, does not ensure its unconstrained alienability. The transferability of some assets\textsuperscript{54} might be limited under laws and regulations adopted to effectuate different public policies. In a similar vein, the transfer of digital assets that are classified as financial instruments is likely to be subject to regulatory regimes governing securities and capital markets laws.\textsuperscript{55} Hence, transferring and enforcing property rights in these assets might require smart contracts or multi-signature wallets to be designed to ensure that transactions are compliant with applicable regulatory provisions, including an obligation to ensure that only qualified purchasers may acquire certain types of securities.\textsuperscript{56}

Some secured transactions laws may override the effect of restrictions imposed by other laws. For instance, UCC Article 9 renders any restrictions contained in the rule of law, statute, or regulation on the creation, attachment, and perfection of security interests (but not their enforcement) in certain types of collateral ineffective.\textsuperscript{57} States implementing the UNCITRAL Model Law should consider the effect of statutory restrictions when incorporating Article 1(6).\textsuperscript{58} Under the laws that do not override the effect of statutory restrictions, secured creditors should take restrictions into account, as they would preclude the use of a digital asset as collateral because the grantor may not have the necessary right or power to create a security right.

The preceding discussion reveals that the legal and economic effects of a transaction involving digital assets might be disjointed. Some administrators of DLT systems purport to allocate property rights to digital assets stored therein and regulate their transfers. They thus purport to provide a “notary function”, but without sufficient authority of the applicable law. A transfer of digital assets may not have any proprietary legal effect, including the perfection of a security right, unless it has satisfied the requirements of the law.\textsuperscript{59} For non-native assets where a ledger entry merely reflects rights created and transferred outside of the ledger, such as where A sells a motor vehicle to B, an entry in a ledger that is not maintained by
the relevant government agency will not be dispositive of rights to the motor vehicle. Furthermore, such a token would not even embody property rights to a motor vehicle. For native digital assets, including various types of tokens, the analysis may be different, depending on the framework governing the effect of transfers, as entries in ledgers may be dispositive, i.e., the transferee, including a secured creditor, acquires an interest in the token upon an entry in the ledger.  

2.2 COLLATERAL TYPES UNDER SECURED TRANSACTIONS LAWS

Secured transactions laws may classify assets into different types, to which different rules may apply. Secured transactions laws may thus classify digital assets as a type of collateral for their internal purposes. For instance, Article 2 of the UNCITRAL Model Law defines securities in a functional manner, as a result of which assets may fall under this definition that would not otherwise meet a definition of security under the applicable securities laws. In contrast, many other secured transactions laws define securities by a reference to the domestic securities laws, in which case any definition provided for the purposes of the securities laws, as well as its judicial and regulatory interpretations, would equally apply for the purposes of the secured transactions law. Whether a security token qualifies as collateral for the purposes of the secured transactions law may thus be determined by the secured transactions law itself, based on the characteristics and functions of the token, or by the applicable securities law.

Another example is money, which the UNCITRAL Model Law defines as “currency authorized as legal tender by any State”. Accordingly, some other law must be examined to determine whether the particular cryptocurrency may be money. The UCC definition does not require money to be authorized as legal tender; the test is sanction of the government authorizing it as official currency, thus potentially recognizing a broader range of currency as money. Acceptance of cryptocurrencies in satisfaction of some obligations owed to the government, such as taxes, would not amount to their authorization as legal tender. In contrast, the issuance of a cryptocurrency by the government, as in the case of Petro in Venezuela, or potentially by a central bank as a sovereign digital currency, commonly referred to as Central Bank Digital Currencies (CBDCs), would qualify as a legal tender.

A physical wallet used to carry coins and bills has some parallels to a digital wallet. Losing a physical wallet is similar to losing a private key required to access a digital wallet – in both cases, the holder may not be able to access the cash or digital assets. In contrast, a person who forgets a password to access an online bank account may relatively easily reset it.

Regardless of whether some cryptocurrency meets the definition of money, secured transactions laws include priority rules that essentially limit the breadth of that classification to money in tangible form. Article 48 of the UNCITRAL Model Law establishes that a transferee who obtains possession of money takes it free of any existing security right. In other words, even if some other law defined money to include cryptocurrency as legal tender or currency in a State, the relevant priority rule of the UNCITRAL Model Law, if enacted by the State as such, would not be applicable because it depends on possession of money, which, as explained below, applies only to tangible assets. Accordingly, without a specific “takes free” priority rule applicable to cryptocurrency, including CBDCs, the protection given to possessors and transferees of physical money would not apply to cryptocurrency. Policy questions with respect to granting the status of “money” to all types of virtual currencies should be considered, as the policy reason for providing such protection to any virtual currencies needs to be articulated, as such protections would elevate virtual currencies issued by private entities to the status of government-issued money.

Since cryptocurrency would not meet the definition of money, one may consider its classification as a right to payment of funds credited to a bank account. Though the UNCITRAL Model Law does not define this particular asset class, it provides a definition of a bank account as “an account maintained by an authorized deposit-taking institution to which funds may be credited or debited”. For cryptocurrency to be classified as funds under the UNCITRAL Model Law, they must be maintained in some form of an account and by an authorized deposit-taking institution. Whether the financial institution is authorized to take deposits and whether dealing in cryptocurrencies must comply with regulatory requirements are matters that rest outside secured transactions law and pertain to domestic and international regulatory regimes. If such regulatory authorization exists, and wallets or other mechanisms of digital storage are treated as bank account – provided that the cryptocurrency is capable of being credited to and debited from such an account – then all the elements of the definition
Note 1: Collateral Registry, Secured Transactions Law and Practice

will be satisfied. However, this definition effectively precludes classification of cryptocurrency as funds if the “account” is held by an entity other than an authorized deposit-taking institution. This may not be the case under some other secured transactions laws, such as UCC Article 9, that may simply require the bank to be engaged in the business of banking. The definition of bank account thus imposes a number of requirements that a cryptocurrency must satisfy to be classified as a right to payment of funds credited to a bank account.

Some secured transactions laws not only provide flexible definitions of asset types for the purposes of those laws, but may also allow some flexibility for the parties to arrange their relationship in a manner that would affect the classification. This is the case of the UCC Articles 8 and 9, under which a digital asset may be classified as a financial asset if the securities intermediary undertakes to hold it as such, i.e., it credits the digital asset to a securities account. This opt-in to the UCC Article 8 scheme, however, requires that a third party qualifies as a securities intermediary that maintains a securities account to which financial assets may be credited. This may be challenging for custodians of digital assets even though the UCC Article 8 definition is not limited to brokers, banks, or regulated entities. Otherwise, the digital asset would be classified as a general intangible. However, this ability to affect the classification by an action of the parties is far from a universal approach to the classification of assets under secured transactions regimes and would not be available under the UNCITRAL Model Law.

The collateral type classification will dictate the nature of the rights against, and obligations of, the issuer of digital assets, which is especially important for security and utility tokens. Some of these may be addressed in the applicable specialized laws, for instance, the liability of issuers of securities, which are then supplemented in a secured transactions law. The UNCITRAL Model Law, in Chapter VI, provides for the rights and obligations of third parties, but limited to specific classes of assets: debtors of receivables, issuers of negotiable instruments and negotiable documents, banks that maintain bank accounts, and issuers of non-intermediated securities. If a digital asset is not classified as one of these types of asset, the UNCITRAL Model Law does not provide supporting rules delineating the rights and obligations of issuers in relation to the secured creditor and the grantor. Other laws also determine the nature of rights and obligations of certain third parties, such as bailees that issue negotiable documents, but no similar statute may have been enacted addressing the rights and duties of issuers or custodians of digital assets.

An asset is classified under the secured transactions law according to its use. For instance, a motor vehicle may be consumer goods, equipment, or inventory depending on its use and by whom it is held (e.g., held as inventory offered for sale by a dealer). Generally, the asset type established at the time of entry into a secured transaction (creation) is not impacted by any subsequent change in use. Accordingly, a security agreement and a notice that describes the collateral as “all inventory” would perfect the security right even if the dealer starts using a car held for sale (inventory) as a loaner car (equipment). Digital assets may also undergo a transformation in their type. For instance, a token is initially issued for investment (security), but subsequently the issuer alters the rights embedded thereunder so that its nature ceases to be an investment and becomes a general intangible from which the holder may derive some other benefit. The laws may contain a specific provision on the time of classification that is limited to goods and not applicable to intangible assets. In the absence of a specific statutory prescription, the same principle should apply to intangible assets, including digital assets.

### 2.3 CREATION

A security right becomes effective between the grantor and the secured creditor upon creation. To become effective against third parties (perfection), a further step is required. As a general rule, Article 6 of the UNCITRAL Model Law provides that the creation of a security right requires a written agreement signed by the parties that identifies secured creditor and grantor, and reasonably describes both the secured obligation and the encumbered asset. The grantor must have a right in the asset to be encumbered or the power to encumber it. A written security agreement is required unless the secured creditor is in possession of the collateral. Since possession is defined in reference to a tangible asset, a written security agreement will be necessary to create a security right over a digital asset. Some jurisdictions also recognize control as a substitute for a security agreement, which is not the case with the UNCITRAL Model Law.
As explained above, secured transactions laws facilitate the taking of security rights in whatever rights (or power) the grantor has in the collateral, whether proprietary or contractual. For instance, the grantor may own a motor vehicle or have a right to damages for a breach of a contract. Both of these constitute assets for the purposes of a secured transactions law.

The general requirements for the description of the collateral in a security agreement as well as a registered notice would equally apply to digital assets. The secured creditor may thus describe the collateral as “all assets”, “all intangible assets”, “all digital assets”, or “all cryptocurrencies” or specifically identify the digital asset(s), all of which may be sufficient descriptions. However, some descriptions may not adequately identify all the relevant digital assets intended to be used as collateral, such as where certain tokens may not be technically classified as “cryptocurrencies” and thus not covered by that description. Some more specific and technical identification may need to be included if the collateral is a specific digital asset that must be further distinguished from other digital assets of the grantor that are not subject to a security right. For example, a security agreement and a notice may need to indicate a Bitcoin address.

A digital asset might be created and issued subject to contractual restrictions that limit its transferability and use as collateral. Article 13 of the UNCITRAL Model Law provides that stipulations of this nature affecting a receivable do not prevent or void the creation of a security right in these assets. Similarly, pursuant to Article 15 of the UNCITRAL Model Law, a security right in a right to payment of funds credited to a bank account will be effective irrespective of any agreement limiting the grantor’s right to create a security right. However, these provisions are crafted narrowly and will only apply to digital assets in the circumstances in which they qualify as receivables (e.g., tokens that are representations of receivables) or funds in bank accounts. The UNCITRAL Model Law overrides the effect of such contractual restrictions with respect to a narrower category of assets as compared to UCC Article 9. Any restriction on the transfer of a token that is in fact a receivable would be overridden by both regimes, but a restriction on the transfer of a general intangible asset would be overridden only under the latter regime.

A security right may be created in digital assets as original collateral or proceeds, such as when a security right is taken in inventory that is sold by the grantor for a cryptocurrency. The definition of proceeds in the UNCITRAL Model Law is broad enough to encompass any digital asset. For a security right to automatically extend to proceeds, they must be identifiable, which may be a concern for digital assets if they are commingled. Article 10(2) of the UNCITRAL Model Law provides for an exception from the identifiability requirement that is, however, limited to money and funds to which the lowest intermediate balance rule will apply. Since digital assets may be neither money nor funds, they must remain identifiable for a security right to automatically extend to them as proceeds.

### 2.4 METHODS OF PERFECTION - REGISTRATION AND POSSIBLE ALTERNATIVES

A security right is not perfected until the secured creditor has taken an action that typically involves some form of public notice, such as registering a notice or taking possession of the collateral. Secured transactions laws also recognize additional methods, including perfection by control, automatically, and by temporary means. Some of these methods may be applicable only to particular types of asset, such as control over deposit accounts, while registration may be generally applicable. The legal nature and classification of digital assets, as well as the categorization of collateral types in the applicable secured transactions law, determine which method(s) may be used to perfect a security right in the particular digital asset. Finally, the application of a method of perfection may also depend on whether a security right is taken in a digital asset that is original collateral or a security right is taken in some asset, such as equipment that is sold for funds deposited into a bank account (proceeds) that are used to acquire a digital asset.

### 2.5 PERFECTION AS TO ORIGINAL COLLATERAL

The following paragraphs examine only registration and control, which are the methods most likely to apply to perfecting security rights in digital assets. Automatic and temporary perfection have some application in specific contexts. For instance, a security right in inventory perfected by registration would automatically continue in any identifiable cryptocurrency paid to the seller of the inventory. Temporary perfection could play a role under the circumstances covered by Article 23 of the
UNCITRAL Model Law where the grantor moves from a State where a security right was properly perfected to another State. Possession may be generally excluded as a method of perfection since it applies to tangible assets only, at least under the UNCITRAL Model Law.86

Digital assets do not have a tangible nature even where a token might have been issued as representation of some tangible asset. Digital assets are stored in hot or cold wallets, which raises the question of whether transferring a right to access the wallet could be equated to delivery of constructive possession under the applicable law. Holding keys to a car would not convey property rights over the car itself, and their delivery to a secured creditor would not amount to possession under the UNCITRAL Model Law, though that may not be the case under other legal regimes.87 The key to a digital asset is much more intertwined with the asset itself as without it the asset may not be accessed, while a car can be repossessed and disposed of without its key, which may be replaced. However, holding a private key to access the cold wallet in which the digital asset is contained would not be equated to possession of the asset itself under the UNCITRAL Model Law.

Registration is generally applicable to security rights in any type of asset under the UNCITRAL Model Law,88 while under some regimes, it does not perfect a security right in all types of movable assets.89 Accordingly, under these regimes (e.g., UCC Article 9), registering a notice covering an account in which some cryptocurrency is held, as long the account holding the cryptocurrency qualifies as a deposit account, would not perfect a security right in the cryptocurrency taken as original collateral. Registering such a notice would perfect a security right under the UNCITRAL Model Law.

Conclusion of a control agreement is a perfection method that is not generally applicable to security rights in all types of assets. Under the UNCITRAL Model Law, the secured creditor may take control over a deposit account or non-intermediated securities, i.e., those held directly and not through an intermediary. Control is also a recognized method of perfection for security rights in intermediated securities under the laws that govern security rights in such assets.90 Accordingly, classification of digital assets as a type of asset will determine whether perfection by control is available. If the digital asset is not classified as one of those types, taking the mechanical steps to achieve control would not perfect a security right, though the secured creditor may obtain some undertaking of the issuer to abide by the instructions of the secured creditor pursuant to some control agreement or have the digital assets transferred to its own wallet. As mentioned above, the definitions in the secured transactions law or some other law would determine the available perfection methods with respect to particular types of digital assets.

A legislative action would be required to extend the control method to security rights in digital assets. In the United States, the National Conference of Commissioners on Uniform State Laws promulgated the Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Businesses Act (URVCBA) to enable the use of virtual currency as collateral, with respect to which, security interests may be perfected similarly to securities accounts subject to UCC Article 8. Control is defined in the Act as the “power to execute unilaterally or prevent indefinitely a virtual-currency transaction.” Official Comment 5(a) to URVCBA explains that “as a policy matter, it is preferable for the perfection and priority scheme for investment property rather than general intangible to apply to the virtual-currency account.” An Official Comment also states that the classification of virtual currency as a financial asset should not determine its characterization for the purposes of other laws, especially the regulation of commodities and securities.91

### 2.6 PERFECTION AS TO PROCEEDS

Article 19 of the UNCITRAL Model Law provides for the automatic perfection of a security right in proceeds of the collateral but distinguishes between two situations. On the one hand, a security right remains continuously perfected when the proceeds are in the form of money, receivables, negotiable instruments, or bank accounts. These types of asset are commonly referred to as “cash proceeds”. On the other hand, a security right in proceeds that are not one of the four mentioned types remains perfected only temporarily (e.g., 20 days after they arise). If a digital asset is received by the grantor, upon disposal of the collateral, its classification would determine whether the perfection is continuous or limited. All types of proceeds, however, must remain identifiable.
2.7 PRIORITY CONSIDERATIONS

The preceding Section highlighted the importance of classification of digital assets for the determination of the applicable perfection method(s). Such classification is also critical in determining the applicable priority rules, both in the context of conflicts between competing secured creditors as well as for transfers of digital assets to third parties subject to security rights. The consequence of this classification is that the rules pertaining to the various types of collateral will allocate the priorities between competing security rights, as well as establish whether transferees acquire their rights subject to or free of the security right. The following paragraphs examine these situations separately within the context of temporal and non-temporal priority rules. An example of a temporal priority rule is the first to register, such as under Article 29 of the UNCITRAL Model Law, while an example of a non-temporal rule is Article 47 of the UNCITRAL Model Law, which gives priority to perfection by control agreement over an earlier-in-time registration.

As explained above, the only method of perfection for digital assets that are intangible assets is registration under the UNCITRAL Model Law. Accordingly, the first secured creditor to register would have priority. Digital assets are not the types of asset that may be subject to an acquisition security right (also known as a purchase money security interest) that gives their holders priority over earlier perfected security rights, so this set of rules is inapplicable. Acquisition security rights may be created in tangible assets, intellectual property rights, and their licenses, which digital assets are not. As stated above, digital assets may also be proceeds of some other collateral. The priority of a security right in proceeds is generally the same as the priority of the security right in the original collateral from which the proceeds arose.

The analysis is different if the digital asset is a deposit account or a non-intermediated security, which would trigger the application of non-temporal priority rules that allow a later-in-time secured creditor to take priority. The other rules generally applicable to security rights in intangible assets, such as the freedom given to the parties to alter their priority through a subordination agreement, remain applicable.

Many digital assets have been designed to emulate the features of “real world” assets, such as money and securities. The value of these assets is enhanced by the protection given to transferees that balances the interests of secured creditors. Money and securities have been traditionally negotiable, allowing their transferees to cut off any rights and claims of third parties, including the secured creditor upon satisfaction of certain conditions, such as taking possession of money without knowledge that the transaction violated the rights of the secured creditor. The lack of such protections for transferees of digital assets impedes their transferability and affects their value. See Box 2 for an example of the due diligence requirement this imposes on transferees.

Transferees would be protected if, for instance, digital assets were classified as money or a non-intermediated security under the UNCITRAL Model Law, investment property, or after adoption of a specific legislative solution with the appropriate taking-free rule. Laws would have to be amended to superimpose a negotiability regime on digital assets for them to become functional equivalents of, for instance, investment property. In the past, secured transactions laws have been amended to facilitate particular financing products that entailed providing electronic equivalents of tangible assets with comparable strong transferability. For the moment, the rights of secured creditors won’t be affected by transfers unless the secured transactions law requires the secured creditor to register an amendment notice to identify the transferee within a specific period of time or the digital asset is acquired by a person located in another State.
Company A buying Bitcoin from Company B would not benefit from the priority given to transferees of funds from a bank account or money under Articles 47 and 48 of the UNCITRAL Model Law over a creditor that has a security right in the Bitcoin. Instead, Company A should conduct due diligence and search the relevant collateral registry to discover any encumbrances created by Company B. Furthermore, Company B might have acquired the Bitcoin from Company X, which itself could have potentially created a security right perfected by registration. That security right might not be extinguished upon sale of the Bitcoin to Company B. Therefore, Company A should conduct due diligence against not only Company B but any predecessor in title that might have created a security right that could still be effective, though it may have difficulties identifying any prior transferors to be able to conduct its due diligence effectively.

2.8 ENFORCEMENT

Upon default of the debtor, the secured creditor may enforce its rights through judicial means, or, where the law does not preclude it, extra-judicially. The latter method of enforcement is more efficient and promoted in Chapter VII of the UNCITRAL Model Law. This Section examines two aspects: i) enforcement of security rights in digital assets used as collateral; and ii) the use of DLT to facilitate enforcement of security rights in “traditional collateral,” such as motor vehicles.

A borrower, through a lending platform, sends its digital assets to the collateral wallet of a secured creditor to secure the repayment of a loan. The secured creditor can be either the lending platform itself or a third party, in which case the platform may act as a custodian of the collateral. The collateral wallet may also have the capability to automatically satisfy the secured obligation through a smart contract. For example, in the event that the loan-to-collateral value ratio dips below a certain threshold, the collateral is automatically liquidated.

A secured transaction will entail a different enforcement mechanism when no custodian is involved, such as when the digital asset is deposited directly into a wallet of the secured creditor. However, the process for automatically liquidating the digital assets upon the occurrence of certain conditions may apply.

The preceding two scenarios assume that the secured creditor properly perfected its security right, such as by registration, and in addition requested a deposit of the encumbered digital assets into a collateral wallet. Alternatively, if the secured transactions law recognizes control for the perfection of security rights in such assets, deposit of digital assets into a wallet may suffice.

A third possibility is when the secured creditor perfected by registering a notice without taking any other action to facilitate enforcement. In this case, it will need to identify the relevant collateral and demand its surrender, relying on cooperation of the grantor. Surrender of the collateral in custody of a third party may require a court order similarly to enforcing a security right in a bank account perfected by registration.

a. Extrajudicial Remedies

Where the secured creditor decides to dispose of the collateral without applying to a court, it must act in a commercially reasonable manner and satisfy certain requirements. The secured creditor who simply perfected by registration may face certain challenges in enforcement because it must rely on cooperation of the grantor to virtually repossess the digital assets that may be, at the time of default, in the grantor’s wallet. In the absence of cooperation, the secured creditor may need to obtain a court order. Accordingly, it may be more efficient, in addition to registration, to also procure delivery of the digital
assets to the secured creditor’s wallet or to that of a designated agent. The steps that a secured creditor would want to take to facilitate enforcement may also depend on the nature of its grantor’s business, which may actively trade digital assets, making delivery to the secured creditor’s wallet impracticable.

Once the secured creditor controls the digital assets, it would proceed to their disposal, a process that includes giving notification of its intention to dispose of the collateral to the parties entitled to that notification (e.g., the grantor and the debtor). Article 78(8) of the UNCITRAL Model Law provides for an exception from the notification requirement where the collateral may speedily decline in value or is of a kind sold on a recognized market. Arguably, digital assets may speedily decline in value, and, when traded on platforms, those platforms may be recognized markets for the purposes of applying this exception. Despite these exceptions from the notification requirements, commercial reasonableness would also include providing a time period, before the collateral is eventually disposed of, during which the grantor may redeem the collateral or a senior secured creditor may take over the enforcement process. As such, a smart contract enforcing the security right automatically upon the debtor’s default, whether the collateral is held with a custodian or in the secured creditor’s wallet, might not be enforceable if it violates the grantor’s or third parties’ rights. The grantor and debtor may waive their rights, but only after default.

Digital assets may be disposed of in a public or private sale. Public auction may not be commercially reasonable since a digital asset is expected to attract a higher value when sold on a specialized exchange. The requirements to enforce a security right in a digital asset that is an intermediated security will be lower than those applicable to non-intermediated securities.

Instead of disposing of the collateral, the secured creditor may also propose to accept the collateral in satisfaction of the secured obligation. To use this remedy, the secured creditor must send a proposal to the parties entitled to receive it, including the grantor and the debtor, but, unlike in the case of a disposition, there is no exception from the notification requirement, and the parties must be given a reasonable period of time to send their objections or acceptances. As with the disposal, automated enforcement would be precluded under the UNCITRAL Model Law, which aims to protect the rights of the grantors and other parties.

No notifications or time periods are required for collection of the collateral. However, this remedy may be enforced only against particular types of collateral, namely, receivables, negotiable instruments, deposit accounts, and non-intermediated securities. As explained above, digital assets would most likely be classified as general intangibles (under UCC Article 9) or intangible assets (under the UNCITRAL Model Law), with respect to which this remedy is not available. However, this is the type of remedy for which automated enforcement through smart contracts would be suitable, at least with respect to some types of digital assets that embody payment obligations. Without a change in the applicable secured transactions law, the secured creditor would need to proceed as if enforcing its security right in an ordinary intangible asset. In contrast, perfection by control, such as where the digital assets are delivered to a wallet of the secured creditor or that of its agent, would allow for swift enforcement.

b. Judicial Remedies

There are many circumstances that may leave the secured creditor with no other option but to enforce its rights judicially, such as when the grantor objects. The situation is more complicated when the secured creditor has perfected by registration, as it will need to identify the relevant digital assets to enforce against. If the digital assets are held in the secured creditor’s or custodian’s wallet, there may still be a need for a court order, but the process will be easier than in a situation where the digital assets are held in the grantor’s wallet. A court order may also be necessary to enforce a security right in a Central Bank Digital Currency (CBDC), especially when it is held in an account with the central bank. If the secured creditor knows where the digital assets are held (e.g., with a custodian), it may apply for an asset-freezing order. If it does not, it will have to rely on the grantor’s cooperation, which may not be forthcoming. Accordingly, a good practice would dictate that the secured creditor not only perfect its security right but also put itself in a position to be able to practically enforce its rights, such as by having the grantor deposit the digital asset into a collateral wallet. Otherwise, the relative ease of transferring digital assets could expose the secured creditor to a number of risks.
2.9 DLT AS A FACILITATOR OF ENFORCEMENT

DLT can facilitate the enforcement of security rights in traditional collateral, such as machinery and motor vehicles, due to its potential to improve the current processes for tracking, assessing the value, and recovering the collateral.\(^\text{111}\) In the case of motor vehicles, both floor-plan lenders and lenders providing traditional auto loans to consumers can benefit from the tracking enabled by DLT. For instance, floor-plan lenders could track lot sales that affect the borrowing base and be able to determine when any proceeds from the sale were generated.\(^\text{112}\) The purchase could trigger a smart contract that would result in an automatic payment from the dealer to the lender, reducing the loan balance. This tracking capability will reduce the risks of dissipating proceeds, since the floor-plan lender will no longer have to rely on the dealer’s notification about sales.\(^\text{113}\)

DLT could also be used by secured creditors to obtain a more accurate assessment of a vehicle’s condition.\(^\text{114}\) This could be possible if third parties and the driver input relevant data into a DLT ledger.\(^\text{115}\) Information regarding maintenance, repairs, and vehicle condition would be linked to the vehicle’s unique identifier, and secured creditors could use this information to more accurately assess the value of a used car before taking an enforcement action. Such centralization of the relevant information would also stimulate the formation of secondary markets or enhance the efficiency of existing ones.\(^\text{116}\) Finally, the recovery of motor vehicles from grantors can also be facilitated by DLT. A smart contract could be programmed to automatically disable the vehicle upon default, but likely without triggering the application of the relevant provisions of secured transactions laws on repossession because this action would not amount to repossession.\(^\text{117}\) Nonetheless, such immobilization should be effectuated in a reasonable manner, so as not to expose the grantor to danger by, for instance, disabling the car at an intersection. Some States (e.g., California and Colorado) expressly provided for “electronic self-help” in their legislative frameworks.

It should be noted that lenders have been using “traditional technology” for some of these processes, such as starter interrupt devices to disable a vehicle, for years.\(^\text{118}\) It is unclear whether some of these processes may be executed only through DLT, whether DLT enhances their efficiency, makes them more available, or simply provides an equally viable alternative.

2.10 CONFLICT-OF-LAWS REGIME

Parties to a secured transaction must be able to determine which law applies to the creation, perfection, priority, and enforcement of the security right. Most secured transactions do not involve “foreign elements,” such as the collateral being located in a country that is different from the location of the grantor. However, commerce is becoming increasingly international, which emphasizes the importance of predictable and clear conflict-of-laws rules.\(^\text{119}\) These issues are of significant importance for assets that may easily be acquired and transferred to persons located in different jurisdictions.

This Section is limited to some issues of law applicable to perfection of security rights in digital assets.\(^\text{120}\) Most secured transactions laws provide for the general rule of \textit{lex rei sitae} to determine the law applicable to the perfection of security rights in tangible assets.\(^\text{121}\) Rights to a tangible asset, such as a computer or mobile device, may be transferred in accordance with \textit{lex rei sitae} at the time of the transaction (\textit{lex situs}), but the same choice-of-law solution would not apply to digital assets stored in that device, as that would conflate distinct tangible and intangible assets.\(^\text{122}\)

For security rights in intangible assets that do not have any physical representation, the law of the location of the grantor governs perfection under the UNCITRAL Model Law, though some regimes may apply alternative connecting factors, such as the law governing the contract between the debtor of the receivable and the grantor. The UNCITRAL Model Law and modern secured transactions laws also provide for special rules applicable to bank accounts, securities, intellectual property rights, and other assets.\(^\text{123}\) The issues of determining the applicable law compound in a DLT environment for different types of assets, native and non-native tokens, and different types of ledgers, permissioned and permissionless. The analysis is also affected by the nature of the custodial arrangement where a third party may be holding the digital asset itself or access rights to a wallet in which digital assets are stored as well as the regulatory treatment of the different types of tokens that may determine their classification as a specific type of collateral. Finally, some regulatory regimes, such as those applying to security tokens, may determine the classification of the token under the secured transactions law and thus the applicable connecting factor.
Many native digital assets are created and held in a DLT environment governed by a set of rules agreed to by the participants that may include a choice of law. However, such a selection will generally not be enforceable when it purports to determine the law applicable to the proprietary aspects of transactions with those digital assets. Instead, and assuming the absence of rules specific to native digital assets in secured transactions laws, some of the following rules may apply depending on the classification of the digital asset:

i) the law of the location of the collateral may apply if the applicable law recognizes that some physical representation of the digital asset, such as the flash drive on which the access right to a wallet is stored, or a printout of the password to a wallet, is the asset itself;
ii) the law of the location of the grantor where the digital asset would be classified as a general intangible asset; or
iii) the law selected in an agreement between the grantor and the intermediary/depository bank, or the location of the intermediary/depository bank where the digital asset is classified as a security or a bank account. For the last category, one would need to distinguish between securities held directly and those held through intermediaries, as laws provide for the application of different connecting factors to security rights taken in these two categories of securities. Furthermore, a security token may need to be classified as debt or equity, as the law may provide for different connecting factors.

Statutory solutions may need to be fashioned to consider a specific connecting factor for various types of digital assets. For instance, for those held in permissioned and centralized ledgers, it may be the law of the administrator or operating authority of the ledger. For other types of ledgers, it may be the law of the location of the grantor or the law chosen by the parties that governs the custodial arrangement. Given the variety of digital assets, a single legislative solution may not suffice. Furthermore, a legislative solution may need not be limited to security rights in digital assets but may consider more broadly the nature of those assets and the proprietary effects of transfers, including the law governing the rights of transferees.

2.11 ROLE OF INTERMEDIARIES

DLT emerged as a mechanism to disintermediate various relationships. Payments were expected to be completed between the originator and beneficiary directly, and transfers of securities would not need to involve a securities intermediary/custodian. In transactions where digital assets are used as collateral, intermediaries may play a role as custodians holding digital assets or keys to access them, including in hot or cold storage. Certain custody arrangements are more complex, utilizing the services of a sub-custodian. The technological complexity associated with digital assets increases the complexity of custodial arrangements and thus legal complexity. Furthermore, the industry has been plagued by high-profile hacks that resulted in losses for investors, raising questions about the security of custodial arrangements and adequate legal safeguards for clients of custodians. Currently, custodians only provide services with respect to a limited number of digital assets and may not have the capability to hold cash for a client.

The legal framework governing the duties of intermediaries/custodians has been designed to apply to particular types of assets, such as securities or financial instruments, which would not generally cover digital assets or would only cover some of them (e.g., security tokens). As explained above, some exceptions exist, such as under UCC Article 8, where a digital asset may be a financial asset credited to a securities account maintained by a securities intermediary. The holding of digital assets by third parties raises issues similar to those for holding securities, especially with respect to protecting the customers of custodians. In the absence of a specific statutory framework governing custody relationships, customers’ rights and custodians’ duties would be established in agreements; however, applicable general law may alter the effect of such agreements. Legislative efforts are emerging to regulate these relationships to provide for certainty and protection of customers, such as under the URVCBA, which is, however, limited to virtual currencies.
Note 1: Collateral Registry, Secured Transactions Law and Practice

Box 4: Illustrative Custody Arrangement

The following operational details emerged during the BitGrail insolvency before the Court of Florence in Italy. Cryptocurrencies (Bitcoin, ETH, and Nano) deposited by users to their wallets were not stored therein but moved into a centralized BitGrail address through a script. Every night, this script would collect all cryptocurrencies from the individual wallets and transfer them to BitGrail’s centralized hot wallets (one per different type of cryptocurrency). Cryptocurrencies were at the disposal of BitGrail for purposes of managing their withdrawals or purchases and sales between different cryptocurrencies. These centralized wallets were controlled by BitGrail’s code or by those holding private keys, who were the owners of BitGrail. Users did not have private keys, meaning that, without logging onto BitGrail’s website, users could not carry out any transactions. The expert witness made an analogy with a bank account holder who cannot withdraw funds if the bank branches are closed, its website does not work, and debit or credit card services are not available. The expert witness concluded that, since all cryptocurrencies were held in a centralized account, in the event of a shortfall, it would be impossible to establish the number of cryptocurrencies owned by each user, as they were not segregated by the individual user.

Uncertainty exists with respect to the application of existing custodial frameworks to digital assets held by intermediaries. For instance, legal and regulatory frameworks may require custodians to implement certain safeguards when they hold money for clients. However, since cryptocurrencies would not meet the definition of money in these frameworks, such as the U.K. client money rules, the custodians would not be required to implement the relevant safeguards. In contrast, the European Securities and Markets Authority (ESMA) regards holding of private keys on behalf of clients as “safekeeping services so that rules to ensure the safekeeping and segregation of client assets should apply to the providers of those services.”

The U.S. Securities Exchange Commission in 1972 adopted the Customer Protection Rule with the objective of providing safeguards regarding the custody and use of customer securities. Under the Rule, custodians must maintain possession or control of fully paid securities of their customers. When a digital asset meets the definition of security, holding a private key in a cold storage may be equated to holding possession of actual security certificates. Holding a private key in hot storage may in turn satisfy the requirement to hold a security in a digital storage medium or system. Control means that the broker-dealer holds the securities in one or more locations specified in Rule 15c3-3(c). However, no guidance has been issued on how a broker-dealer may satisfy its duty with respect to custody of tokenized securities. Rule 206(4)-2 under the Investment Advisers Act of 1940 provides for certain safekeeping requirements that apply to funds or securities held on behalf of clients by registered investment advisers. Again, it is uncertain whether the Act would apply to the custody of digital assets. Even when custodians hold unregulated digital assets, a certain regulatory framework may be applicable based on the nature of their activities.

The U.S. State of Wyoming authorized commercial banks to act as Special Purpose Depository Institutions to provide digital asset custodial services. Bank customers may opt in to one of the following custodial relationships with a bank for each digital asset: i) custody under a bailment as a nonfungible or fungible asset – digital assets in this form shall be strictly segregated from other assets; or ii) custody under a bailment in which the bank may, upon an instruction from a customer, transact with the digital asset. The statute considers custody of digital assets as bailment, though the entire body of law outside this statute contemplates bailment for tangible property only. The Wyoming framework seeks to align digital assets custodial services provided by a bank with the Investment Advisers Act of 1940. This is done by providing that a bank must maintain customer “digital assets, funds and other securities which are not digital assets” i) in a separate account for each customer under that customer’s name; or ii) in accounts that contain only customer digital assets, funds, and other securities that are not digital assets, under the bank’s name as agent or trustee for customers.

Additional issues would need to be taken into account depending on the nature of the custodial arrangements, such as when the custodian uses a sub-custodian who may even be located in a foreign jurisdiction. One such issue would be the law applicable to the rights of customers to the digital assets held by the sub-custodian.
2.12 EFFECT ON LENDERS’ PROCEDURES AND PRACTICES

DLT and artificial intelligence (AI)\textsuperscript{145} may affect several aspects of secured creditors’ processes with respect to collateral. Monitoring, valuation, and risk mitigation techniques could be integrated with regulatory standards, ensuring compliance and data collection, including on the probability of default. However, secured creditors should bear in mind any data privacy regulations that may affect the type of information that they collect on their grantors when deploying AI to track the business activity or use of the collateral.

In particular, DLT and AI can facilitate initial valuation of the collateral to establish the amount of available credit, and its continuous valuation throughout the life of the credit facility, among others, to determine the availability of advances. The degree of monitoring and valuation will depend on the type of credit facility, which may be an all-assets deal that does not rely primarily on digital assets for the repayment of the loan, or a transaction secured with digital assets that may be the sole collateral. Several risks are also mitigated, particularly the unauthorized transfer of the collateral and the challenges of following it into the hands of transferees.

The administration and monitoring required for certain types of facilities are time and cost intensive. This is particularly true for revolving asset-based-lending (ABL) facilities. In ABL, the value of the underlying asset determines the loan amount and the availability of funds. Lenders commonly obtain updated appraisals of the collateral after loan disbursement and throughout the loan’s life for purposes of monitoring the collateral value, industry trends, and adequacy of the borrowing base. Where available, lenders rely on expert appraisals or valuations performed by companies experienced in asset liquidation, the processes that DLT and AI could automate, enabling real-time appraisal of ABL collateral, including those for which market prices are not transparent and publicly available. However, software that does not rely on DLT has already been in use, particularly for valuation of market-based assets for which public prices are available, such as securities. The software, whether DLT-based or not, may be configured to automatically respond to changes in the asset valuation, such as requesting the grantor to top up the collateral.\textsuperscript{146} Likewise, software may monitor real-time pricing from exchanges for commodities covered by warehouse receipts.

Large food retailers are already implementing DLT to bring transparency to supply chains for food-safety purposes. Retailers may thus see when the commodity is harvested, loaded into a truck, and delivered to the next participant in the supply chain. This information helps them make more effective recalls and avoid liability. Lenders could leverage the same information to have real-time visibility of the status of the commodity. This will assist them in effectively and more efficiently monitoring and tracing the collateral.

2.13 SECURITY RIGHTS IN INSOLVENCY

Classification of digital assets, as explained above, is also important for the purposes of insolvency law. While some of the classification approaches would be the same as under the secured transactions law, such as whether a digital asset may be subject to a property right, some others would be different, such as whether the enforcement of a right in a digital asset is subject to the automatic stay. For instance, if digital assets qualify as commodities, an agreement for their transfer may fall under a forward contract or swap exempted from the application of certain provisions of insolvency law, including the automatic stay.\textsuperscript{147} Even though insolvency laws may contain their own definitions of particular asset classes,\textsuperscript{148} insolvency courts may also defer to the interpretations of relevant regulatory agencies, such as the SEC in the United States with respect to “security”.\textsuperscript{149}

On the commencement of insolvency proceedings, an estate is created. Typically, it is defined broadly to encompass any interests of the debtor in property, which would include rights to any digital assets, whether or not they are subject to a security right.\textsuperscript{150} Insolvency law affects the rights of secured creditors in a number of aspects, some of which are summarized in this Section, drawing lessons primarily from several recent insolvency proceedings, including Mt. Gox in Japan, Cryptsy
in the United States, BitGrail in Italy, and South Korea’s YouBit. All of these entities operated a platform for the trading and holding of digital assets. Insolvencies of holders/owners of digital assets, such as the Russian case of Mr. Tsarkov, are on the rise as well, uncovering different types of issues. Insolvency laws do not provide specific provisions applicable to digital assets. As a result, the general provisions as well as those that apply to financial instruments need to be examined.\textsuperscript{151} The following paragraphs explore the classification of rights of creditors and holders, tracing and recovery of assets, and valuation of claims.

Depending on whether digital assets convey property rights, their holders may be entitled to economically different distributions in insolvency of an entity that holds the digital assets, such as an exchange operator or a custodian that maintains wallets. If the rights are proprietary, the insolvency administrator may be required to return the digital assets to the holders. If the holder retains a power of disposal, such as through a private key to access a wallet maintained by an insolvent custodian, the holder will be entitled to segregate its digital assets from the estate.\textsuperscript{152} In contrast, if the rights are contractual, the holders may be entitled to a distribution within the class of unsecured creditors. A Japanese court, analyzing Article 85 of the Civil Code, held that Bitcoin are not a “thing” capable of ownership under the Civil Code and thus the holders were not entitled to segregation under Article 62 of the Japanese Bankruptcy Act.\textsuperscript{153} In contrast, the Russian Appellate Court interpreted Article 128 of the Russian Civil Code on property to potentially include digital assets since the article refers to “other assets” that may be objects of property. The Appellate Court concluded that any assets of economic value should not be excluded from the estate.\textsuperscript{154} Similarly, a Dutch court stated that “Bitcoin represents value and is transferable…it thus shows a characteristic of a property right.”\textsuperscript{155} An Italian court in the BitGrail insolvency case also determined that cryptocurrencies can be considered property in accordance with Article 810 of the Italian Civil Code.

The classification of a digital asset as cash proceeds, as explored above,\textsuperscript{156} would also affect its treatment in insolvency, specifically the power of the insolvency administrator to use and dispose of the collateral, which is abridged with respect to cash proceeds.\textsuperscript{157}

**Box 5: Mt. Gox**

Mt. Gox, a Japanese Bitcoin exchange, became insolvent following the theft of a large number of Bitcoin it held. A client, who claimed Mt. Gox held 458 Bitcoin on his behalf, brought a lawsuit against the bankrupt exchange and the bankruptcy trustee. The client’s primary argument was that because he owned the Bitcoin, the trustee should segregate it from the Mt. Gox estate and transfer the Bitcoin to him, under the right of segregation in Article 62 of the Japanese Bankruptcy Act. The client also claimed damages arising from the trustee’s failure to transfer the Bitcoin to him.

The arguments and the judgment centered on the question of whether Bitcoin was a “tangible thing” that can be the object of ownership under Japanese law. The Court held that Bitcoin could not be the object of ownership, finding that Bitcoin did not fulfil either of the two criteria required for ownership of a “tangible thing”: that it be i) tangible; and ii) subject to exclusive control.
Digital assets may be further classified as a type of asset that may be entitled to a particular treatment in insolvency. For instance, for tokens that were issued as securities,\textsuperscript{158} holders’ rights may be treated as equity or debt, depending on the rights embedded in the digital asset; if equity, holders will be entitled to a distribution only after unsecured creditors.\textsuperscript{159} The classification of the digital asset as a claim or equity also determines the nature of possible participation of the holder in insolvency, for instance, as a member of a committee of unsecured creditors.\textsuperscript{160} For some security tokens, the classification as either debt or equity may not be clear.

The task of the insolvency administrator to gather the assets in which the insolvent person has some rights to form the estate is expected to be complicated by the difficulty in identifying and tracing digital assets or their current holders. Furthermore, digital assets may be easily transferred to someone outside the jurisdiction of the insolvency court.\textsuperscript{161} The anonymity of transactions on some DLT systems may complicate the application of some of the tools available to insolvency administrators, such as unwinding transactions as preferential transfers or fraudulent conveyances.\textsuperscript{162} Nonetheless, the incentive of the debtor to conceal a private key to access a wallet or transfer digital assets beyond the reach of the administrator are moderated by the rules that deny discharge to the debtor or provide for criminal penalties.\textsuperscript{163}

The price volatility of digital assets also affects the satisfaction of claims of creditors, as evidenced in the Mt. Gox insolvency, where the value of Bitcoin skyrocketed between the time of filing for insolvency and the recovery of Bitcoin by the insolvency administrator. If the value of the claim is set corresponding to the value of the property held by the estate at the time of filing for insolvency, the holders and their creditors will be entitled to a much lower distribution and would not benefit from any increase in the value of the digital assets.\textsuperscript{164} Similarly, upon insolvency, there might no longer be any secondary market for the type of digital asset that creditors hold, especially when its issuer is insolvent, in which case the claims of creditors may have a minimal value.
3. FINAL OBSERVATIONS

Several considerations emerge from the analysis on the legal implications of implementing DLT in STCR. There have not been any actual DLT installations of collateral registries that would allow further analysis. For the most part, non-DLT technology has been successfully implemented to design collateral registries. In contrast, digital assets have been used as collateral, and DLT implemented to streamline some processes of secured creditors, such as in the valuation and monitoring of the collateral. Yet those transactions are far from being as established as the classical asset-based loans secured with inventory and receivables.

In respect to the implementation of DLT in collateral registries, this Guidance Note highlights several specific aspects:

- The technology supporting modern collateral registries ensures that notices with incomplete (mandatory) fields are not registered but does not aid the registrant in the entry of accurate or sufficient information. DLT can also efficiently ensure completeness of mandatory information, but the nodes, like the registry software or a registry clerk, would not be able to verify whether the information entered is sufficient or even accurate.
- Non-DLT technology and DLT authenticate registrants to reduce the risk of unauthorized registrations.
- Implementation of any further mechanisms to reduce the risk of unauthorized registrations, whether through non-DLT technology or DLT, would require changes in the law.
- Like the non-DLT registries, DLT may efficiently provide for timestamping of registrations and their storage in a chronological order.
- DLT is inherently more resilient to a single point of failure, as it does not rely on a centralized database that stores registrations. However, non-DLT databases are protected against inadvertent and malicious attacks, and no known event of loss or corruption of data has been reported. DLT installations are susceptible to some tampering of data, such as through exploiting vulnerabilities in the software.
- The searcher not only must be confident that the search result has not been tampered with but also should be able to easily conduct the search. Blockchain ledgers hold only hashes of information that confirm its integrity, but do not reveal transaction details. As a result, an additional search of the non-DLT database would need to be made. While this architecture may increase the confidence of the searcher, it requires two searches.
- Interoperability of collateral registries with other registries, such as motor vehicle registries, has been a challenge. It remains a challenge for DLT.
- Commercial utility of some of the proposed features that may be implemented through DLT, such as tokenizing registrations, is questionable, or they can already be achieved under the current law using existing technology.

In respect to the application of the secured transactions law pertaining to digital assets, this Guidance Note highlights several specific aspects:

- Laws and regulations dictate the nature of digital assets as well as the rights of their holders, at times limiting or precluding the creation of security rights.
- The UNCITRAL Model Law and other modern secured transactions laws do not provide specific collateral types for digital assets, as they do for receivables or inventory, for applying specific rules to security rights in those types of assets. Accordingly, the rules that generally apply to the residual category of intangible assets would likely apply to security rights in digital assets.
- Cryptocurrency would not be classified as money or funds credited to a bank account under the UNCITRAL Model Law if a State implements it as adopted. Consequently, the general rules applicable to intangible assets, including the rights of their transferees, would apply. As a result, unlike transferees of money or funds, the ability to acquire cryptocurrency free of a security right would be much more limited.
- The inapplicability of takes-free rules may impact the level of due diligence expected to be undertaken by transferees and secured creditors.
- The classification of digital assets as general intangible assets, subject to some exceptions such as security tokens,
determines the applicable perfection mechanism, which is limited to registration in the collateral registry.

- Some of the touted benefits, such as automated and immediate enforcement of a security right upon default, must be balanced against the requirements of proceeding in a commercially reasonable manner and protecting affected parties, such as providing a notification of disposal. Enforcement rights would be enhanced by the recognition of control as a perfection method for security rights in digital assets.
- DLT facilitates some aspects of secured lending practice, including valuation and monitoring of the collateral, which, if performed efficiently, may satisfy the regulatory requirements applicable to banks and other regulated lenders.
- While blockchain has been promoted as a system that disintermediates relationships, digital assets are commonly held with custodians, exposing their holders to a number of risks that are mitigated for securities held with intermediaries in the applicable frameworks, which only now start to emerge for custodians of digital assets.
- The classification of digital assets as property or personal claims drives the level of satisfaction of the claim in insolvency of a custodian.

2 For explanations of private, public, permissioned, and permissionless DLT systems, see Guidance Note on Distributed Ledger Technology and Secured Transactions Frameworks: A Primer (WBG, 2020) [hereinafter DLT-STCR Technology Note].

3 For an analysis of the applicable regulatory regimes to different DLT-STCR outputs, the reader should refer to the companion Guidance Note on Distributed Ledger Technology in Secured Transactions Law & Collateral Registries: A Regulatory Perspective (WBG, 2020) [hereinafter DLT-STCR Regulation Note].


5 Id. Arts. 7, 8 of the Model Registry Provisions.

6 This may also be some period of time after expiration; see UCC 9-522(a).

7 For a description of the permissioned and permissionless DLTs, DLT-STCR Technology Paper, supra note 2, at 4.1.

8 Id.

9 Id.

10 A hash is a unique representation of data created by applying a hashing function (calculation) to the original data. The original data used to create the hash cannot be determined from the hash even when the hashing function is known. By contrast, encrypted data can be decrypted (e.g., using a password) to access the original data.

11 Storage of registrations is discussed in Section 1.5 infra.

12 See Section 1.7 infra.

13 This is not the case of UCC filing systems in the United States. See UNCITRAL Model Law, supra note 4, Art. 5.1(b).

14 Rob Cowan & Donal Gallagher, “The International Registry For Aircraft Equipment – The First Seven Years, What We Have Learned” (2014) 45 UCC L. J. 225, 230, https://www.aviareto.aero/wp-content/uploads/2015/03/UCCLJ-Volume-45-No3-Cowan-Gallagher.pdf (last accessed Apr. 3, 2020); PKI uses industry standard protocol (Secure Sockets Layer [SSL] and Transport Layer Security [TLS]) to establish secure communications that i) authenticates users and machines with digital certificates issued by trusted third parties; ii) encrypts communications and data transmissions by using a secret private key and a mathematically related public key; and iii) assures non-repudiation (i.e., provides proof of the origin and integrity of the transmitted data); see https://docs.oracle.com/cd/B10501_01/network.920/a06582/pki.htm (last accessed Apr. 3, 2020).


16 Id. at 15.

17 Id.

18 While all blockchains add blocks in sequential order, some DLT platforms (e.g., Hyperledger Fabric) can ensure that multiple transactions (registrations) within each block are similarly in sequential order.

19 UNCITRAL Model Law, supra note 4, Model Registry Provisions, Art. 5(2).

20 Cape Town Convention, supra note 1, Art. 20. See further Cowan & Gallagher, supra note 14, at 231 (“...each party to a registration must confirm their consent to a registration by applying their digital signature, which is stored as an integral part of the registration data, thereby ensuring the integrity of each individual record, or group of records”).


22 Yaga et al., supra note 15, at 34.

23 Id. at 17.

24 Id.

25 Id.

26 Id. at 14.

27 Id.

28 See further DLT-STCR Technology Paper, supra note 2, at 2.

29 Another key element are fees charged for various registry services, which is a policy choice that is not examined in this Guidance Note of technical nature.

30 UNCITRAL Model Law, supra note 4.

31 Using a Merkle tree data structure (also known as a binary hash tree), containing cryptographic hashes, it is only necessary to make, at most, 2 x Log2(N) calculations to determine if a tree contains a specific hash (where N is the number of hashes in the tree). For example, for a tree containing 2,000 hashes, at most, only 22 calculations (2 x Log2(2,000) = 22) would need to be checked to determine whether a specific hash was contained in the tree; for more on Merkle trees, see Andreas M. Antonopoulos, Mastering Bitcoin, Chapter 7: The Blockchain, (O’Reilly) https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html (last accessed Apr. 3, 2020); and see Damien Cosset, “Blockchain: What Is In A Block?” (27 Dec. 2017, DEV), https://dev.to/damien_cosset/blockchain-what-is-in-a-block-48jo https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html (last accessed Apr. 3, 2020).


33 Using a Merkle tree data structure (also known as a binary hash tree), containing cryptographic hashes, it is only necessary to make, at most, 2 x Log2(N) calculations to determine if a tree contains a specific hash (where N is the number of hashes in the tree). For example, for a tree containing 2,000 hashes, at most, only 22 calculations (2 x Log2(2,000) = 22) would need to be checked to determine whether a specific hash was contained in the tree; for more on Merkle trees, see Andreas M. Antonopoulos, Mastering Bitcoin, Chapter 7: The Blockchain, (O’Reilly) https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html (last accessed Apr. 3, 2020); and see Damien Cosset, “Blockchain: What Is In A Block?” (27 Dec. 2017, DEV), https://dev.to/damien_cosset/blockchain-what-is-in-a-block-48jo https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html (last accessed Apr. 3, 2020).

34 See Section 1.7 infra.

35 Id.

36 See Section 1.7 infra.

37 This is not the case of UCC filing systems in the United States. See UNCITRAL Model Law, supra note 4, Art. 5.1(b).

38 For the legal challenges presented by the coordination between collateral registries and IP registries, see Andrea Tosato, Secured Transactions and IP Licenses: Comparative Observations and Reform Suggestions, 81 Law and Contemporary Problems 155-180 (2018), at 175-176.
Registries, Univ. L. Rev., 1999-2, 335, 343.
39 For example, the Australian Personal Property Securities Register allows several separate payment options, including separate credit card payments for each registration; see https://www.ppsr.gov.au/method-payment-0 (last accessed Mar. 20, 2020).
40 DLT-STCR Technology Paper, supra note 2, at 5.1.
41 A tokenized security may also be supported by an actual asset, such as an immovable owned by the company that issued the tokenized equity security.
43 Id. 16.
44 For an overview of the main regulatory regimes impacting on digital assets and secondary markets, see DLT-STCR Regulation Paper, supra note 3, Section 2.
45 UNCITRAL Model Law, supra note 4, Art. 1(3)(d).
46 Id. Art. 6(1).
47 In limited circumstances, the secured transactions law may vest the grantor with the power to create a security right, such as Article 6(1) of the UNCITRAL Model Law.
48 Id. Art. 1(6).
50 Cryptocurrencies in Public and Private Law (Fox & Greene eds.) Cryptocurrencies in the Common Law of Property 141 and 146 and Cryptocurrencies as Property in Civilian and Mixed Legal Systems 147. In National Provincial Bank Ltd v Ainsworth 2 All ER 472 (1965), the House of Lords stated: “Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability.” See further McGrath, Transacting in a Vacuum of Property Law.
53 See the Internal Revenue Office issued Notice 2014-21, stating that convertible virtual currencies are property for tax purposes.
54 See In re Tracy Broadcasting Corp., 438 B.R. 323 (Bankr.D.Colo. 2010) for the discussion of broadcasting licenses under the U.S. law.
55 See DLT-STCR Regulation Paper, supra note 3, Section 6 (on the regulatory classification of digital assets) and Section 7 (on the application of regulatory regimes to secondary markets for collateral).
56 Token Alliance, supra note 42, 20.
57 UCC 9-408(c).
58 Articles 13 and 15, examined below, are limited to the override of contractual restrictions on a transfer of receivables and the creation of security rights in a right to payment of funds credited to a bank account.
59 Cryptocurrencies in Public and Private Law (Fox & Greene eds.) Cryptocurrencies in the Common Law of Property 156.
61 See Kenya’s Movable Property Security Act No. 13 of May 2017, s. 2 (Kenya MPSR).
62 Official Comment 24 to UCC 1-201.
63 Irina Marinescu, Market Making in Crypto – A Secured Lending Lawyer’s Learnings, 49 No. 1 UCC L.J. ART 5 (July 2019).
64 DLT-STCR Regulation Paper, supra note 3, Section 6.4.
65 INSOL, Cryptocurrency and Its Impact on Insolvency and Restructuring, 12 (May 2019) [hereinafter INSOL].
66 UNCITRAL Model Law, supra note 4, Art. 2(c).
67 For an overview of the applicable regulatory regimes, see DLT-STCR Regulation Paper, Section 5; see also Section 6.2 on stablecoins and their characterization under banking and payment laws, and Section 6.4 on Central Bank Digital Currencies and their characterization as money.
68 See UCC 9-102(a)(8) and (29).
69 See Section 2.7 infra.
70 For an analysis classifying Bitcoin under UCC Article 9, see Lorena Y. Gely-Rojas, Cryptocurrencies and the Uniform Commercial Code: the Curious Case of Bitcoin, 8 University of Puerto Rico Business Law Journal 129. See also Kevin V. Tu, “Perfecting Bitcoin,” GEORGIA LAW REVIEW (August 2018).
71 See, for instance, Saskatchewan Personal Property Security Act 2. 1(3).
72 See Section 2.4 infra.
73 UNCITRAL Model Law, supra note 4, Art. 6(1)-(3). This provision provides enacting States with the option to also require that the security agreement specify the maximum amount for which the security right may be enforced. However, for the purpose of this Guidance Note, this option is inconsequential.
74 See UNCITRAL Model Law, supra note 4, Art. 2(z), defining possession as “the actual possession of a tangible asset by a person or its representative, or by an independent person that acknowledges holding it for that person”.
75 See UCC 9-203(b)(3)(D).
76 Supra Section 1.1.
77 UNCITRAL Model Law, supra note 4, Model Registry Provisions, Art. 11.
78 Id. Art. 13(1). Notably, Art 13(2) specifies that a person who grants a security right in a receivable contravening a contractual agreement will not be shielded from liability for such a breach of contract.
79 See Id. Art 2(dd) for the definition of “receivable”.
80 See UCC 9-406(d) and 9-408.
81 See UNCITRAL Model Law, supra note 4, Art. 2(bb).
82 UNCITRAL Model Law, supra note 4, Guide to Enactment paras 100-101.
83 UNCITRAL Model Law, supra note 4, Art. 25.
84 Id. Art. 24.
85 Id. Art. 26(3).
86 Id. Art. 18(2). See also supra Section 1.3.
87 Under English law, delivery of car keys may represent the delivery of the car itself. Iain McDonald and Anne Street, Equity & Trusts Concentrate: Law Revision and Study Guide, 45 (2013).
88 See Id. Art. 18(1).
89 This is the case under UCC Article 9 for security interests in money and deposit accounts (as original collateral).
90 See the UNIDROIT Convention on Substantive Rules for Intermediated Securities (“Geneva Securities Convention”), Art. 12.
On the classification of digital assets under securities and commodities exchange law as well as other financial regulatory regimes, see DLT-STCR Regulation Paper, supra note 3, Section 6.1.

92 See UNCITRAL Model Law, supra note 4, Art. 2(b).
93 Id. Art. 32.
94 Id. Art. 43.
95 Id. Art. 48(1).
96 Id. Art. 51(5).
97 See UCC Arts. 8, 9.
100 UNCITRAL Model Law, supra note 4, Model Registry Provisions, Art. 26 Option A.
101 UCC 9-316(a)(3).
102 See UNCITRAL Model Law, supra note 4, Art. 78(1).
103 Id. Art. 78(4).
104 Id. Arts. 75-76.
105 Id. Art. 72(3). See also UCC 9-624.
106 See the Geneva Securities Convention, Arts. 33 and 35.
107 UNCITRAL Model Law, supra note 4, Art. 80.
108 Id. Arts. 82-83.
112 Id.
114 Kyle A. Owens, supra note 111.
115 Id.
116 See further DLT-STCR Regulation Paper, supra note 3, Section 7.
120 See Arts. 85 and 88 of the UNCITRAL Model Law, but compare with UCC 9-301(1), under which the law of the location of the debtor is the connecting factor for security rights in both tangible and intangible collateral.
121 UNCITRAL Model Law, supra note 4, Art. 85. Compare with UCC 9-301(1).
122 Cryptocurrencies in Public and Private Law (Fox & Greene eds.) Cryptocurrencies and the Conflict of Laws 127.
123 See UNCITRAL Model Law, supra note 4, Arts. 97, 98, and 100.
124 Id. Art. 3(1).
126 See UNCITRAL Model Law, supra note 4, Art. 100.
127 FMLC Paper, supra note 60, 18.
128 Id. at 21.
129 Certain issues of general nature relating to digitalization of assets may also be left up to the courts. Swiss Report, 78.
130 See further, DLT-STCR Regulation Paper, supra note 3, Section 3.1.
131 Freshfields, Bruckhaus & Deringer, Cryptocurrency – What You Need to Know, 1 (March 2019).
133 Token Alliance, supra note 42, 33.
138 Of the control locations enumerated in paragraph (c), only a securities depository, such as the Depository Trust Company, or a bank could hold tokenized securities. The term bank primarily includes federally supervised banks, but no federal bank agencies have permitted federally chartered banks to hold tokenized securities. Token Alliance, supra note 42, 28.
139 Token Alliance, supra note 42, 30.
140 Freshfields, Bruckhaus & Deringer, Cryptocurrency – What You Need to Know, 8.
141 Title 13, Chapter 12. Special Purpose Depository Institutions (SPDIs) are a new bank category that provide banking services to blockchain-based businesses. See https://www.nasdaq.com/article/wyoming-passes-bill-to-secure-banking-relations-for-blockchain-companies-cm1063906 (last accessed Mar. 25, 2020).
142 W.S. § 34-29-104(a).
143 W.S. § 34-29-104(d)(i) and (ii).
144 Draft Regulations, Section 4(a).
145 See further DLT-STCR Technology Paper, supra note 7, Section 6.4.
147 INSOL, supra note 65, 14.
148 See the definition of property in section 436(1) of the U.K. Insolvency Act 1986.
150 INSOL, supra note 65, 23.
151 See, for instance, Swiss Report, supra note 125, at 66.
152 Id. at 67.
155 Id. at 4.
156 Supra Section 1.4.2
157 See Recommendation 52 of the UNCITRAL Legislative Guide on Insolvency Law.
158 Supra Section 1.2.
160 Id. Holders of crypto-assets may also seek appointment of their own committee, such as under the U.S. Bankruptcy Code s. 1102(a)(2).
163 See s. 727 of the U.S. Bankruptcy Code.
164 See further INSOL, supra note 65, 30.