SWISS
BLOCKCHAIN
FEDERATION

Circular 2021/01

Ledger-based Securities

Updated Version of September 2021

Publication date: 2021-10-12

To: Issuers of ledger-based securities and the associated service providers

Authors: Security Token Working Group, consisting of Diego Benz (Kaiser Odermatt), Mauro Cappiello (Blockchain Innovation Group), Hans Kuhn (DALAW), Luzius Meisser (Bitcoin Association Switzerland), Daniel Rutishauser (Inacta), Ricardo Schlatter (SDX), Alexander Thoma (Postfinance), Claudio Tognella (daura), Rolf H. Weber (University of Zurich).
Contact: Daniel Rutishauser, daniel.rutishauser@inacta.ch

Approved by the Board of the Swiss Blockchain Federation on 2021-09-23

Disclaimer: Swiss Blockchain Federation is a private organisation. The recommendations stated in this document are economically and legally sound to our best knowledge but cannot replace personal advice.

Table of Content

1 Introduction

On 1 February 2021, the securities regulations of the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT Act) entered into force (Art. 973d et seqq. of the Swiss Code of Obligations (CO)). The DLT Act introduced ledger-based securities into Swiss law; such securities are created by entry in a securities ledger and can only be exercised and transferred via this securities ledger. The securities ledger must satisfy the requirements mentioned and characterized in Art. 973d (2) CO. The registration agreement creates the constitutive link between the right and the entry in the ledger. ledger-based securities have the same functions as a physical order or bearer instrument (certificated securities), especially the functions of transparency, evidencing of title and protecting commercial transactions (cf. Art. 973e CO).

Through the ledger-based security, the legislator has created a robust legal basis for the tokenization of assets. As with any new law, numerous questions of interpretation arise. That is especially true in the case of the DLT Act, because it introduces a number of new concepts. With the present Circular, the Swiss Blockchain Federation (SBF) makes its contribution towards a common understanding of the requirements for the securities ledger and the registration agreement and thereby develop a standard shared by all the relevant stakeholders.

Free transferability of securities is a cornerstone of Swiss securities law. Unlike in other jurisdictions, it is not mandatory under Swiss law to dematerialize securities or hold them through financial intermediaries. This policy has been clearly confirmed when the Federal Intermediated Securities Act (FISA) has been adopted, which created an open system which permits the export of intermediated securities in order to be held directly by investors (see art. 8 FISA). Free transferability is also a cornerstone of the law of ledger-based securities. Any attempt of regulators to limit transferability to whitelisted investors or to investors having been identified by a financial intermediary would be in violation of a clear policy stance. Nor can a legal obligation of the issuer to identify acquirers of register securities or security tokens be derived from AML/TF rules and regulations; i.e. the issuer of shares or security tokens is not a financial intermediary under article 2(3) AMLA.

Registered shares subject to transfer restrictions (in German: “vinkulierte Namensaktien”), which are not listed at a stock exchange, may be transferred only with the issuer’s consent (Art. 685b CO). The transfer of ownership to the acquirer is perfected only once the consent has been granted (article Art. 685c (1) CO). In relation to the issuer only the person registered in the shareholder book (in German: Aktienbuch) is deemed to be a shareholder, and a registration requires that the acquirer's identity be established (Art. 686 (1) and (2) CO). The issuer of registered shares therefore has an interest in being capable of identifying acquirers of its registered shares. Since there are some open questions regarding the transfer restrictions, this topic will be discussed in a future edition of this paper.

2 Requirements for the Securities Ledger

2.1 Term and definition

A ledger-based security is a right that is entered in a securities ledger under a registration agreement and only can be exercised and transferred via this securities ledger (Art. 973d (1) CO). The entry in the securities ledger is the digital equivalent to the certification of a right as a physical security; as an electronic ledger it enables the entry of rights that are thereby converted into ledger-based securities.

Swiss law (Art. 973d (2) CO) leaves the structure and design of the securities ledger open. It does lay down four requirements, however, that must be met by such a facility in any case in order to be characterized as a securities ledger: Use of technological processes to give the creditors, but not the obligor, power of disposal over their rights (item 2.2); protection of the integrity of the facility and the corresponding entries (item 2.3); transparency of rights and functions in the ledger (item 2.4); minimum required content of the entries (item 2.5). Since the ledger represents property rights, it must also satisfy the general public notice requirements (item 2.6).

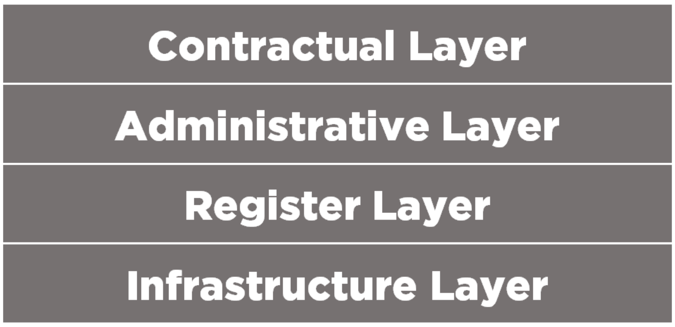
Clarity about the statutory requirements is of central importance for the following reasons: if a mechanism fails to meet the requirements mentioned in Art. 973d (2) CO, then the right registered there will not be a ledger-based security but only an uncertificated security or ordinary debt claim, as the case may be. Such a right cannot be transferred upon entry in the ledger nor can it have the effects of evidencing title or protecting commercial transactions under Art. 973e CO.

For the application of these requirements, it is important to understand the multi-layered architecture of DLT based systems. We distinguish between four layers.

- The **infrastructure layer** provides the technical foundation and typically fulfills the basic requirements regarding decentralization and integrity. However, it is unaware about securities, tokens, or other concepts defined by the issuer. An example choice for this layer could be the Ethereum blockchain.
- The **register layer** is built on top of the infrastructure layer and contains the actual register, namely entries that map addresses to balances. This register typically comes in the form of one or more connected smart contracts written and deployed by the issuer or by a service provider tasked by the issuer. These contracts fulfill the requirements of the law when deployed on a suitable infrastructure and equip the token holders with power of disposal over their token.
- On the **administrative layer**, additional features are added to the register as agreed to in the articles of association (in case of shares), an extended registration agreement, or other suitable legal documents. On this layer, the power of disposal of the token holders might be restricted again, for example through functions for the enforcement of statutory transfer restrictions (Vinkulierung). Typically, these additional

features concern all security tokens in circulation, but it is also conceivable to have different groups of users or classes of tokens with varying additional features or restrictions.

- On the **contractual layer**, contractual agreements between token holders, token holders and the issuer, token holders and the beneficial owners, etc. are implemented. These agreements might be of purely contractual nature but might also be fully or partially enforced through smart contracts deployed and managed by the parties of the respective agreements. Examples could be a shareholders' agreement, vesting in an employee participation plan, or a deposit agreement between a token holder and an exchange.



Contractual Layer

Administrative Layer

Register Layer

Infrastructure Layer

2.2. Power of disposal

2.2.1. Principle

As the first constitutive requirement, number 1 of Art. 973d (2) CO requires that the securities ledger confers upon "the creditors but not the obligor power of disposal of their rights through technological processes". "Power of disposal" here means a person's de facto control over a ledger-based security or token and is comparable with possession of physical objects. The power of disposal over ledger-based securities is therefore functionally equivalent to possession of a physical share certificate. The requirement of power of disposal by the creditor but not by the obligor is a distinguishing feature from centralized ledgers (e.g. in the case of intermediated securities) and creates a parallel to certificated securities, which are likewise subject to sole power of disposal by the creditor.

The fact that the creditor but not the obligor must have power of disposal does not prevent the creditor from entrusting the administration or custody of the ledger-based securities to a third party - including the issuer - thereby exercising only indirect control over the ledger-based securities. In particular, the creditor may have the ledger-based securities held in custody by the issuer. The creditor must have the option, however, of exercising control over the ledger-based security directly, when desired. Nor does that requirement prevent the issuer from having privileged access to the other functions of the ledger. The issuer is still responsible, for instance, for issuing the ledger-based securities, and thus for increasing the number of securities outstanding.

From the requirement of the power of disposal, the Dispatch of the Federal Council derives at least a minimum of decentralization, i.e. the creditor must be capable of initiating “the transfer of ledger-based securities […] in principle without the intervention of a trusted central authority that alone manages the ledger, and of [executing the transfer] according to the rules of the securities ledger" (Dispatch, Federal Gazette 2020, 278). This requirement will be analysed in more detail in 2.3.

2.2.2. Rights of intervention

In practice, token contracts often involve a number of different special functions that are under the control of the issuer or of an authorized third party. Such functions include pausing the entire ledger, white-listing, freezing of individual addresses and retrieval of lost tokens. There is no obligation under civil law to provide for the exercise of such options of intervention at the ledger level. It is left up to the issuer to weigh the risks and benefits of the individual functions and to endow the ledger with them only to the extent compatible with the requirements for the securities ledger.

Such functions are compatible with the requirement of power of disposal by the creditor, but not by the obligor, only if appropriate governance prevents misuse by the obligor. At least the following is required to that purpose:

- The registration agreement gives a clear and transparent description of the creditor's rights of intervention and the prerequisites for exercising them. The freezing of tokens is usually permissible only pursuant to a formal order by a competent authority (e.g. attachment order, ruling of a criminal investigation authority, inter alia).

- The creditor has established procedures and processes to prevent misuse of the intervention rights, e.g. by depositing the private key with an independent third party (notary, escrow agent).

The pause function is sometimes justified on the grounds that in case of a “hard fork” it can help point out which of the two systems will contain the true ledger from that point forward, while the false ledger is paused. When the pause function is activated, the creditor loses the power of disposal over its ledger-based securities and the securities ledger ceases to meet the statutory requirements. In the case of a hard fork, that is the desired effect, since the ledger in the "false" system should no longer be a valid securities ledger. In general, the pausing of securities ledger should be avoided.

Allow-listing, i.e. the express approval of each address to which a token can be transferred, is permissible and comparable from the legal standpoint with agreeing on transfer restrictions in relation to debt claims. One prerequisite for allow-listing is the consent of the first takers at the time of issue or the consent of the creditor at the time of deployment. If the ledger-based securities are registered shares, the obligor is required to allow all transfers that comply with the transfer restrictions and/or to activate the target addresses on request. Neglecting or failing to comply with the above obligation does not change the classification of the securities ledger as such.

Functions that enable freezing or transferring ledger-based securities without the creditor's intervention, e.g. the function to recover lost tokens, are more problematic. Such functions are not permitted if they can be exercised by the obligor and the creditor has no way of depriving the obligor of that possibility. To avoid doubts about the classification of the securities ledger, it is advisable to give the creditors a technically viable "opt-out" from recovery functions and the like.

2.3 Integrity

Number 2 of Art. 973d (2) CO stipulates as the second constitutive requirement the protection of the integrity of the ledger, by securing “integrity through adequate technical and organizational measures, such as joint management by several independent participants, to protect it from unauthorised modification.”

In contrast to number 1, which stipulates requirements for the rules of the ledger, numbers 2 and 4 impose requirements on the system for implementation of those rules. Blockchains use two technological methods to that purpose: electronic signatures and a consensus mechanism. While number 4 concerns the use of electronic signatures, this number concerns the consensus mechanism and thus the question of how transactions can be recognized as complying with the rules and how the participants can reach an agreement in case of dispute. The “participants” mentioned in the Law are the operators of the underlying system. It must be assumed that creditors submit their transactions with those participants and are free to choose which participants they will use for that purpose.

To secure the integrity of the system, the following must be clarified from the outset:

- how the system participants are defined and what happens in case of the loss of a participant and/or violation of the rules by a participant;
- how the participants receive transactions from creditors and how they are exchanged between the participants;
- how, in case of more than one participant, simultaneously submitted contradictory transactions or other contradictions are dealt with.

Although such requirements are met by a typical Blockchain, they can conceivably be satisfied by other systems, too. For example, the Paxos algorithm[1] is often used in IT systems with

[1] https://en.wikipedia.org/wiki/Paxos_(computer_science)

strict system availability and integrity requirements. In general, it can be proven that a system that is supposed to be robust when f equal-ranking participants are compromised must consist of at least 2*f + 1 participants. If a ledger is required to deal successfully with the failure of a single participant, it must consist of at least three participants.

Exceptionally, decentralization is assured if there are only two equal-ranking participants, providing that there is a mechanism of resolving a contradiction between the two participants with the involvement of a third party.

Decentralization presupposes that the participants are mutually independent. Such independence is assured if the multiple participants are not under joint control, which must be evaluated taking all the circumstances into account.

2.4. Transparency obligations

As the third constitutive requirement, number 3 of Art. 973d (2) CO requires that the content of the rights, the functioning of the ledger and the registration agreement be recorded in the ledger or in linked accompanying data. According to the Dispatch, the exact content of the certificated right (amount of the equity interest, amount of the debt claim, due date, etc.) must be clear from it. Moreover, the registration agreement must be clear and transparent for the Parties and include information about the functioning of the ledger. As the Dispatch goes on to explain, that information does not have to be mapped on the DLT system itself but can be contained in the linked accompanying data such as terms of issue, articles of association, offering circulars or a white paper. In any case, the information must be technologically linked with the ledger, e.g. by embedding a human-readable link to a website where the registration agreement and other relevant documentation is available. Additionally, a cryptographic fingerprint (hash) of the relevant documents can be added, allowing token holders to verify with cryptographic certainty that the terms found under the provided link are the correct ones and have not been altered.

One possibility of meeting such requirements is to record a link to a static document with the hash number as an attribute in the document, e.g.:

terms = “nestle.com/investors/registrationagreement.pdf?sha3=0xc4755faf95…”

Ideally, the cryptographic linking goes two ways, with the registration agreement containing the fingerprints (blockchain addresses) of the smart contracts that constitute the register and the register containing the fingerprint (hash) of the registration agreement. However, since the fingerprint of the registration agreement changes when inserting the fingerprint of the register and vice versa, this can in practice only be achieved by first deploying the smart contract without cryptographic link to the register and then later add the hash by calling an according function (e.g. setTerms as defined in annex “ERC-20 Extension”). We take the position that in practice, a one-way hash (either from the register to the agreement or from the formally enacted agreement to the register) is sufficient to fulfill the linking requirement of the law, as long as the register enables the token holders to find the agreement.

It is also important in that connection to provide for a possibility of modifying the registration agreement and the link to it, e.g. if additional ledger-based securities are issued so that the quantity of them is adjusted. An alternative approach would be to publish a separate, static registration agreement for each issue. Both of those approaches meet the statutory requirements.

In sum, the information requirements under number 3 of Art. 973d (2) CO are fulfilled under the following conditions:

- The securities ledger and/or the linked accompanying documents make it possible to derive basic information about the content of the ledger-based securities. It is necessary to specify the type of certificated security (share, debenture, etc.), the designation of the obligor and the nominal value or other information about the denomination.
- The ledger provides access to the registration agreement and information about the functioning of the ledger.

If the registration agreement is temporarily unavailable (because the issuer's website is off-line, for example) the transparency requirements under number 3 of Art. 973d (2) CO are still satisfied in any case. The foregoing is without prejudice to the issuer's liability under Art. 973i CO.

2.5. Rights of inspection and verification

Under number 4 of Art. 973d (2) CO, a securities ledger must also ensure that the creditor can inspect and verify the information and ledger entries as well as the integrity of the ledger contents concerning him, without the intervention of third parties. The purpose of the rights of inspection and verification under number 4 is to ensure the integrity of the ledger entries under number 2 and should be read in that context. The most important thing is that verification must be possible without the cooperation of the obligor.

To allow the creditors to verify whether the ledger actually complies with the rules of the registration agreement, the source code of the ledger (but not the underlying system) should be disclosed, possibly as an annex to the registration agreement. In addition, it must be possible to check whether the cited source code coincides with the bytecode stored in the system.

It is unlikely that a verification of the smart contract by an independent third party (so-called “token audit”) suffices, because number 4 of Art. 973d (2) CO expressly stipulates that the creditor must be able to verify the integrity of the relevant ledger content without the intervention of a third party. That includes the verification of whether the rules were applied properly during the creation of the ledger content and whether one's own ledger entry can really be modified only in accordance with the published rules.

In the case of Blockchain-based systems, the integrity check has a specific technical meaning, i.e. verification of the electronic signatures of the relevant transactions and the verification that the transactions were accepted by the system and inserted into a specific position in the Blockchain. In the process, the practice of “pruning” (deleting of old transaction data) should be acceptable if the corresponding transaction data was available sufficiently long for inspection and verification. The Law and Dispatch leave it open whether a creditor must be able to check not only the present ledger entries concerning him but also the old entries or transaction chains that gave rise to the creation of his entries.

Blockchains ensure that they are tamper-proof - as mentioned above - by using two technical features, i.e. electronic signatures and a consensus mechanism. Whereas the purpose of Art. 973d (2) CO is to ensure the availability of a robust consensus mechanism, number 4 concerns the use of electronic signatures. Only such signatures allow a creditor to check the integrity of a transaction with mathematical certitude, without the intervention of a third party. It should be noted, however, that there is a subtler but more decisive difference between ZertES electronic signatures and electronic signatures as they are used in the context of Blockchains: the former prove the identity of the signatory, whereas the latter prove authorization. This means that the latter are better suited to creating an independently verifiable ledger. A signature that only proves the identity of the signatory is useless unless it is simultaneously necessary to present proof that the signatory is entitled to perform the transaction in question.

It might be possible to meet the requirements of the Law even without electronic signatures. Considering the origins of the DLT Act, however, it is advisable to use such signatures because they are currently the most secure known method of meeting the requirements of the DLT Act.

2.6. Public notice

The main purpose of a securities ledger is to ensure public notice of rights in relation to the ledger-based securities. The DLT Act only deals with that issue implicitly; but public notice is a basic prerequisite for a system intended to guarantee rights of ownership. The securities ledger therefore also has to ensure that the legal authority to ledger-based securities or limited rights in rem (pledges, usufruct) is recognizable to third parties (particularly, potential acquirers of such rights).

The DLT Act differentiates between security rights with and without possession (Art. 973g (1) CO). In the case of rights with powers of disposal, the public notice is provided by the power of disposal over the ledger-based securities, which implies that the holder of the power of disposal has lawful authority.

Art. 973g (1) CO opens up another possibility of having security rights to ledger-based securities without possession. The prerequisite is that (1) the collateral is visible in the securities ledger and (2) it is ensured that only the secured party can dispose of the ledger-based security in case of default. The first prerequisite is satisfied if the corresponding entry in the securities ledger displays that a security right was created in the ledger-based security, e.g. by flagging or colouring the corresponding token. The second condition is satisfied if the secured party can acquire sole power of disposal over the corresponding ledger entry in case of default. In case of a pledge, that may also occur through an enforcement action for the realization of pledged property (Art. 151 et seqq. DEBA); in the case of other security interests (title transfer arrangements), however, no administrative procedure is available. In that case, the parties must agree on a legally enforceable procedure for the acquisition of the power of disposal by the secured party.

2.7. Organizational responsibility

According to CO Art. 973d (3), the obligor likewise must ensure that the securities ledger is organized in accordance with its purpose and functions in accordance with the registration agreement at all times. The DLT Act therefore makes the obligor (issuer) responsible for proper functioning of the ledger. If loss or damage occurs due to the improper organization of the ledger, the obligor shall be liable in accordance with the general principles of contractual liability (Art. 97 CO et seqq.); liability for unlawful pre-contractual conduct is also conceivable.

Further liability claims may arise from incorrect information (Art. 973i (2) CO), which will be analysed further in 7.

3 Registration agreement

3.1. Term

Thanks to registration, a right is linked with a ledger entry so that it can only be transferred and exercised on the basis of the ledger. The legal significance of the entry and link results from its so-called registration agreement. The registration agreement is an agreement pursuant to which the right is entered in the securities ledger and can only be transferred and exercised on the basis of the ledger (Art. 973d (1) CO). By codifying and mentioning the registration agreement, the DLT Act implies that the Parties have an express agreement on that subject.

In principle, the registration agreement is reached between the issuer and the person who acquires the ledger-based security as the first legal transaction ("first acquirer"). That is either the underwriter or (in the context of a firm underwriting) an issuing bank. Subsequent acquirers join it through acquisition of the ledger-based security. In the case of ledger-based securities that represent legal positions under corporate law (shares, equity interests, dividend-right certificates, etc.), the registration agreement is represented by corresponding articles of association (Art. 622 (1) CO). The articles of association may also confer on the board of directors the right to establish the details of registration in regulations. The resolutions formulated according to the articles of association and applicable laws shall apply to all shareholders, even if they have not consented to the registration.

At least in the case of existing companies, it is hardly realistic to force all the shareholders to hold tokens. It may therefore be advisable to grant the shareholders an option between shares designed as a ledger-based security in the form of a digital token or ordinary uncertificated security. It is also conceivable to design all shares in the form of ledger-based securities in the form of digital tokens and to procure intermediated securities for shareholders who want to hold the shares via their custody account. The DLT Act is very flexible in that respect.

3.2. Minimum content

The necessary content of the registration agreement is the agreement that the right is entered in the securities ledger and can only be transferred and exercised on the basis of the ledger (Art. 973d (1) CO). First, the agreement covers the entry in the securities ledger. Beyond that, the registration agreement must also specify the rules according to which the ledger-based security will be transferred, since the law itself does not specify the mode of transfer but only makes reference to the registration agreement in that respect (Art. 973f (1) CO).
That is generally done by referring to a certain DLT protocol and/or its rules of transfer. In the case of the best-known protocols, a general reference will usually suffice ("… transferred according to the rules of the Ethereum Blockchain for ERC 20 tokens…"). In the case of the lesser-known protocols or systems with unusual properties, a more extensive explanation may be appropriate.

Finally, the registration agreement should contain a choice-of-law clause specifying the national law applicable to the transfer, thereby creating legal certainty in that respect. Art. 145a of the Swiss Private International Law Act (PILA) provides for the possibility to choose the law governing the transfer of ledger-based securities, at least for ledger-based securities that represent debt claims.

It should also be advisable to provide a rule in case an existing ledger is supposed to be carried over to a new one, e.g. for purposes of error correction or a technical upgrade.

In the case of ledger-based securities in the form of pay-to-order instruments a provision should also be included according to which the transfer of the ledger-based security is classified as an endorsement according to the rules of the system.

An example can be found in Appendix 2.

3.3. Form

The Law does not prescribe any specific form for the registration agreement. In any case, the registration agreement should be recorded in the ledger or in the linked accompanying data in accordance with number 3 of 973d (2) CO, which presupposes that the registration agreement is available in a form that can be evidenced by text. According to the Dispatch, the registration agreement may also be contained in the terms of issue or general terms and conditions. In keeping with well-established securities practices, the Parties are not required to adopt a certain wording.

4 Rights represented

Ledger-based securities may be any type of legal position under private law capable of being certificated in a security: i.e. any kind of debt claims, membership rights or rights in rem, as well as other rights such as intellectual property rights. An exception is said to be applicable according to the legislative materials for cryptocurrencies but that view is unconvincing because it would lead to interminable definitional problems and is also devoid of any basis in fact.

First of all, the transfer of the tokens follows the same technical rules as asset or utility tokens, so that the same legal issues arise in connection with their transfer. Even banknotes no longer confer a legal claim; nevertheless, their transfer is subject to the same rules as for bearer instruments, including the possibility of good-faith acquisition (cf. Art. 935 Swiss Civil Code).

Secondly, the exclusion of payment tokens gives rise to major classification problems; it is very hard to say what constitutes a pure payment token versus a mixed asset and/or utility token. Secured payment tokens such as Stablecoins, for example, do indeed confer legally enforceable claims if they are secured by and convertible into legal currency or other assets.

According to the opinion expressed here, tokens that have the function of a means of payment in whole or in part can also be structured as a ledger-based security under Art. 973d seq. CO by being registered in a securities ledger on the basis of a registration agreement. In addition, issuers of cryptocurrencies also have the option to structure them as a right *sui generis*. In effect, this amounts to an opt-in right for cryptocurrencies.

5 Interface with intermediated securities

Tokens in the form of ledger-based securities can be held directly by the investor. Certain investors, in particular institutional investors, prefer to hold tokens through the same infrastructure they are using for intermediated securities (in German: “Bucheffekten”) in order to be capable of using one single infrastructure for managing securities positions. Such a wish can easily be accommodated by creating intermediated securities on the basis of ledger-based securities through an interface established by the DLT Act. Intermediated securities are then transferred by way of credits to securities accounts (article 24 FISA) or by way of control agreements (article 25 FISA).

According to article 6(1)(d) FISA, intermediated securities are created with ledger-based securities as an underlying be delivering the ledger-based securities into an omnibus wallet maintained by a custodian (in German: Verwahrungsstelle) in accordance with article 4 FISA (i.e. a bank, a securities house, a central securities depository) and the credit of the securities to a securities account. Unlike in the case of simple uncertificated securities (in German: einfache Wertrechte, Art. 973c CO), no main registry (Hauptregister) is maintained. The custodian must keep control of the ledger-based securities as long as intermediated securities are in existence in order to satisfy the requirements of article 6(3) FISA that the ledger-based securities be immobilized.

It is in theory also possible to tokenize intermediated securities, although it is difficult to envisage an application making much sense. It should be observed, however, that the current FISA version excludes the transfer of intermediated securities by way of an operation not reflected by a credit in a securities account, e.g. by way of an assignment. The transfer of tokens representing intermediated securities would therefore only be effective if and when the transfer is mirrored in the securities account.

In case a bona fide acquirer of a certificated security and a bona fide acquirer of the ledger-based security have a conflicting claim to the same right, the former takes precedence over the latter. Therefore, any and all certificated securities must be collected and be destroyed before ledger-based securities are issued.

6 Cancellation and recovery of tokens

Art. 973h CO provides for cancellation (mortification) as a control process in the case of loss of the power of disposal over tokens (i.e. loss of the private key). The cancellation process is a procedure of voluntary jurisdiction that is relatively time-consuming and expensive. At present, it is also unclear what requirements the courts would impose for the designation of a lost token (e.g. numbering or indication of the public address).

The issuer should therefore consider providing the terms of issue with an optional process for the replacement or recovery of lost tokens. The associated prerequisites should be defined precisely. The issuer could also conceivably make the replacement conditional on depositing sufficient collateral, since a good-faith acquirer of a lost token could still derive claims from it. In the case of legal positions under corporate law, the replacement of a lost token is only possible if the company has sufficient holdings of treasury shares.

7 Information and liability

The DLT Act places quite some emphasize on disclosing the functioning of the securities ledger to investors (cf. number 3 of Art. 973d (2) CO). The organizational responsibility for doing so is imposed on the issuer (Art. 973d (3) CO). CO Art. 973i covers that organizational responsibility by requiring the issuer to provide every acquirer of a ledger-based security with certain information about the technical design of the issue (item 1). Moreover, the issuer is unconditionally liable for damage caused to the acquirer through information that is inaccurate, misleading or fails to comply with the corresponding requirements (item 2).

The duty to inform under Art. 973i (1) CO initially relates to the functioning of the securities ledger and the measures to protect its functioning and integrity. As shown by the reference to Art. 973d (2) and (3) CO, the requirements mentioned therein for the securities ledger are meant. It is therefore in the first place necessary to provide information about the four constitutive features of a securities ledger, i.e. power of disposal, integrity, the minimum required content, and public notice. It is also necessary to disclose how the securities ledger is organized and how it is ensured that it functions in accordance with the registration agreement at all times. Part of that information (functioning of the ledger and registration agreement) already form part of the minimum required content that must be recorded in the ledger or in the linked accompanying data in order to create a securities ledger in the first place (Art. 973d (2)(c) CO).

If that information is not included in the ledger or in the linked accompanying data, then it cannot even be called a securities ledger.

Moreover, number 1 of Art. 973i (1) CO also requires the issuer to disclose information about the "content of the uncertificated security”. Such information, too, forms part of the minimum required content that must be included in the ledger or in the linked accompanying data according to Art. 973d (2)(c) CO in order for it to be considered a securities ledger. It is limited to such information as is necessary to clearly define a certain ledger-based security, i.e. the designation of the type of ledger-based security, the nominal value and the denomination.

The DLT Act and the legislative materials say nothing about the details of the duties to inform. According to the legal principles governing prospectuses, which are also applicable here, the information must be complete, consistent and understandable (Art. 51 (1) Financial Services Act). The information should be made permanently accessible.

8 Example Cases

This section provides a number of examples to illustrate the interplay between the various legal and technical requirements and their impact on usability.

8.1 Refused Token Custody

A shareholder wants to store her tokenized shares with a financial intermediary. The intermediary has a token storage system in place that supports the ERC-20 standard and that automatically segregates all client tokens directly in the register, dynamically generating new addresses as needed. Unfortunately, the share tokens are subject to an allowlist managed by the issuer, which is incompatible with the custodial system of the intermediary. Therefore, the intermediary does not accept the client’s security tokens for storage unless the issuer deactivates the allowlist for all tokens delivered to the intermediary. The issuer, however, is concerned about losing control over who the shareholders are and refuses to do so. As a consequence, the shareholder cannot store her tokenized shares with her intermediary.

8.2 Security Token as Collateral

The founder of a company wants to use his share in that company as a collateral to get a credit from a bank. Art. 973g CO states that the collateralization of ledger-based securities requires the shares to be flagged in the register and that there are provisions in place to make sure that the bank can take control of the collateral in case of a default of the founder. The simplest way to achieve this is to simply transfer the share tokens into the custody of the bank. Thereby, the bank becomes the holder of the tokens according to the registry and has exclusive control over it, satisfying Art. 973g CO.

In more detail, Art. 973g CO states that if the creditor of a ledger-based security is declared bankrupt, if his or her property is distrained or if a debt restructuring moratorium is authorized, the creditor's decisions regarding ledger-based securities are legally binding and effective against third parties, provided that they (1) were made beforehand; (2) have become irrevocable under the rules of the securities ledger or another trading facility; and (3) were actually recorded in the securities ledger within 24 hours.

Moreover, collateral may be posted even without the transfer of the ledger-based security, if (1) the collateral is visible in the securities ledger; and (2) it is ensured that only the collateral recipient can dispose of the ledger-based security in the event of default. Please note that in other respects, the special lien on ledger-based securities is governed by the provisions on special liens that apply to certificated securities (Art. 895–898 et seqq. Swiss Civil Code (CC)) and the pledging of ledger-based securities is governed by the provisions on liens on debts and other rights as applicable for certificated securities (Art. 899–906 et seqq. CC)

Annex 1 - Statutes Example

The following is an example clause that enables a company to issue shares as ledger-based securities when put into the articles of association:

The Company issues its shares in the form of uncertificated securities or ledger-based securities. The shareholders are not entitled to the printing and delivery of certificated securities. The Company is authorized to convert uncertificated securities into ledger-based securities pursuant to Art. 973d et seq. CO and, to the extent permissible, ledger-based securities into uncertificated securities. The Company is also authorized to issue ledger-based securities in the form of digital tokens. The Board of Directors shall regulate the issuance and transfer of shares or tokens in the form of ledger-based securities in a set of regulations which shall be deemed to be a registration agreement pursuant to Art. 973d para. 1 CO.

German Text
Die Gesellschaft gibt ihre Aktien in Form von einfachen Wertrechten oder Registerwertrechten aus. Die Aktionäre haben keinen Anspruch auf Druck und Auslieferung von Wertpapieren. Die Gesellschaft ist ermächtigt, einfache Wertrechte in Registerwertrechte gemäss Art. 973d ff. OR und, soweit zulässig, Registerwertrechte in einfache Wertrechte umzuwandeln. Der Verwaltungsrat regelt die Ausgabe und Übertragung von Aktien in Form von Registerwertrechten in den zugehörigen Registrierungsvereinbarungen gemäss Art. 973d Abs. 1 OR.

Annex 2 – Template Registration Agreement

An editable template for a registration agreement can be found at:
http://blockchainfederation.ch/registration-agreement-template/

LEXR AG (lexr.ch) is providing this template under the following terms:

The sample document is provided ‘as is’ without any warranty of any kind. All liability is excluded to the extent permissible by applicable law. Anyone can copy and redistribute the material in any medium or format, remix, transform, and build upon the material for any purpose, including commercially. The LEXR logo and name can only be used with prior approval of LEXR AG.

Annex - ERC-20 Standard Extension

ERC-20[2] is the most popular standard for the issuance of crypto assets. The only feature it misses to satisfy the requirements of ledger-based securities is the link with the registration agreement. Further, there are several useful features, for which it is desirable to have a common standard to increase compatibility between the tokens of different issuers. The interface functions to access these features are defined in the following table:

Function Signature in Solidity	Description
`terms() returns (string)`	Returns a URL to a website on which the registration agreement can be found. Optionally, it could include a fingerprint in form of a URL parameter: “firm.com/investors?hash=0x12ab34cd”
`setTerms(string terms)`	Allows the issuer to update the link to the terms.
`setName(string symbol, string name)`	Allows the issuer to change the ticker symbol and the name of the security.
`totalShares() returns uint256`	Returns the total number of issued units of the security, regardless of their form. This could for example be useful for calculating the market capitalization of a company. This number is higher than totalSupply from the ERC20 standard if there are additional outstanding units of the security in other legal forms or in other registers. The total can also be lower than totalSupply in case there are tokens that have been declared invalid but that have not (yet) been burned.
`setTotalShares(uint256 total)`	Allows the issuer to set the total number of shares.
`announcement(string message)`	Allows the issuer to make a public announcement that is embedded on chain, for example a change of the registration agreement.

[2] https://eips.ethereum.org/EIPS/eip-20