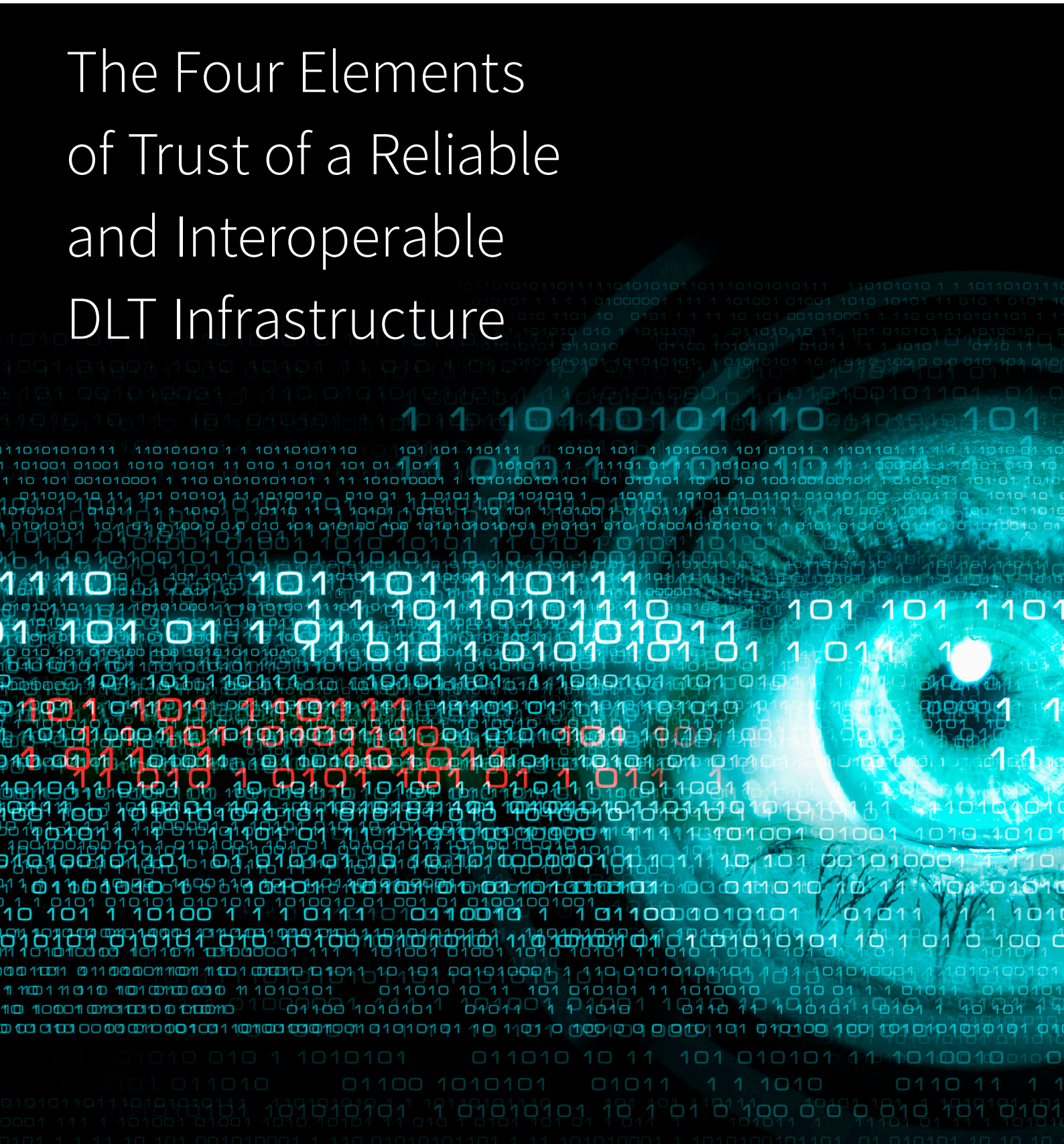
Whitepaper 4T-DLT

The Four Elements of Trust of a Reliable and Interoperable DLT Infrastructure



4T-DLT is an independent, cross-industry initiative to create an open repository for the technical and legal information, definitions and standards which apply to a secure, interoperable and reliable Swiss Distributed Ledger Technology (DLT) infrastructure.

Under the umbrella of “digitalswitzerland”, the initiative’s members are pursuing a “federative, collaborative innovation” approach with the aim of further strengthening Switzerland’s position as a leading financial center and a global innovation hub for DLT and fintech projects.

4T-DLT was initiated and is led by Dr. Luka Müller-Studer and Johs Höhener.

This Whitepaper, along with five related video recordings, have been made possible thanks to the efforts of our 4T-DLT Contributors.

4T-DLT Whitepaper Contributors:
Dr. Adrien Treccani, Aurelia Nick, Dr. Bruno Pasquier,
David Meirich, Dominic Vincenz, Fedor Poskriakov,
Gian Pfister, Gino Wirthensohn, Guillaume Gabus,
Prof. Dr. Harald Baertschi, Dr. Jacques Iffland, Johs Höhener,
Dr. Luka Müller, Marc Stammbach, Marcel Hostettler,
Dr. Mattia Rattaggi, Michael Svoboda, Nathan Kaiser, Orkan Sahin,
Patrick Oltramare, Patrick Salm, Rolf W. Guenter, Travin Keith,
Dr. Sebastian Bürgel, Dr. des. Stepan Meyer, Dr. Yannick Hausmann

September 2021

Introduction

In the current digitalization age, there is a growing need to conduct legal transactions on a purely digital basis. To this end, the Federal Council has amended several federal laws in order to take the rapid developments in technology into account. Since February 2021, rights can be mapped and transferred using Distributed Ledger Technology (DLT). These amendments are intended to increase legal certainty and to remove legal hurdles. The focus of the amendments is on securities law (including corresponding amendments to other laws, e.g., financial markets law) in the wake of the emergence of new ledger-based securities. This new law illustrates modern lawmakers' endeavors to address the challenges posed by the rapid technological developments in this field, as well as trusted digital information. This Whitepaper addresses the main technical and legal elements of a trusted digital data infrastructure.

Thematically, the Whitepaper is divided into four parts, each of which deals with a basic pillar of a trustworthy DLT infrastructure. These are referred to as the "4 Trusts" or "4Ts". The trust element of legally relevant **information ("T1")** describes how to ensure the authenticity, integrity, confidentiality and availability of information on digital assets. The trust element of **consensus ("T2")** sets out the requirements for DLT protocols (e.g., interoperability between protocols). The trust element of **custody ("T3")** addresses how digital assets can be reliably and easily stored within (self-) custody solutions (e.g., security standards, user experience, auditability). And finally, the trust element of the **transaction ("T4")** discusses how the liability (deposit of value), allocation (number of shares) and transfer (e.g., peer-to-peer between ledger-based users) of digital assets can be ensured in an efficient, legally secure and straightforward manner. The final section provides an overview of use cases that apply this infrastructure both as part of and beyond capital market activities.

A deep and common understanding of DLT by all involved parties is crucial in order to unleash its full potential. It creates the basis that digital assets and rights can be stored autonomously and transferred easily, efficiently and in compliance with the law between participants in a DLT ecosystem. Switzerland is therefore positioning itself as the world's leading location for the setting of standards for trusted digital information using technologies such as DLT.

Our objective in producing this Whitepaper is to provide a foundation for the future implementation of standards for products and services, ongoing DLT initiatives, and industry experts. Our hope is that in defining the core elements of the DLT infrastructure of the future it will further promote the understanding of all ecosystem participants, tax and supervision authorities, advisors and auditors. It is the outcome of a federative, innovative collaboration between academic thought leaders, legal practitioners, financial intermediaries, technology specialists, industry associations and regulatory experts.

This Whitepaper is the result of discussions, workshops and research, and the combined effort of all Contributors involved. Opinions expressed herein may not necessarily correspond with those of each person involved in the project, nor do they necessarily represent the views of their organizations.

We would like to express our sincere gratitude to all Contributors for their tireless efforts, both in terms of the time and intellectual work they have invested. Our collaboration with them has been challenging, constructive and a great pleasure at all times.

Luka Müller and Johs Höhener
Zurich, September 2021

Table of Contents

Table of Contents

II. T2
The Trust Element of Consensus

III. T3

Table of Contents

III. T3
The Trust Element of Custody

IV. T4
The Trust Element of Transaction 51

Table of Contents

IV. T4
The Trust Element of Transaction

Table of Contents

IV. T4
The Trust Element of Transaction

V.

VI.

Legal Basis

- Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, February 2021.
- Dispatch on the further improvement of the framework conditions for DLT / blockchain dated November 27, 2019 ("Dispatch DLT").

Bibliography

- Federal Council, DLT report, December 14, 2008.
- Fedor Poskriakov, Conservation et négoce de cryptoactifs – aspects choisis du droit des marchés financiers, in CEDIDAC Droit et économie numérique, 1ère éd., 2021, 83 et seq.
- Jacques Iffland / Ariel Ben Hattar, Central Securities Depositaries in the Age of Tokenized Securities, Caplaw-2020-05.
- Hans Caspar von der Crone / Merens Derungs, Shares as digitized values, SZW 91 (2019), 481 et seq.
- Hans Caspar von der Crone / Martin Monsch / Luzius Meisser, Share Token – A private-law analysis of the possibility to use DLT systems for the mapping and transfer of shares, GesKR 1 / 2019, 1 et seq.
- Hans Caspar von der Crone / Franz J. Kessler / Luca Angstmann, Token in the Blockchain – private-law aspects of DLT, SJZ 114 (2018), 337 et seq.
- Hans Caspar von der Crone / Fleur Baumgartner, Digitization of securities law – the issuance of shares as ledger-based securities, SZW 92 (2020), 351 et seq.
- MME, Statement of September 26, 2018 on the Consultation of the Blockchain / ICO Taskforce.
- MME, BCP Framework for Assessment of Crypto Tokens, https://www.mme.ch/de/magazin/bcp_framework_for_assessment_of_crypto_tokens/
- Rauchs et al., Cambridge University, Distributed Ledger Technology Systems, A Conceptual Framework, August 2018, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf
- Stefan Kramer / David Oser / Urs Meier, Tokenization of financial instruments de lege ferenda, Jusletter, 6 May 2019.
- Swiss Blockchain Federation, Circular 2021 / 01 on ledger-based securities, February 1, 2021.

Definitions

ACTUS	ACTUS encodes the payment obligations of all kinds of financial instruments contracts in a mathematically unambiguous and consistent form.
AML	Anti-Money Laundering
AMM	Automated Market Makers are smart contracts that create a liquidity pool of ERC20 tokens, which are automatically traded by an algorithm rather than an order book.
Asset token	Asset tokens digitally represent assets such as participations in real physical underlyings, companies, or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives.
Asset-backed token	Asset-backed tokens are blockchain-based units of value that are pegged to real-world assets, such as company shares, real estate, diamonds, or commodities.
Bitcoin	Bitcoin is a digital or virtual currency created in 2009 that uses blockchain technology to facilitate instant payments.
Blacklist	Blacklisting means a blockchain address can no longer receive or send tokens (this is sometimes referred to as “freeze”).
Blockchain	Blockchain is a type of DLT where transactions are recorded with an immutable cryptographic signature called a hash. The transactions are then grouped in blocks and each new block includes a hash of the previous one, chaining them together, hence why distributed ledgers are often called blockchains.
BLS	BLS (Boneh Lynn Shacham) digital signature is a cryptographic signature scheme which allows a user to verify that a signatory is authentic.
Burn tokens	Burning tokens decreases the total supply of tokens and the balance of the account the tokens are burned from.
Chain code	A chain code is attached to private and public keys which are then respectively referred as extended private and public keys, so as to define the derivation function.
CMTA	Capital Markets and Technology Association
Consensus mechanism	A consensus mechanism is a fault-tolerant mechanism used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems.

Definitions

CRES/wCRES token

While CRES is an ERC20 token, the CRES token contract is governed by a compliance layer. The CRES token carrying this additional governance layer to enable voting for registered shareholders is "heavier" and consumes more gas when being transferred. The wrapped ERC20 version on the other hand is a simple ERC20 token and optimized for fast and cheap transferability.

Cryptographic hash function

A cryptographic hash function is an algorithm that takes an arbitrary amount of data input, a credential, and produces a fixed-size output of enciphered text called a hash value, or just "hash". The enciphered text can then be stored instead of the password itself, and later used to verify the user.

CSD

A central securities depository (CSD) is a specialized regulated financial organization holding securities such as shares, either in certificated or uncertificated (dematerialized) form, allowing ownership to be easily transferred via book-entry rather than by transferring physical certificates.

Custodian

A custodian is a financial institution that holds clients' tokens/securities for safekeeping to prevent them from being stolen or lost.

DApp

Decentralized application that runs on a distributed computing system.

DLA

Digital ledger addresses

DLT-MTF

DLT-based multi-trading facility. A multilateral trading facility is a regulated institution for multilateral securities trading the purpose of which is the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules without listing securities.

DACS

The CMTA's Digital Assets Custody Standard (DACS) aims to clarify the differences between the storage of cryptocurrencies and traditional assets and to establish basic security and operational requirements.

DAO

A Decentral Autonomous Organization is an organization represented by rules encoded as a computer program that is transparent, controlled by the organization members and not influenced by a central government.

DLT

Distributed Ledger Technology, a system of electronic records that enables a network of independent participants to establish a consensus around the authoritative ordering of cryptographically-validated (signed) transactions. These records are made persistent by replicating the data across multiple nodes, and tamper-evident by linking them by cryptographic hashes. The shared result of the reconciliation/consensus process – the "ledger" – serves as the authoritative version for these records. The blockchain is a specific form of distributed ledger.

Definitions

DLT trading facility	Commercially operated, regulated institution for multilateral trading of DLT securities.
DLT securities	Securities entered in a DLT-based register
DTI	Digital Token Identifier
ECDSA	Elliptic Curve Digital Signature Algorithm offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.
EdDSA	Edwards-curve Digital Signature Algorithm is a digital signature scheme.
ERC20	Token standard on the Ethereum blockchain
ETH / Ethereum	Ether is the native cryptocurrency built on top of the open source Ethereum blockchain, which runs smart contracts and is an open-source computing platform and operating system.
EULA	An end-user license agreement is a legal contract entered into between a software developer or vendor and the user of the software.
EWASM	Ethereum's version of the WebAssembly – WASM – code which is an open standard that defines a portable binary-code format for executable programs.
FATF	Financial Action Task Force
Fiat	Fiat money is a currency (a medium of exchange) established as money, often by government regulation.
Finality	Moment when a transaction can be considered completed, respectively when it becomes impossible to revert or alter a transaction that has been added to the blockchain.
Fungible assets	Fungibility is the right to exchange a product or asset with other individual products or assets of the same kind. Fungible implies equal value among assets.
HSM	A hardware security module is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.
HTLC	A hashed timelock contract reduces counterparty risk in decentralized smart contracts by effectively creating a time-based escrow.

Definitions

Immobilization	Ledger-based securities are to be immobilized while intermediated securities are in existence. Immobilization requires that the securities can no longer be transferred without the involvement of the custodian.
Interoperability	Interoperability is the ability of two or more DLT networks or applications to exchange information and to mutually use the information that has been exchanged.
IPFS	The Interplanetary File System is a protocol and peer-to-peer network for storing and sharing data in a distributed file system.
ISIN	International Securities Identification Number
ISO 10962	Asset Type Classification Code to describe the structure and function of each financial instrument.
Issuer (also referred to as obligor)	Swiss company limited by shares, duly organized under Swiss law and registered in the commercial register, which uses DLT to digitize its share register and to issue digitized shares (e.g., in the form of ledger-based securities).
ITIN	Individual Taxpayer Identification Number
Key generation event	“Secret generation” or “key ceremony” of tokens
KYA	Know Your Asset information
KYC	Know Your Customer information
Ledger	Digital register in which specific information is stored securely and unalterably and grouped into data structures.
Ledger-based securities	A ledger-based security is a right which, in accordance with an agreement between the parties, is registered in a securities ledger and may be exercised and transferred to others only via this securities ledger (art. 973d para. 1 CO).
Merkle tree	A Merkle tree or hash tree is a tree in which every leaf node is labeled with the cryptographic hash of a data block, and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes.

Definitions

Mint tokens	Minting tokens increases the total supply of tokens and the balance of the account that the tokens are minted to. In the context of ledger-based securities this can be the primary issuance of equity (e.g., incorporation of a new entity) or a capital increase of an existing company.
MPC	Multiparty computation is a field of cryptography focusing on the joint calculation of mathematical functions over inputs being fragmented over multiple parties.
MTF	A multilateral trading facility is a regulated institution for multilateral securities trading the purpose of which is the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules without listing securities.
Multisig contracts	Such smart contracts require multiple signatures from different addresses for a transaction to be executed.
Multi-tokens	The ERC-1155 Multi Token Standard allows for each token ID to represent a new configurable token type, which may have its own metadata, supply and other attributes.
Native token	Native tokens can be transferred to a DLT ledger from one party to another, but do not grant any rights vis-à-vis a counterparty.
Node	A computer participating in a global peer-to-peer blockchain network.
NFT	A non-fungible token is a unit of data stored on a digital ledger which can represent a unique digital item, often used for collectibles.
ODEM	ODEM offers various services in the field of education. Its platform provides access to courses and other services. On a broader level, ODEM's platform connects educational institutions, educators, students, but also employers.
Off-chain	Transactions occurring on a cryptocurrency network which move the value outside of the blockchain.
On-chain	Transactions that occur on a blockchain that are reflected in the distributed ledger.
Open Source	Open source refers to software or other projects with source code that can be viewed, modified, or upgraded by anyone.
OpenVASP	An open-source initiative that implements a P2P communication protocol on top of the Ethereum blockchain.

Definitions

OTF	An organized trading facility is an establishment for multilateral or bilateral trading in securities or other financial instruments whose purpose is the exchange of bids.
Pause a contract	Ability to implement an emergency stop mechanism that can be triggered by the pauser role to halt or resume the contract (this is why it is sometimes called a “circuit breaker”). When the contract is paused, all transfers are blocked.
Payment token	Payment tokens are synonymous with cryptocurrencies and have no further functions or links to other development projects. Tokens may in some cases only develop the necessary functionality and become accepted as a means of payment over a period of time.
Peer-to-peer / P2P	Direct exchange of tokens between two parties without the involvement of an intermediary / third party.
Platform provider	Provider of a digital platform on which issuers can issue ledger-based securities.
Power of disposal	Legal power to dispose of a token.
Pre-operational tokens	Tokens that are not yet fully operational.
Private Key / PIK / PK	A PIK is the non-public key of the asymmetric key pair necessary to sign and transfer virtual currencies, digital assets or information.
PoW	Proof of work is a form of cryptographic zero-knowledge proof in which one party (the prover) proves to others (the verifiers) that a certain amount of computational effort has been expended for some purpose. Verifiers can subsequently confirm this expenditure with minimal effort on their part.
Proxiable	If the contract is upgradeable and uses the Universal Upgradeable Proxy Standard (UUPS30), the administrative role allows for the contract logic to be updated while maintaining a contract status. Often, this role is assigned to the owner of the smart contract.
Public Key / PUK	Public Keys are used in DLT to convert a message into an unreadable format. Decryption is carried out using a different, but matching, private key. An address is generated as a hash of the PUK.
Registration Agreement	Agreement defining the legal relationship between the issuer of a ledger-based security and its beneficiary pursuant to art. 973d para. 2 no. 3 CO.

Definitions

Revoke tokens	Revoking tokens has no effect on the total supply, it increases the balance of the account revoking the tokens and decreases the balance of the account the tokens are revoked from.
SDX	Swiss Digital Exchange
Securities ledger	A securities ledger according to art. 973d para. 2 CO refers to a ledger of securities based on a DLT infrastructure.
Security token	A security token is a type of digital asset that represents or derives its value from another, external asset and is issued on top of a third-party blockchain network.
Smart contract	A computer protocol stored and run on a decentralized basis, in accordance with a previously programmed logic.
Stablecoins	Stablecoins are cryptocurrencies designed to minimize the volatility of the price of the stablecoin, relative to a “stable” asset or basket of assets.
SWIFT	The Society for Worldwide Interbank Financial Telecommunication provides safe and secure financial transactions for its members.
Tezos	With the support of the Tezos Foundation and on the Tezos blockchain infrastructure, the project aims to network the decentralized KISS cooperatives so that the recording and storage, but also the transfer of time credits can be transparent, secure and traceable at any time.
Token	A token is a standardized smart contract called by a transaction.
Token classification	Classification of tokens according to the FINMA ICO guidelines.
Tokenization	Initial generation of tokens and / or DLT-based digitization of a right or asset, meaning the configuration of legally relevant information with DLT information.
Unhosted wallet	The term “unhosted” is applied to all situations where the private key of a wallet is managed personally and not by a third-party service or company.
Uniswap	Open-source automated market maker protocol for trustless token swaps on the Ethereum blockchain.
User (also referred to as creditor)	Registered user of a digital platform enabling the issuance of tokenized shares or other digital assets. In case of ledger-based securities, the user is also called a creditor (“*Gläubiger*”).

Definitions

Utility token	Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.
UTXO	A UTXO (unspent transaction output) is a value received by a wallet, which has not yet been spent for an outgoing transaction.
UUPS	Universal Upgradeable Proxy Standard
VASP	Virtual Asset Service Provider
Wallet	Software application or other program / service for the control (i.e., holding, safekeeping and transfer) of tokens by means of public and private keys. This is information that parameterizes a cryptographic algorithm and thus controls it.
Whitelist	Whitelist refers to a list of cryptocurrency addresses which users define as trustworthy.
Wrapped	A wrapped token is a cryptocurrency token pegged to the value of another crypto. It is called a wrapped token because the original asset is put in a wrapper, a kind of digital vault that allows the wrapped version to be created on another blockchain.

I.

T1

The Trust Element of Configuration

Authors:

David Meirich, Stephan Meyer, Aurelia Nick, Dominic Vincenz

Contributors:

Luka Müller-Studer, Johs Höhener, Sebastian Bürgel, Marc Stammbach

A. Introduction

This part of the Whitepaper focuses on T1, which stands for trust in legally binding digital information. It is divided into four separate sections. The introduction to the topic is followed by an explanation of the technical context behind legally binding digital information and the relevance of on- and off-chain digital information. An initial technical section focuses on the connection between on- and off-chain information, as well as access and role concepts. In the following section, the legal context will be described in more detail and applied to the technical requirements for the securities ledger. A specific focus is placed on the implementation of the approach to ledger-based security in Switzerland, including the Registration Agreement that defines the legal relationship between the issuer of a ledger-based security and its beneficiary.

B. Technical Context

A DLT system is a system of electronic records that enables a network of independent participants to establish a consensus around the authoritative ordering of cryptographically-validated ("signed") transactions. These records are made persistent by replicating the data across multiple nodes and tamper-proofed by linking them using cryptographic hashes. The shared result of the reconciliation / consensus process – the "ledger" – serves as the authoritative version for these records.[1]

Swiss Private and Securities Law does not use the term Distributed Ledger Technology (DLT), as it aims to provide a technology-neutral basis that can be applied to technical circumstances in practice. Nonetheless, as described below, the concept of "securities ledger" in art. 973d et seq. of the Swiss Code of Obligations ("CO") is based on the specific characteristics of distributed ledgers.

According to art. 973d CO, a securities ledger must fulfil the following technical and conceptual requirements:

1. It uses technological processes to give the creditors, but not the obligor, power of disposal over their rights;
2. Its integrity is secured through adequate technical and organizational measures, such as joint management by several independent participants, to protect it from unauthorized modification;
3. The content of the rights, the functioning of the ledger and the Registration Agreement are recorded in the ledger or in linked accompanying data;
4. Creditors can view relevant information and ledger entries, and check the integrity of the ledger contents relating to themselves without intervention by a third party.

From a conceptual point of view, there are two aspects of particular relevance for *T1 – Trust in legally binding information:* the integrity and persistence of the link between ledger-based information and off-chain accompanying data configuration as well as configuration and ledger access (role concept).

1. Technical Link (On-Chain/Off-Chain Information)

In order for the creditor / user to verify their legal position, the ledger on-chain needs to provide all relevant information (e.g., interest rate, due date, etc.). However, full details on the securities ledger itself are not required. The content of the rights can also be presented in readable accompanying data that is adequately linked to the ledger. In this scenario, a unique hash of the relevant data is stored in the ledger and serves as an immutable connection between off-chain and on-chain data.

Accordingly, the link between the ledger and related off-blockchain data must have the following characteristics:

- **Uniqueness:** The technical link should be unambiguous (or with very low collision probability), in order for the investor to be sure of the affiliation between the accompanying data and the respective ledger-based security;
- **Completeness:** The technical link should refer to all relevant accompanying data, not just to individual documents (e.g., by using a Merkle tree);

[1] *Rauchs et al., Cambridge University, Distributed Ledger Technology Systems, A Conceptual Framework, August 2018, www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2018-10-26-conceptualising-dlt-systems.pdf*

- **Location information:** The technical link should provide the investor with information on the location of the accompanying data so that they know where to look for the corresponding identifier/hash;
- **Information on timeliness:** The technical link should permit conclusions about its timeliness/validity, expiration as well as update frequency;
- **Bidirectionality:** The technical link should lead from the ledger-based security to the accompanying data and vice versa;
- **Data availability:** The availability of off-chain data must be ensured at all times and the content must be verified without the intervention of a third party.

Based on the above-mentioned characteristics and in order to ensure the integrity of the securities ledger, the following *information* is required *in the technical link* between on- and off-chain data (see I.B.1).

- **Validity:** The validity information ensures transparency between on- and off-chain resources with regard to the current valid status and updates. Creditors can therefore better assess whether regular changes are to be expected. Consequently, this mitigates the risk of the accompanying data being out of date;
- **Storage location:** The storage location information enables the creditor to query the relevant information in a targeted manner;
- **Integrity:** The "integrity information" enables the creditor to check the integrity of the information located or received. In case of the Ethereum blockchain, this can be achieved, for example, by depositing a hash value to such accompanying data, which is inseparably linked to the blockchain.

At a minimum, the new legal concept of ledger-based securities requires the respective Registration Agreement to be linked to the ledger-based security. In practice, this can be done by recording a link to a static (PDF) document with the hash number as an attribute in the document. Additional but optional documents to be linked may include the excerpt from the commercial register entry for the issuing company, its Articles of Association and – where applicable – shareholder agreements, terms of issuance, investment prospectuses, a Whitepaper or similar documents.[2]

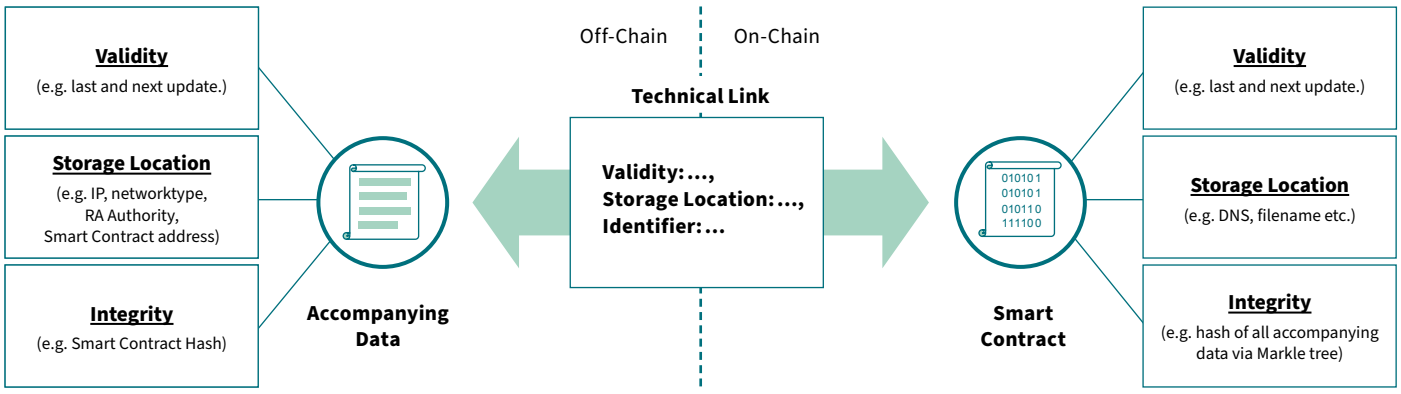


Figure 1: Technical Link On- and Off-Chain Data

[2] *KRAMER/OSER/MEIER, N 15.*

2. Configuration Access and Role Concept

From a technical point of view, there might be four different roles, each with different access rights and functionalities:

1. The **Issuer** of the ledger-based security must have access to the ledger for the purposes of the configuration and deployment of the respective smart contract ("Configuration Access"), but not to the ledger-based securities themselves (see art. 973d para. 2 no. 1 CO). Unilateral or unauthorized changes to the smart contract leads to the Issuer's contractual liability.
2. The issuer may delegate the configuration and deployment of the respective smart contract to an **Admin / Developer,** who may also conduct audits of the smart contract.
3. A **Platform Provider** – where applicable – may have a segregated access to the platform for the technical support *without* having control over the configuration and deployment of the Smart Contract ("Admin Access").
4. And finally, the **User** needs to be provided with access in order to view and manage transactions. Therefore, the investor has an exclusive transaction access, providing direct power of disposal over their ledger-based securities without any involvement of an intermediary / third-party ("Transaction Access"). The User does not necessarily need direct control over the private key related to their ledger-based securities, but exclusive control over their ledger-based securities has to be ensured technically and / or cryptographically.

Depending on the underlying rights as well as potential regulatory requirements, there are three different types of transactions of ledger-based securities:[3]

- **ID transaction+:** This kind of transaction requires that the new creditor / user is personally known to the issuer prior to a transfer. This is particularly relevant for shares with restricted transferability (e.g., restrictions on the transferability of registered shares). From a technical point of view, this can be achieved via whitelisting, which allows the issuer to ensure – through smart contract management – that only approved addresses can receive the ledger-based security.
- **ID transaction:** This transaction requires the new creditor to register with the issuer in a timely manner in order to exercise rights related to the ledger-based security. In contrast to the ID transaction+, the new investor does not necessarily have to be known to the issuer prior to a transfer. A registration is crucial to exercise the shareholder's rights (e.g., dividend payments, attending a general meeting, etc.). Referring to the previous section on the technical linking of on- and off-chain data, the description of how and where to register either needs to be part of the ledger-based security itself or the accompanying data.
- **Non-ID transaction:** By executing a Non-ID transaction a creditor is not known to the company and is not obliged to register. This applies particularly to debt instruments.

C. Legal and Regulatory Context

1. Challenge: Synchronization of Legally Relevant Information with Digital Information

Many legal systems are lagging behind the rapid developments in the technology sector. One example is the written form requirement for the assignment of uncertificated securities. Whereas in the past it was necessary to securitize the transfer process of securities in order to safeguard evidence, proof of the transfer of ownership can now be reliably provided by entry in an electronic register.

Prior to the adaptation of the Swiss Code of Obligations to developments in DLT, the major challenge with regard to the tokenization of shares effectively consisted in linking legally relevant information with DLT information ("on-chain information"). When analyzing the options for establishing, structuring or transferring rights by means of a DLT system, the data supplied by the DLT must be analyzed in detail (DLT information): Often DLT information is limited to transaction information (sender, recipient, booking, timestamp) as well as to certain information and functions additionally programmed by means of smart contracts (e.g., limited number, allocation of share to addresses, balance accounting, mapping of information, etc.). Therefore, this information is limited in terms of content.

[3] *For more information on the transfer of ledger-based securities, please refer to Part IV of this Whitepaper (T4 Transfer of Tokens).*

Only by synchronizing DLT information (booking entries and information from smart contract) with

- legally relevant information (content-related **information synchronization,** on-chain / off-chain);
- the actual transfer of rights (**synchronization of rights transfer;** see T4); and
- the holder of rights (**rights holder synchronization**)

can an inseparably interlinked, simultaneous transfer of rights and tokens from one beneficiary to another be guaranteed. Although the actual DLT information constitutes important transaction data, it is, on its own, not enough to (a) generate legally relevant information (i.e., for content information synchronization), nor (b) to transfer the right (i.e., right transfer synchronization), nor (c) to clarify ownership of the right (i.e., for right holder synchronization). Against this background, the digital securitization of rights had to be considered within the context of the digital infrastructure used (cf. Figure 2 below).

Pursuant to the Swiss legislation and legal concept in place prior to the DLT amendments to federal law, the inseparable link between the token and the underlying right could not be provided. Although contractually connected to a certain degree, the right existed independently from the respective token, and the token and the right could be separated (transfer of token without transfer of right). The token – which only acted as a representation of the right, and not as its actual embodiment – had the function of a (rebuttable) proof of ownership of a right by the token holder.

2. Solution: The Ledger-Based Security According to Art. 973d. et seq. CO

With art. 973d et seq. entering into force, the Swiss Code of Obligations allows for the digital registration of rights in electronic registers ("securities ledgers"), thereby recognizing the automatic, systeminherent synchronization of legally relevant and DLT information as described above.

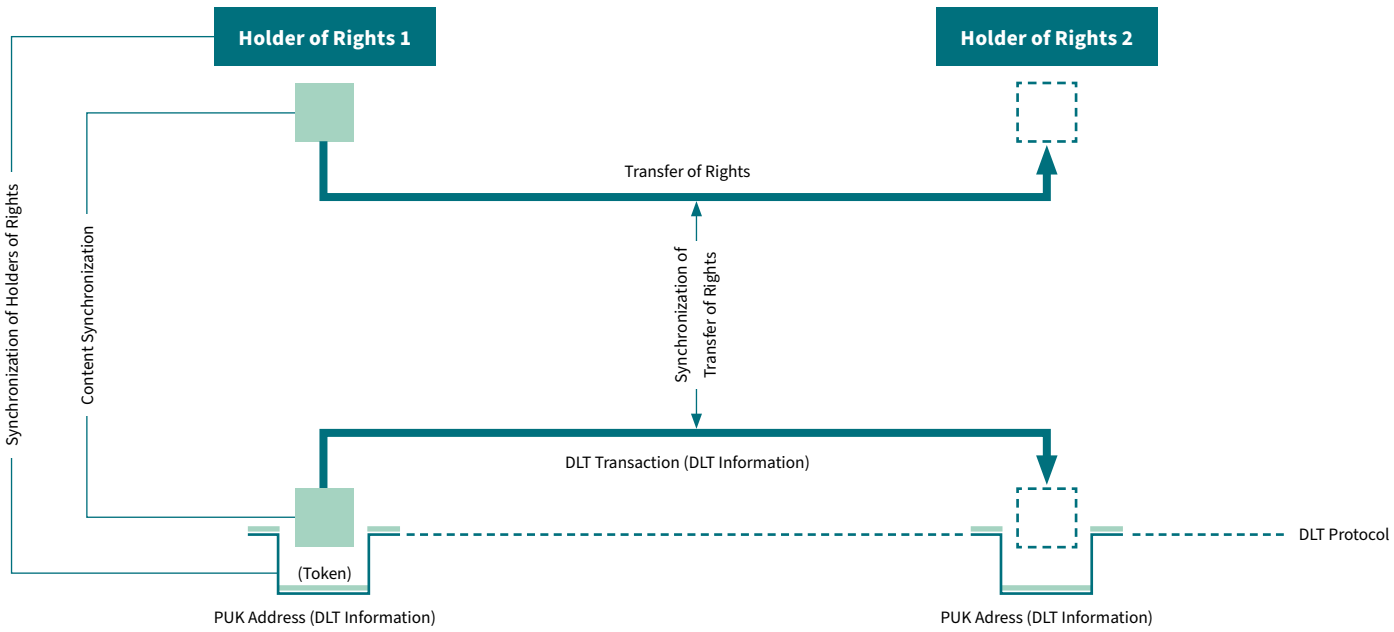


Figure 2: Three-Layer Synchronization of Rights

According to art. 622 para. 1 CO, a statutory basis is required for the issuance of shares in the form of uncertificated (art. 973c) or ledger-based (art. 973d) securities. The Articles of Association may either provide for a direct link between the shareholder position and a token (new – primary – *issuance* of tokenized shares, resp. of ledger-based securities) or authorize the Board of Directors to tokenize existing shares that have been previously issued in another form (*conversion* of uncertificated securities or negotiable securities into ledger-based securities). According to art. 973d para. 1 no. 1 CO, ledger-based securities are created by mapping the respective rights to an electronic register which meets the legal requirements as set forth in art. 973d para. 2 CO (see B 1 above). The securities must be mapped to the securities ledger in such a way that they are visible to the other users. The parties who are entitled to and bound by the right must consent to its electronic registration. The issuance is subject to formal (contractual) requirements and must be agreed on between the issuer (obligor) and the creditors (e.g., shareholders) in a what is referred to as a "Registration Agreement" (see Section 2.2.2. below).[4]

2.1 Qualification as Ledger-Based Securities

2.1.1 Short Excursus: Importance of Token Classification

Key elements that are crucial for the classification of tokens include the existence and type of counterparty along with the presence of an underlying asset or value. For example, if the token includes some form of asset and a counterparty, it will have significant legal and regulatory differences compared to a native "currency-like" token. All tokens are transferable property that may carry out certain functions, including the transfer of rights or revenue.

By way of an example for the many token classifications, in February 2018, the Swiss Financial Market Supervisory Authority, FINMA, published guidelines ("ICO Guidelines") setting out how it intends to apply financial market legislation to the handling of enquiries regarding the applicable regulatory framework for initial coin offerings ("ICO"). This classification was mainly based on the intended functionality, whether the token should be used as a means of payment (payment token), provide a utility (utility token) or transfer other assets (asset tokens). More private law-oriented frameworks, respectively token classification models, distinguish whether: i) the token holder does not have any rights vis-à-vis other parties (native token), ii) the token transfers relative rights (counterparty token), or iii) serves as an instruction instrument to transfer absolute rights as ownership of physical assets or IP (ownership token).

a) Native Token

Native tokens can be transferred in a DLT ledger from one user to another, but do not grant any rights vis-à-vis a counterparty. The owner of a native utility token does not have any relative or absolute right, except for the right relating to the token itself. The relevant criteria for this category consist of the lack of a relative right against a counterparty, such as the token generator or a third party.

b) Token in a Counterparty Context

Tokens which (shall) grant a relative right to the holder entitled thereto vis-à-vis a third party are referred to as "counterparty tokens". The underlying relative right can be structured in different ways:

- a right to purchase or use products or services;
- a right to receive a financial payment;
- a right to receive an asset (*Vermögenswert*);
- a right to receive a bundle of shareholder or membership rights.

In order to create a functioning tokenization model, synchronization on three layers is required: (a) the additional information relevant to the right with the token (*content information synchronization*), (b) the actual transfer of the right (*right transfer synchronization*) and – if necessary – with (c) the authorized right holder (*right holder synchronization*). Without content information synchronization, a token cannot represent either a relative or an absolute right.

[4] *VON DER CRONE/BAUMGARTNER, 355 f.*

2.1.2 Content of Ledger-based Securities

All rights that may be securitized as (classic) securities may also be issued as ledger-based securities. These include membership rights (if provided for by law), rights in rem (if provided for by law, such as mortgage certificates pursuant to art. 842 Civil Code)[5], or bond issues secured by a lien pursuant to art. 875 Civil Code) and all kinds of claims. Consequently, not only asset tokens, but also utility tokens (in line with FINMA ICO guidelines) may be structured as ledger-based securities as the latter often represent claims under civil law. Finally, the new regulation may also cover tokens issued as a means of payment (e.g., stablecoins) if the token represents a claim against the issuer.[6] Pure cryptocurrencies, crypto-based payment instruments (pure payment tokens) or utility tokens, which do not give rise to a claim against a counterparty (i.e., the issuer), do not qualify as ledger-based securities.

In analogy to the intermediated securities, the electronic register must be able to provide information about the securitized right. According to art. 973d para. 2 no. 3 CO, the content of the rights must be recorded in the register or in associated accompanying data. This information must be made permanently[7] accessible to creditors and protected against unilateral changes. Art. 973d para. 2 CO further requires that creditors be able to inspect and verify all information and register entries concerning themselves without the intervention of third parties, in particular without the involvement of the obligor.[8]

2.2 Contractual Setup

The issuance of ledger-based securities is embedded in a multilateral contractual basis. Four independent, yet interrelated contractual relationships form the basic legal pillars of the issuance of ledger-based securities. The core element is the Registration Agreement between the issuer and the holder of the ledger-based security.

2.2.1 Contractual Relations

Issuing shares as ledger-based securities requires a Registration Agreement between the issuer and the initial, original investor. For reasons of transparency and clarity in legal transactions, a registration clause must subsequently be recorded in the register itself or in associated accompanying data. This registration clause will also apply to all subsequent investors when the ledger-based security is transferred to them.[9]

Due to practical reasons, it is therefore recommended that the Registration Agreement be structured as a set of general conditions, as they can be attached to a share purchase agreement if shares are transferred. The Registration Agreement sets out the prerequisites and conditions for the registration of rights in a securities ledger. Furthermore, all rights and obligations of the parties arising out of the Registration Agreement are outlined therein (see section 2.2.2. below).

Besides the Registration Agreement, other contractual relationships may arise depending on the specific setup. The following provides an overview of the necessary contractual agreements to be concluded in the following two cases: (*a*) the obligor issues ledger-based securities directly without a third-party platform provider (on a public permissionless DLT infrastructure); and (*b*) the obligor issues ledger-based securities via a third-party platform provider (using either a public permissionless DLT infrastructure or a private permissioned DLT infrastructure):

a) Obligor Issues Ledger-Based Securities Directly Using a Public Permissionless DLT Infrastructure

- **Registration Agreement: Obligor – Creditor** (art. 973d para. 2 no. 3 CO). The issuer (obligor) of the ledger-based security and its original purchaser (recipient, creditor), are required to conclude a Registration Agreement. The purpose of the Agreement is to define the rights and duties of each party regarding the functionality of the ledger and also the transfer mechanism based on the relevant underlying infrastructure;
- **Share Purchase Agreement.** A Share Purchase Agreement must be concluded between creditors in the case of peer-to-peer transfers (purchase or sale) of ledger-based securities.

[5] *Dispatch DLT, p. 45.*

[6] *Dispatch DLT, p. 44 et seq.*

[7] *The short-term unavailability of the information should not call the securities effects of the registered rights into question. In order to establish the necessary disclosure, however, it will still be necessary to require that the possibility of inspection is available as a rule.*

[8] *VON DER CRONE/BAUMGARTNER, 355 et seq.*

[9] *KRAMER/OSER/MEIER, N 24.*

b) Obligor Issues Ledger-Based Securities via Platform Provider

- **Registration Agreement: Obligor – Creditor** (art. 973d para. 2 no. 3 CO). The issuer (obligor) of the ledger-based security and its original purchaser (recipient, creditor), are required to conclude a Registration Agreement. The purpose of the Agreement is to define the rights and duties of each party regarding the functionality of the ledger and also the transfer mechanism based on the relevant underlying infrastructure;
- **Terms of Use: Platform Provider – Creditor.**[10] All creditors seeking to use the respective platform to access the functionalities on the ledger to receive, store and transfer ledger-based securities are subject to Terms of Use of the platform as stipulated by the platform provider;
- **Platform Usage Agreement: Platform Provider – Obligor.** Another contractual relationship emerges between the issuer (obligor) and the provider of the digital platform providing a user interface by means of which the ledger-based securities are configurated and issued on a DLT infrastructure (platform provider). The issuer and the platform provider are subject to a Platform Usage Agreement, setting out the Terms and Conditions for the issuance of ledger-based securities on said platform;
- **Interface Agreement: Platform Provider – Infrastructure Provider.** In cases where ledger-based securities are issued on a private permissioned DLT infrastructure, a contractual relationship emerges between the platform provider and the provider of the underlying technical (DLT) infrastructure ("infrastructure provider") on which the platform user interfaces are built. The platform provider and the infrastructure provider are subject to an Interface Agreement, setting out the Terms and Conditions for the access and functioning of the DLT infrastructure.
- **Share Purchase Agreement: Creditor – Creditor.**[11] A Share Purchase Agreement must be concluded between creditors in the case of peer-to-peer transfers (purchase or sale) of ledger-based securities.

The obligor must ultimately ensure that the securities ledger operates in accordance with the Registration Agreement at all times. According to art. 973i CO, the obligor is liable for damages incurred by the creditors, unless the obligor can prove that they acted with due diligence. However, since (in most cases) the obligor is not the developer, operator and / or administrator of the underlying technical infrastructure, they will have to enter into a contractual relationship with service providers such as a platform provider of their choice (see above Platform Usage Agreement).

In the case of public permissionless DLTs, there usually is no contractual or license relationship between the obligor and developers working on the infrastructures or related protocol foundations. The same applies to the platform provider developing their solutions on the basis of public permissionless protocols.

The Platform Usage Agreement as well as the Interface Agreement as outlined above contain, in particular, the technical specifications, including service level support, between the two parties. However, the parties to the agreements are not the same. In the event of a technical failure and liability vis-à-vis the creditors, the obligor has a right of recourse against the platform provider based on and to the extent agreed in the Platform Usage Agreement. Where the platform is based on a public permissioned DLT infrastructure, the platform provider also has an Interface Agreement with the infrastructure provider, which consequently provided them with a right

[10] *Creditors of ledger-based securities may require access to a provider's platform to receive, hold and transfer them digitally. For this purpose, they must go through an onboarding and registration process with the tech provider, thereby becoming platform users. As part of the onboarding process, creditors must agree to Terms and Conditions defining the purpose rights and the limits of use. The platform Terms of Use may also include data protection provisions relating to access, use, retention, and distribution of user data.*

[11] *Any transfer of ledger-based securities is subject to a Share Purchase Agreement (or an equivalent underlying transaction, such as a Donation Agreement) between the assigning (seller) and the acquiring (acquirer) investor. The ledger-based securities are transferred digitally and without written form via the securities ledger. The transfer itself is subject to the provisions set out in the Registration Agreement (art. 973f para. 1 CO). Upon entry in the securities ledger (resp. shareholder register), the acquirer is recorded as the new owner (resp. shareholder) of the ledger-based security.*

of recourse vis-à-vis the infrastructure provider based on and to the extent agreed in the License Agreement.

Depending on the specific Platform Usage Agreement, the platform provider in the case of private permissioned DLTs also ensures that the underlying technical infrastructure fulfils the legal requirements with regard to data integrity, adequate technical and organizational measures, as well as joint management by several independent network participants.

2.2.2 The Registration Agreement

The contractual core of every ledger-based security is its Registration Agreement. As out-lined in Section B, the recording of rights in a securities ledger is subject to certain technical requirements. The parties who are entitled to and obliged by these rights are required to consent to this registration contractually. The declarant becomes a (classic) holder of rights by agreeing that the performance owed must be validly rendered only against presentation of the paper (double-sided presentation clause or simple security clause). The agreement to assert or transfer a right only via a tamper-resistant securities ledger is equivalent to this. A right becomes a ledger-based security only upon this agreement, whereby the underlying right either already exists or is newly created upon registration at issuance. The agreement to register a security digitally may also be concluded via Terms and Conditions of Issue, Bond Terms and Conditions or General Terms and Conditions, which must be accepted at the latest when the ledger-based security is acquired.[12] In addition, the Registration Agreement defines the rules for transferring ledger-based securities by taking the details of the underlying infrastructure into account. Especially in public permissionless DLT systems featuring gradual transactions, it should be clearly defined when a transaction has been finalized along with rules as to whether the ledger-based security can be transferred by handing over the private key outside of the securities ledger.

The law provides for minimum requirements only in respect of the content and the effects of the Registration Agreement as a contract between the parties. The issues to be covered by the Registration Agreement can be summarized as follows:

- **Operability.** The obligor must ensure that the securities ledger which usually consists of both an underlying infrastructure and a smart contract on the application layer is organized in accordance with its intended purpose. In particular, the obligor must ensure that the ledger operates in accordance with the Registration Agreement at all times.
- **Performance.** Pursuant to art. 973e CO, the obligor under a ledger-based security is entitled and obliged to render performance vis-à-vis the creditor specified in the securities ledger only, and subject to appropriate modification of the ledger. By rendering the performance due at maturity to the creditor specified in the securities ledger, the obligor is released from the obligation even if the specified creditor is not the actual creditor, unless the obligor is acts in bad faith or with gross negligence.[13]
- **Effects.** When acquiring a ledger-based security in a securities ledger from the creditor specified therein, the acquirer is protected even if the seller was not entitled to dispose of the ledger-based security, unless the acquirer acted in bad faith or with gross negligence. The obligor may only raise objections against claims arising out of a ledger-based security, which:
  (i) are aimed at contesting the validity of the registration or derived from the securities ledger itself or its accompanying data;
  (ii) they are personally entitled to raise against the current creditor of the ledger-based security; or
  (iii) are based on the direct relationship between the obligor and a former creditor of the ledger-based security, if the current creditor intentionally acted to the detriment of the obligor when acquiring the ledger-based security.[14]
- **Replacement and Conversion.** In addition, the obligor is entitled to change the type of securitization at any time, i.e., they may replace fungible negotiable securities or global certificates with uncertificated securities or ledger-based securities provided the Conditions for Issue or the Articles of Association provide therefor, or the bailors have consented

[12] *Dispatch DLT, p. 44.*
[13] *Dispatch DLT, p. 51 et seq.*
[14] *Dispatch DLT, p. 53 et seq.*

thereto. They are required to inform the creditor within a reasonable period of time of the impending change in the type of securitization and subsequently deliver the corresponding securities or proof of ownership to the creditor.[15]

– **Liability:** In the event of a mere temporary malfunctioning of the register, the security character of the ledger-based securities shall be preserved. The obligor shall undertake all steps set out in the Registration Agreement to safeguard the operation and integrity of the ledger. The obligor is liable for any damages incurred by the acquirer arising out of information that is inaccurate, misleading or in breach of statutory requirements, unless they can prove that they acted with due care. Any agreements that limit or exclude this liability are void.

The Registration Agreement should ideally also define constellations in cases where changing from one securities ledger to another is desired. This could be the case if doubts about the integrity of the first securities ledger arise, or if new technologies are introduced. Changing the type of securitization of a right also requires the consent of all parties involved, i.e., the obligor and the creditors at the very least. A prior contractual arrangement could make it considerably easier for the obligor to change the ledger provided the agreement contains adequate provisions.[16] Apart from replacing the securities ledger, in certain constellations, different ledgers for the primary market issuance and secondary market trading might be used. Provided the Registration Agreement precisely defines the details and the relevant legal requirements with regard to data integrity, the uniqueness of the ledger-based security and exclusive control are fulfilled, the interoperability of securities ledgers would appear to be feasible.[17]

3. Delimitation of the Financial Market Infrastructure

3.1 Ledger-based Securities as DLT Securities Pursuant to FinMIA

According to art. 2 let. b of the Financial Markets Infrastructure Act ("FinMIA"), standardized certificated and uncertificated securities, derivatives and intermediated securities suitable for mass trading are qualified as securities (*Effekten*).

With the entry into force of the DLT amendments to the FinMIA, ledger-based securities, if standardized and issued *en masse,* are deemed to be DLT securities (*DLT-Effekten*). The provisions of financial market law that are applicable to securities will apply to DLT-securities accordingly.[18]

3.2 The DLT Trading Facility[19]

The DLT amendments to federal laws introduced a new type of financial market infrastructure to the FinMIA, namely a license category specifically addressing trade and post-trade (including custody) in DLT-based securities.[20]

Similar to existing (traditional) trading venues, the DLT trading facility will allow for multilateral trading in securities, i.e., the simultaneous exchange of offers among several participants and the conclusion of contracts in line with non-discretionary rules. However, the DLT trading facility differs in terms of the securities that can be traded on it, namely, the aim of the DLT trading facility is the exchange of DLT securities. Pursuant to art. 973d CO, DLT securities include ledger-based securities and also securities issued under foreign laws provided they fulfill the (legal and technical) requirements for DLT securities as stipulated by the FinMIA. In addition, all of the tokens set out in the FINMA ICO Guidelines (asset tokens, payment tokens, utility tokens) may be traded on a DLT trading facility.

[15] *Dispatch DLT, p. 44.*

[16] *Dispatch DLT, p. 44.*

[17] *For more information on the interoperability of ledgers, please see Part II of this Whitepaper (T2 – Consensus and (Inter-)Operability).*

[18] *Dispatch DLT, p. 31.*

[19] *For more information on the transfer of ledger-based securities and trading in DLT securities (via a DLT trading facility), please see Part IV of this Whitepaper (T4 – Transfer of Tokens).*

[20] *Dispatch DLT, p. 40.*

D. Conclusion and Outlook

Establishing trust in legally binding digital information is crucial and forms the starting point for any reliable and secure DLT infrastructure. This trust can be achieved by securely programming and configurating smart contracts, respectively by accurately synchronizing off-chain and on-chain information. It is only by effectively linking off-chain documents (such as the Registration Agreement) to the respective DLT information that the potential of this newly introduced technology may be efficiently realized in practice.

The DLT amendments to Swiss federal laws allow, inter alia, for the secure, fully electronic issuance and transfer of ledger-based securities, thereby improving legal certainty with regard to tokenization. It also helps to further promote Switzerland's attractiveness as a leading hub for financial market institutions and technological innovation against the background of a sound regulatory environment. However, the Code of Obligations does not specify details regarding the transfer of tokens, nor does it stipulate the requirements for the underlying technical infrastructure of a securities ledger.

Therefore, market participants, together with the regulators, will show how the DLT legislation will be implemented in practice, and they will also determine the standards that will prevail in the respective markets.

II. T2
The Trust Element of Consensus

Authors:
Mattia Rattaggi, Travin Keith

Contributors:
Yannick Hausmann, Michael Svoboda

A. Introduction

The emergence of distributed ledgers over the course of the last ten years or so and the exponential rate of their adoption constitute a highly significant technological advancement – comparable to the introduction of computers, the internet and mobile telephony.

The move from centralized ledgers, whereby participants and the transactions conducted between them are administered centrally and the central authority gains trust in the system through sophisticated governance and audit rules, to distributed ledgers, where transactions are not processed centrally and trust is based on mere technology, constitutes a paradigm shift. This became possible when the issue of "double spending" was resolved without the need to trust a central authority, i.e., when a consensus mechanism was defined and implemented in order to grant full trust to all participants regarding the nature and validity of direct transactions between them.

While specifying and implementing a consensus mechanism within the context of distributed ledgers is a necessary criterion for technology like this to emerge, other aspects need to be addressed in order for the technology to be generally adopted. As the development of financial DLT infrastructure is still in its infancy, the definition of standards will require time and coordination between industry participants. As a first step, this Whitepaper aims to highlight some of the challenges and outlines a number of principles which should adhere to. Key aspects which we develop in this paper concern the need for standardization to ensure seamless execution of transactions within the context of a distributed ledger, and the way communications between distributed ledgers should be organized in terms of minimum standards so as to avoid the interface between various distributed ledgers becoming the "weak link" that compromises adoption and the benefits associated with distributed ledger technology. We propose ten general minimum standards.

B. Technical Context

1. Distributed Ledgers and Consensus

a) Ledger Functionality

Centralized ledgers have been the backbone of economic transactions since the dawn of civilization. Evidence that centralized ledgers were used to record events dating back to over 5,000 years ago was found in the ancient city of Uruk, Mesopotamia (modern day Iraq) in the form of an engraved stone. The need to record data independently from individual memory is probably much older and linked to the development of sedentary societies. The double-entry accounting system introduced in northern Italy 700 years ago was a key step in the history of centralized ledgers and a key determinant of the capitalist system governing our society ever since. The system ubiquitously governs economic activity in our societies, including the activity of banks and central banks. Apart from economic activity, any kind of shared event is typically registered in a centralized ledger. In transactions, the centralized ledger acts as the intermediary. Each centralized ledger has its own administrator, who manages it within the context of the governance and audit rules required to ensure trust in, and the correct functioning of the system.

b) Distributed Ledgers

Distributed ledgers store information on events or transactions executed between networked individuals in a fully secured and trustless way, without the need for a centralized ledger, centralized intermediary, or central authority. The information stored is the same across all participants and verified by cryptography among the group of users in line with a predefined network protocol. There is no need for trust in the administration of a centralized ledger and transfer of data and values can occur directly between the parties. Distributed ledgers use independent computers owned by each participant to record, share and synchronize transactions in each ledger (instead of keeping data centralized as in a traditional ledger).

c) Consensus on Spending (No Double Spending)
An important hurdle in the introduction of a valid and functioning decentralized ledger has been finding a solution to the issue of double spending, i.e., ensuring that a participant in a distributed ledger system can only transfer a value and ownership of it directly to another participant once and not to multiple participants. Distributed ledgers use cryptographic and algorithmic methods to ensure double spending cannot occur. In the case of the popular bitcoin blockchain, when a participant wishes to add a record of transactions to the shared ledger, the transaction information is shared across the entire network to all "nodes" (groups of participants) and network participants collectively determine the validity of the transaction in line with a predefined algorithmic validation method – referred to as the "consensus mechanism". Only after validation can all participants add the new block to their respective ledgers. In brief, in a distributed ledger environment, untrusted parties come to an agreement on the status of the database without the need to rely on an intermediary.

d) Consensus Mechanism
A key differentiator between distributed ledgers is the prevailing consensus mechanism. Public distributed ledgers use a consensus method that is not controlled by any one party but is instead collaboratively agreed to by all participants in the blockchain. The bitcoin block-chain uses "proof of work" (PoW) to establish consensus in the global decentralized network. PoW is generated by repeatedly running one-way cryptographic hashing algorithms until a string of numbers that satisfies a predefined but arbitrary criterion is produced. This then determines which nodes involved in the processing of adding new transactions, known as mining nodes, compute the next block of transactions to be included in the blockchain, thereby collecting the integrated transaction fees as well as the set block reward, which decreases by half approximately every four years. The process is complex in computational terms and imposes a significant computational cost on network participants for processing new entries in the distributed ledger, due to the competition involved in processing the next block. Ethereum's plan for the digital currency Ether (ETH) will require significantly fewer computing resources. This is called "proof of stake" (PoS) and it allocates a greater probability of processing the next block for nodes that are actively participating in the processing system based on coins held and actively staked over computing power. Although details regarding staking vary among implementations since its inception in 2013, in general, the network coin is used as the determinant for this amount.

e) Permissioned Distributed Ledgers
Permissioned distributed ledgers feature an even wider variety of consensus mechanisms and their implementations in order to fulfil more specific requirements. However, they generally do not have open access to participate in the network processing according to its respective consensus mechanism as restrictions on who can and cannot enter are usually in place. This may differ from those who may participate in the network in terms of initiating and receiving transactions. A fully private blockchain is one where permissions to write, read and execute are administered centrally and participants are fully limited by means of permission. However, permission to read the ledger may be granted to those who are not part of the network in a defined, bespoke way. Hybrid or federated constitute common implementations between fully public and fully private distributed ledger environments. In these models, the consensus process is limited by a selected set of participants, each of which operates a processing node and of which the majority must record each addition in the ledger in order for the addition to be valid.

f) Efficiency Gains
A distributed ledger environment provides a number of advantages, such as a shared common view of the transaction history, status and security (a distributed ledger system is designed to prevent tampering and fraud), as well as transparency, openness, and trust. A setup like this improves ledger auditability, compliance processes (as records cannot be tampered with), data management (through real-time sharing across all participants and the general public, and transparency in respect of data provenance), the concept of ownership (by design there is no

need to verify the history of the transacted item beyond the ledger), processing and verification of transactions (as no centralized verification is required), and management costs (less oversight than for centralized ledgers; no process duplication).

2. The Need for (Inter-)operability Standards

The discussion surrounding the issue of consensus and trust that has emerged with distributed ledgers and how it is addressed is based on the assumption that transactions are recorded in only one type of distributed ledger.

When moving from theory to practice, achieving seamless transactions within the context of a single distributed ledger requires solving and specifying a number of parameters and processes at various levels.

A focus on financial securities, formats and descriptions of the reference data characterizing the securities needs to be standardized to avoid the risks of a loss in quality and the need for reconciliation and manual intervention. Standardization extends to legal aspects, such as company Articles of Association and Registration Agreements. The provision of standards is required in order to facilitate the integration of security registers. For plausible reasons, each participant may need to add additional functionality to the securities transacted on the distributed ledger, such as payout features. The same may apply to custody solutions, where participants will need to agree on interfaces and operating standards in order to deal with these kinds of features in connection with securities. If not, the integration efforts and operational complexities that arise, for instance for custody solutions, could cancel out many of the benefits of distributed ledger-based securities. Adequate standards are needed to ensure that securities are unambiguously identified across the participants. Identifiers such as ISIN have helped to prevent errors and automate processes in the traditional financial infrastructure. Concepts like this need to be adapted and implemented in the context of distributed ledgers (for instance, ITIN or DTI).

Achieving seamless transactions between various distributed ledgers is equally important. Transactions between various distributed ledgers are unavoidable given the proliferation of various distributed ledger solutions legitimately responding to different requirements. It is clear that the interface between various distributed ledgers cannot become the weak link and compromise the communication of digital information stored in distributed ledgers, thereby negatively affecting adoption and benefits.

One of the key technical challenges is to ensure the delivery versus payment (DvP) of a securities transaction between two different distributed ledgers. Imagine a security exists on one ledger (e.g., Corda) and the cash leg or other asset on a different ledger (e.g., Ethereum). There are two approaches to dealing with this: either a trusted intermediary is involved or parties agree on technical solutions, such as hashed timelock contracts (HTLC) which ensure an atomic execution of this kind of a trade. Based on this approach, there are also additional legal issues that need to be considered. For example, where is the legal right represented? Is the right still recorded in the original security register (and synchronized with the second ledger) or is an additional security register created on the second ledger? When is legal finality regarding the security transfer achieved and when can the right be claimed?

The next section proposes ten principles and minimum standards that all distributed ledger interfaces should adhere to in order to achieve effective, secure and flawless communication.

C. Ten Principles for Trusted Interfaces

1. Open Source

All core software involved in the interoperability of DLT networks must be issued under an open-source license in order to assure neutral accessibility to the software, auditability of the code by any party that interacts with it, and replicability and redeployment when improvements and repairs are required. A list of

acceptable software licenses recognized as open source can be found here, which include licenses such as the MIT license, GPL and its versions, as well as Apache licenses: https://opensource.org/licenses.

The availability of the source code which can be audited by anyone is one of the key aspects of an open-source license. It permits all parties involved in transactions to not only validate the preceding history and other relevant data without needing to trust other parties involved, but also verify that the bridges connecting the DLT networks themselves did not alter any data along the way.

However, the availability of the source code alone is not enough for a software license to be categorized as open source, it must adhere to the Open Source Definition. This brings added benefits such as not allowing the core software to restrict other software, thus maintaining neutrality. Without this neutrality, the interoperability core software may restrict the use of third-party software working with it to certain proprietary software, potentially creating a vendor lock-in.

Another key benefit is allowing derived works. This means that anyone may copy the core software code, and then launch their own interoperability bridge. This is especially useful when compared to proprietary software because if the company that owns the software shuts down the program, the bridge is no longer accessible and another company would need to create an entirely new bridge. However, if the code was open source, it would simply be possible for anyone who has the code to launch the software again, or, other entities would already be hosting the same software and thus virtually removing network downtime caused by administration-related issues.

2. Data Integrity Preservation

The possibility of tampering with the data transferred across DLT networks during the process must be excluded. The authenticity of the data must remain verifiable in order for those concerned with the data to be able to confirm that it has not been tampered with. When data is transferred or used outside of a DLT network, the possibility to authenticate the data on the original DLT network must be maintained.

This can be done by having the data go through a cryptographic hash function, such as SHA-256, and have the resulting hash included before the data is bridged over to another DLT network. Consequently, anyone receiving the data can verify independently that the data remains unmodified by verifying that the hashes match after running the data through the same cryptographic hash function. The hash could also be digitally signed with PGP by the party sending the data across networks, signifying that the hash was the data intended to be sent as it can be verified by any party using the sender's public key.

3. Assurance of Data Privacy

The transfer of data across DLT networks should not require the disclosure of additional confidential information or the decryption of the transferred information in order to respect the privacy of the parties involved in the data. This does not affect data that is already freely and publicly available.

This does not in any way impede Principle II, as the data, though encrypted, can still be run through a cryptographic hash function.

4. Minimal Trust Required for Third Parties

To ensure the trust of third parties, the transfer of data across DLT networks must only create minimal additional requirements that are limited to the execution of the transfer itself. Verification of the data and any information related to it must be possible without the inclusion of any third party involved in the bridging.

A relevant example is where data is transferred over a bridge unencrypted, and a bridge encrypts the data or part of the data itself, then charges a fee in order to have the encrypted data decrypted for the interested parties.

5. Maximum Security

The transfer of data across DLT networks should be organized in such a way as to minimize the risk of successful attacks on the interoperability points from any point of view.

This can be facilitated by having multiple bridges available for various DLT networks. This lowers reliance on one bridge and therefore reduces the incentive to attack a specific bridge.

Maintaining other good security practices, such as performing an audit, applying a security disclosure program, or even better, a bug bounty program, as well as securing development channels, would further help to achieve the best security possible.

6. Network Agnostic

The transfer of data across DLT networks must be organized in an agnostic way vis-à-vis various DLT networks and their implementations.

Although network-specific bridges can be created, there must not be any conscious effort to alienate a specific DLT network and their implementations by regulation, except in the case of a breach of these principles.

7. Maximum Transparency

The transfer of the data across DLT networks must include a two-way verification protocol in order for the parties interested in the data in the new network to be able to verify other relevant information, such as previous data holders, in the previous network. In addition, parties in the former network must be able to validate the history of the data after it has crossed to the new network.

This is in addition to Principle II, which allows for the payload data itself to be verified, both in terms of authenticity as well as provenance, as of the point where the interoperability bridge is crossed. In order to meet these additional requirements, read-only access, such as a specific link to a public block explorer page, may be provided to the network explorer of the source network, which can be included in the source transaction before entering the bridge. This would allow recipients of the data on the new network to verify further provenance of the data where necessary.

In the event that this is not fully possible, e.g., in the event of a privately-hosted network within a consortium, the link may feature additional access restrictions, such as encrypting the data visible on the network explorer and requiring the intended recipient to utilize a shared key provided by the sender in order to decrypt the relevant information. This decryption would therefore only permit the intended recipient to view all relevant information on the source network in order to determine provenance, and nothing more.

8. Minimum Friction

The transfer of data across DLT networks must be organized as seamlessly as possible, without any undue burden exerted on the participating parties, such as creating additional requirements stored off the DLT networks in order to circumvent principles. These work-arounds would normally be achieved by creating third-party user interfaces of the bridges that would then require further data in order for the bridges to work, even though the core software does not feature the requirements itself.

Additional examples of friction would be the creation of laws that supersede the open-source licenses and potentially place the software under the proprietary ownership of the relevant state authority.

9. Auditability of Related Software

All directly associated software featuring interoperability, including, but not limited to, graphical user interfaces, must either be auditable by having their source code available or published under an open-source license. The difference to the former is that it may not need to comply with other requirements under the Open Source Definition, as it is only its auditability that is important.

This assures compliance with the other Principles further as it ensures that any interested party using the software may verify for themselves that the other Principles are being adhered to, as well as that no other violations have occurred in terms of their understanding of the use of the related software.

10. Adequate Compliance

The transfer of data across DLT networks must comply with applicable laws and regulatory provisions in the relevant jurisdictions involved.

Different industries are subject to different forms and intensity of regulatory oversight. The financial industry is certainly one of the most regulated industries. While most of the requirements originate from international regulatory bodies, their implementation by various countries differ both in terms of content and timing.

The international transfer of securities via a distributed ledger or via different distributed ledgers should not expose the originator and the recipient individual or organization to the risk of non-compliance with the regulations prevailing in both jurisdictions.

Combining the borderless nature of distributed ledgers with the geographical nature of laws and regulations is a daunting task when structuring distributed ledgers and the interfaces between them.

As a matter of principle, the interface governing the communication of property rights between distributed ledgers must be designed in such a way as to prevent loss of corollary information (as in blockchain-based payments, KYC information on the originator and the recipient), which is essential in order to ensure the transfer complies with prevailing jurisdictional regulations.

D. Conclusion and Outlook

It can be argued that DLT is a catalyst in the democratization of the financial system and the creation of social value through the digitalization of assets. The recently adopted DLT legislation is a major building block that creates additional momentum in the adaptation of the technology.

An entire ecosystem is evolving. Trust is a key pillar. As this paper outlines, trust and scale can only be achieved if (inter-) operability exists between protocols. Ten principles have been defined which all distributed ledger interfaces should adhere to in order to achieve effective, secure and flawless communication. As the examples demonstrate, alignment within a protocol and across protocols should be guided by a common overarching objective and not by particularism.

Parties should continue to work together in a very open, constructive and respectful manner to ensure all stakeholders can achieve the same level of understanding. Only through open and shared knowledge can practical, pragmatic and robust solutions be developed permitting the application of DLT to flourish, as well as to enhance Switzerland's position in furthering innovation and taking it to the next level.

T3
The Trust Element of Custody

Authors:

Patrick Oltramare, Fedor Poskriakov, Adrien Treccani, Nathan Kaiser, Marcel Hostettler

A. Introduction

1. Context

The trust element of **custody ("T3")** addresses how digital assets can be reliably and easily stored in (self-) custody solutions (e.g., security standards, user experience, auditability) and provides an overview of how custody services are regulated by applicable laws in Switzerland, thus ensuring investor protection and the integrity of the financial markets.

Digital assets can be stored either in self-custody or through intermediaries providing professional custody as a service (together, a "custody solution"). A custody solution for digital assets is fundamentally a system that generates secrets and performs computations using said secrets, while – in principle – preventing their theft and unrecoverable loss. In the context of digital assets, secrets are typically seeds[21] from which addresses and key pairs are derived, while computations typically involve digital signatures, as well as various security checks. In general, a custody solution typically involves a combination of software and, pos-sibly, hardware components.

Irrespective of the type of custody solution, it is crucial for the owners of digital assets to understand how the custody solution protects the secrecy and integrity of cryptographic secrets, such as digital ledger addresses ("DLAs") seeds and derived private keys ("PKs"). There are aspects in the custody of digital assets that contrast sharply with the operational and security aspects related to the safekeeping of traditional financial assets. These distinctive features present a number of challenges, the most notable being how to generate, operate and secure the PKs relating to digital assets throughout the lifecycle of the custody solution.

2. Custody Models

2.1 Self-Custody

In general, a self-custody solution implies that the owner of the digital assets is the only person with access to and knowledge of all secrets and key pairs necessary to control the digital assets, or implementations in which no single party has exclusive control over all secrets (e.g., multisignature or multiparty computation implementations).

This kind of custody solution may be as simple as using an open-source non-custodian wallet, or as complex as operating an infrastructure composed of hardware (e.g., hardware security modules (HSM)) and various software components, whether fully hosted by the owner or totally or partially delegated to a non-custodian infrastructure service provider.

2.2 Third-Party Custody Solution

A self-custody solution is, however, not feasible or adequate in all instances. Indeed, not all owners of digital assets can or want to develop, maintain and/or operate a state-of-the-art self-custody infrastructure for digital assets.

On the one hand, when dealing with clients' assets, institutional financial companies, such as collective investment schemes and pension funds are required by law or regulation to work with a qualified custodian or infrastructure service provider that meets a number of requirements. As a result, self-custody is often not viable for these companies. On the other hand, individual investors may prefer to entrust the custody of their digital assets to a professional service provider, in order to ensure a secure and reliable professional custody solution, as opposed to relying on a self-custody non-custodial wallet for private use. Indeed, third-party custody creates certain advantages for the beneficial owner in terms of functionality, thus providing access to functions that would not otherwise or not as easily be accessible without the intermediary, including easier transaction processing and management, fewer operational and administrative burdens, and above all, an increased level of security.[22]

3. Implications of the Choice of Custody Model

Digital assets may be held in custody in accordance with various models, each of which has its own features, parameters and limitations, but most can be classified as one of the high-level model types set out below, each of which may have a number of sub-types to reflect the specifics of a custody solution:[23]

[21] *Deterministic key derivation ensures that all the wallet keys are derived from a single source of entropy called the seed. As long as the seed is properly secured, all wallet keys and addresses can be recovered if lost.*

[22] *DLT Report, p. 65.*

[23] *See F. Poskriakov, Conservation et négoce de cryptoactifs – aspects choisis du droit des marchés financiers, in CEDIDAC Droit et économie numérique, 1ère éd., 2021, p. 83 et seq., 105 (cited "Poskriakov").*

Model	Description	Allocation	Model
Self-custody (Private DLAs)	Self-custody; PKs controlled exclusively by owner or at least no exclusive control by a single party;[24] no third party custody	Non-custodial wallet and infrastructure solution; no custody services provided by a third party[25]	0
Collective allocation (Pooled DLAs)	Digital assets for multiple beneficial owners pooled in one or several DLAs controlled by the custody service provider	Pool-level allocation – internal ledger allocating all relevant digital assets to clients at custodian level (digital assets in each DLA allocated pro rata among all pool members; no allocation within the DL itself)	1[26]
		DLA-level allocation – internal ledger allocating digital assets held in each DLA to specified clients (multiple clients' ownership of digital assets across multiple DLAs) at custodian level (no allocation within the DL itself)	
Individual allocation (Allocated DLAs)	One or several DLAs for each client (and no more than one client per DLA)	Internal ledger allocating each DLA to a single client (allocation mirrored on the DL)	2[27]
Sub-custody	Digital assets held by the primary custodian with a third-party sub-custodian	Sub-custody pool allocation at custodian level (internal ledger), and various models possible at sub-custodian level, depending on jurisdiction (see Models 1 and 2 above)	3

The choice of a custody model has legal, technical, and accounting implications related to the storage and processing of digital assets being kept in custody. These implications notably depend on:

(A) the legal characterization and types of digital assets involved (e.g., cryptocurrencies, claims, securities, and other financial instruments), as well as

(B) the type of custodian (e.g., regulated as a bank or securities company, or non-regulated custodian).

[24] *This includes governance models with either a multisignature control or an alternative approach, such as "multiparty computation" (MPC).*

[25] *Infrastructure services or non-custodial services may be provided by a third party, which, however, does not have exclusive control of the PKs.*

[26] *See art. 242a para. 2 let. b DCBA and art. 16 para. 1[bis] let. b BA.*

[27] *See art. 242a para. 2 let. a DCBA and art. 16 para. 1[bis] let. a BA.*

B. Technical Context

1. Relationship Between Keys and Addresses

A mandatory, centralized authority responsible for the management of identities, permis-sions, and accounts cannot exist in a permissionless DLT. Consequently, DLTs require a distributed principle to demonstrate digital asset ownership. Asymmetric cryptography, or more specifically digital signatures, provide this capability. They rely on the following primitives:

Private key	A private key, also called secret key, is a randomly generated piece of data from which a digital signature may be computed.	A private key is the ultimate secret with which a transaction may be authorized.
Public key	A public key is an identifier derived from the private key that can be published. The relationship between the private key and the public key means that computing the private key from the public key is not computationally feasible in the current computing and algorithmic environment.	A public key is directly related to a DLA.
Digital signature	A digital signature is a method of computing a proof-of-ownership of a private key while authenticating a message without revealing the private key in the process. There are many digital signature algorithms, for instance: – ECDSA: default on Bitcoin, Ethereum, Ripple – EdDSA: default on Stellar, Cardano, Tezos – BLS: default on Ethereum 2.0	A digital signature demonstrates the ownership of a DLA and can authorize an outbound transaction.
Signature validation	A signature shall be verified with the corresponding public key.	The signature(s) of an outbound transaction are validated by third-parties with the DLA's public key.

A DLA is a public identifier directly related to one, or multiple, underlying public keys. In the simplest case (e.g., an externally-owned Ethereum account, or a P2PKH bitcoin ad-dress), the address is a hash of the public key. Because an address is mathematically derived from a private key, they may be generated at will by the DA owner or custodian.

2. Overview of the Main Accounting Paradigms (**UTXO Versus Accounts**)

There are two main accounting models for DLs:

UTXO model	A UTXO (unspent transaction output) is a value received by a wallet, which has not yet been spent for an outgoing transaction. The balance of a wallet subject to a UTXO model is implicitly defined by the sum of the amounts of all UTXOs received by the wallet. A transaction consumes one, or multiple, UTXOs to transfer value out of a given wallet. The UTXOs may relate to distinct DLAs. A UTXO model intrinsically supports multiple addresses per wallet. Example DLTs: – Bitcoin – Bitcoin Cash – Litecoin	Pros: – simpler to implement, audit and maintain at the protocol level – increases privacy – facilitates collective allocation – supports batched transactions Cons: – different from the banking model, may be complex to use – unsuitable for stateful smart contracts – can lead to heavier transactions, and therefore higher fees
Account model	An account model explicitly maintains the balance by crediting, and/or debiting, the account as transactions come in and/or out. An outgoing transaction defines the transfer amount but does not specifically refer to UTXOs. An account model generally only supports a single address per wallet unless leveraging advanced primitives such as smart contracts. Example DLTs: – Ethereum – Ripple – Tezos	Pros: – intuitive, bank-like model, may be simple to use – stateful by de-fault, allowing advanced smart contract use cases Cons: – more complex to implement, audit and maintain at the protocol level – lower level of privacy

For UTXO-based DL protocols, it is considered good practice to generate new DLAs for each incoming and outgoing transaction, e.g., addresses are never reused within a wallet. The plurality of addresses increases privacy by spreading the actions of a single wallet over multiple, seemingly unrelated addresses.[28]

For account-based DL protocols, a wallet generally corresponds to exactly one DLA. Each incoming and outgoing transaction is explicitly correlated to the account for any external observer.

3. Deterministic Key Derivation

An institutional custody service requires the management of multiple wallets, each possibly leveraging multiple addresses. In the case of an individual allocation, each client has at the least one dedicated address per DL (multiple ones for UTXO-based DLs); in the case of a pooled allocation, clients may share the same on-chain wallet(s) per DL, but the custodian still maintains at the least one wallet per DL.

A proper management of the multiple private keys is paramount to the overall security of the system. It should be possible to generate keys (and their corresponding DLAs) on the fly while i) minimizing access to the keystore for security reasons; ii) ensuring proper back-up of the key material for resiliency reasons.

Deterministic key derivation ensures that all the wallet keys are derived from a single source of entropy called the *seed*. As long as the seed is properly secured, all wallet keys and addresses may be recovered if lost.

BIP32, along with its extensions BIP44 and SLIP10, is the most widely used specification for hierarchical deterministic key derivation. Starting from the seed, a virtually unlimited number of children keys may be recursively derived. An additional piece of data called *chain code* is attached to private and public keys – which are then referred to as extended private and public keys – in order to define the derivation function.

We refer to hardened derivation, and / or non-hardened derivation:

Hardened derivation	Pros: – leakage of an extended private key does not contaminate parent keys Cons: – the generation of new DLAs requires an access to the keystore
Non-hardened derivation	Pros: – the generation of new DLAs does not require an access to the keystore Cons: – leakage of an extended private key exposes all related, non-hardened-derived private keys – leakage of the chain code may expose the relationship between multiple addresses

Because both derivation schemes have their strengths and weaknesses, deterministic deriva-tion is often implemented using a combination of a hardened derivation scheme and a non-hardened derivation scheme. Good practice is to derive wallet keys using hardened deriva-tion (so that the leakage of a client wallet would in no way compromise another wallet), but to use non-hardened derivation for the multiple addresses within a wallet (for DL protocols supporting this capability).

[28] *We would like to point out that because the transaction graph remains visible in general, data mining and clustering techniques may be used to correlate separate addresses with a single owner or wallet. Chain foren-sic tools, such as those provided by companies Elliptic or Chainalysis, rely on these techniques to score ad-dresses on-chain, which has relevance for AML and other crimes.*

4. Key Ceremony, Hardware Security and Air-Gapping

The key ceremony is a critical process during which the initial key material is generated, provisioned and backed up. In particular, it is during this process that a seed is generated.

Because of the risks associated with this process and their possible long-term implications (e.g., an attacker may wait for the assets under management to increase before they launch an attack on the system), it is crucial to prevent the exposure of clear-text keys and to secure single points of compromise.

Hardware security modules, also called HSMs, are specialized hardware offering strong security guarantees regarding i) the key generation process (e.g., the amount of entropy), ii) the confidentiality of the keys (e.g., the fact that they do not leave the HSM unencrypted), iii) and physical protections (e.g., zeroing of the confidential data in case of intrusion detection).

The most common certification for HSMs is the FIPS 140-2[29] issued by the National Institute of Standards and Technology (NIST). This certification defines security levels from 1 to 4. It is commonly agreed that a digital asset custodian should aim for a level 3 or level 4 certification, although more recent, software-only key management schemes (e.g., using multi-party computation) are used in practice and do not qualify for a FIPS 140-2 level 3 or 4. We have summarized the main elements of the certification for levels 3 and 4 below:

HSMs often come with a vendor-specific key ceremony process. In general, this process requires smart cards for authentication and back-up, which are used in such a way as to ensure the absence of centralized trust. For instance, the HSM keys may be sharded into multiple fragments, each stored on separate smart cards, so that it is only possible to reconstruct the HSM key by collecting multiple smart cards; in addition, a certain level of redundancy is recommended in order to mitigate the risk of smart card loss or malfunction.

In the most extreme setups, cold storage (or air-gapped storage) may be implemented. A cold storage is a keystore, which, under no circumstances, is connected to any kind of network. It does not have a network card and is fully isolated, possibly under a Faraday cage, with the result that the only option to request a digital signature is to have some form of a physical access.

Cold storage is considered best practice for long-term custody that does not require frequent outbound transactions.

Level 3	The cryptographic module provides evidence of tampering (e.g., tamper-evident coatings or seals) and attempts to prevent an intruder from accessing critical components of the module. In particular, it may rely on tamper-detection mechanisms to zero out all key material in the event of a breach.
Level 4	As the highest level of certification, the cryptographic module detects and responds to any unauthorized attempts at physical access at a high probability and immediately delete any confidential data.

[29] *We would like to point out that successor FIPS 140-3 to FIPS 140-2 is being tested as of September 22, 2020, and is set to become the new standard in the approval of cryptographic modules.*

5. The Governance Challenge

For most custodial services, keys must be regularly used to sign transactions. For this reason, it is crucial that the process under which the keys may be ordered to sign a transaction is properly secure.

In particular, this process must avoid a single point of compromise. It should, at the very least, enforce the principle of double control, and, in general, a clear governance framework based on risk factors. Examples of risk factors include:

- the transaction amount
- the transaction destination (e.g., is it known to the system, or is it an unknown DLA)
- the number of transactions over a given period
- the velocity of the transactions in a given wallet (e.g., how large is the sum of all transaction amounts over a given period of time)

Based on these criteria, a clear process with escalations should be put in place in order to require that there is an appropriate quorum of approvals based on the assessed risk. Low-risk transactions may be automated, for instance, while higher-risk transactions are manually approved.

6. The Alternative Model of Multiparty Computation

Multiparty computation (MPC) is a field of cryptography that focuses on the joint calculation of mathematical functions over inputs that are broken down across multiple parties. In the context of digital assets, MPC is a tool allowing a key to be sharded into multiple fragments and to compute the digital signature of a transaction without ever collecting the respective fragments. It has the advantage that key shares are distributed and would all need to be attacked in order for the key to be leaked.

MPC is an alternative security model which, rather than relying on specialized hardware modules, favors a decentralization model: individually, the key shards may be easier to attack, but because of their multiplicity, an attacker would need to access multiples of them in order to breach the security of the system. Multiparty computation is an elegant solution for hot wallets, in particular.

C. Legal and Regulatory Context

1. General Outline of Legal and Regulatory implications

The choice of custody model and type of solution (a self-custody vs third-party custody solution) has different legal and regulatory implications depending on the specifics related to the actual implementation of a particular custody solution, as well as the characterization of the digital assets concerned. This section highlights the main implications of some of the most common factual patterns.

2. Contractual Relationships

2.1 Self-Custody (Non-Custodial Wallet and Infrastructure Solutions)

The key aspect of a self-custody solution from a legal and regulatory point of view is the fact that, in principle, the solution provider does not have knowledge of or access to the PKs or any other secrets, which can only be accessed by and known to the end-user (owners of the digital assets).

In a self-custody scenario, the typical contractual relationships would be as follows:

- End-user license agreement (EULA) or similar terms relating to the non-custodial wallet software;
- Non-custodial infrastructure agreements with an *infrastructure service provider* covering various aspects of the delivery of a custody solution, possibly including the design, configuration and related consultancy services (Service Agreement), sale of hardware components (Sale and Purchase agreement), and hosting the hardware infrastructure and/or performing certain software services.

However, in the event that the infrastructure service provider has access to and knowledge of the PKs, but without exclusive

control over such PKs (e.g., backup only, shared PKs or MPC solutions), these services may have regulatory implications for the custody solution provider (see III.C.3 below).

2.2 Third-Party Custody Solutions

By definition, in a third-party custody solution, the custodian typically has exclusive access to and control over PKs relating to DLAs or wallets containing balances in digital assets that belong to clients. From a contractual point of view, the relationship between the custodian and the client will be a custody agreement, which will set out the custodian's duty to safe-guard digital assets for the account of the client, and describe the parameters relating to such custody services, including the custody model (i.e., individual custody or collective custody) and related features.

In turn, the custodian will either operate a proprietary custody solution, or will outsource all or part of the elements to third parties, including:

- software licenses and / or EULA relating to software components used or operated by the custodian (other than any proprietary software of the custodian itself);
- non-custodial infrastructure agreements with an infrastructure service provider (see above); and / or
- sub-custody agreements with one or multiple custodians for a full-service third-party custody solution (custody model 3 – sub-custody).

3. Regulatory Implications

Depending on the classification of digital assets for financial market laws[30] and the specific services provided, various financial markets' regulatory requirements may apply to the custody solution provider, in particular – but not limited to[31]:

- the Anti-Money Laundering Act (AMLA);
- the Banking Act (BA);
- the Financial Institutions Act (FinIA);
- the Financial Market Infrastructure Act (FinMIA); and
- the Financial Services Act (FinSA).

3.1 Self-Custody (Non-Custodial Wallet and Infrastructure Solutions)

In a typical self-custody scenario, the infrastructure service provider only provides consultancy services, as along with hardware and software components as part of the custody solution, without any knowledge of or access to the PKs or any other secrets, which are exclusively accessible by and known to the end-user (owner of the digital assets).

Unlike third party custodial solution providers, the providers of non-custodial wallets or infrastructure can neither view nor access clients' wallets or digital assets, nor are they involved in the transfer of digital assets. It is exclusively the end-users (owners of the digital assets) who can transfer such digital assets without the involvement of the infrastructure service provider. In particular, as non-custodial wallet or infrastructure providers typically do not have any power of disposal (whether in fact or by contract) over their clients' digital assets and cannot confirm, validate, or block any transactions or exercise any other form of control through a *smart contract* or otherwise,[32] service providers such as these do not qualify as financial intermediaries.[33]

As a result, the activities of service providers do not constitute financial intermediary activities in accordance with applicable law and for this reason, are not subject to the AMLA or other financial market laws, solely on the basis of such infrastructure services.

By contrast, in the event that a non-custodial wallet or infrastructure provider has non-exclusive knowledge of or access to the PKs or any other secrets, without having exclusive power of disposal over clients' digital assets,[34] but the ability to trigger or approve (sign) transactions in digital assets belonging to a third party individually or jointly with other actors, or otherwise exercise some other form of control through a smart contract, this service provider generally qualifies as a financial intermediary under the AMLA. In other words, having access to and being able to use all or part of the PKs via a wallet or digital assets,

[30] *See Section 6.2 of the DLT Report.*

[31] *In particular, the applicability and the implications, if any, under the Collective Investment Schemes Act (CISA) are not covered in this Whitepaper.*

[32] *See art. 4 para. 1 let. b AMLO and corresponding commentary, Section 5.7, p. 22.*

[33] *See Section 7.4.1.1 DLT Report.*

[34] *By way of example, this includes backups, copies of seeds or PKs, and/or the service provider having only some, but not all, of the PKs in a multisignature wallet setup, or an MPC solution. See also Section 5.2.2.2 DLT Report.*

individually or jointly, may be compared to having authority to sign for a third party's bank account. This means that if they act on a professional basis and absent any other exemptions, service providers such as these are required to be affiliated with an SRO and comply with the various due diligence requirements in accordance with the AMLA.[35]

3.2 Third-Party Custody Solutions

a) Introduction

By definition, providers of third-party custody solutions hold clients' private keys in safe-keeping and enable clients to send and receive digital assets. In contrast to self-custody models, third-party custody models imply an exclusive actual power of disposal over clients' digital assets. Schematically, such solutions can either provide for individual custody and allocation (see Model 2) or collective custody and allocation (see Model 1). A sub-custody model (see Model 3) merely adds a layer of regular intermediated custody on top of either a Model 1 or 2 digital asset custody solution implemented at the sub-custodian level.

From a regulatory point of view, under Swiss financial market laws, providers of third-party custody solutions are subject to a number of general requirements, depending on the type of digital assets involved, as well as specific requirements depending on the custody model (i.e., Model 1 or Model 2). The following merely addresses specific aspects of custody services, any additional services (e.g., trading, management, advice, clearing and settlement, trading infrastructures, etc.) should be assessed separately.

b) Swiss Regulatory Considerations – General Aspects

– AMLA

Insofar as the custodian in a third-party custody solution will have exclusive control over PKs with regard to the digital assets of third parties, this custodian will always be subject to the AMLA at least and will be required to register with an SRO and comply with AMLA due diligence requirements. Depending on the circumstances, additional regulatory requirements may be triggered under other financial market laws.

– Banking Act

The professional acceptance of deposits from the public is subject to the Federal Law on Banks and Savings Banks (Banking Act - BA) and requires either a banking license or a fintech license,[36] and is subject to prudential supervision. These requirements typically apply to pure payment tokens only, as opposed to utility or asset tokens.

In the event that the custody of payment tokens constitutes a deposit under the BA – typically, if the custodian's obligation constitutes pure contractual debt, the underlying assets can be used by the custodian and/or these assets are not segregated in the event of custodian bankruptcy for any reason (see III.C.4 below), and no other exemption applies[37] – the licensing requirements under the BA will be triggered if professional activity thresholds are exceeded.[38]

A fintech license permits the acceptance of deposits of up to CHF 100 million on a professional basis and of payment tokens held in collective custody. This includes traditional deposits and the safekeeping[39] of cryptocurrencies (e.g., Bitcoin, Ether) or other payment tokens as a deposit or in collective custody. Companies with a fintech license are also authorized to hold digital assets classified as securities in custody for clients without any additional license as a securities firm, provided that they only provide pure custody services (see below for a discussion on licensing requirements under the Financial Institutions Act).

Conversely, the safekeeping of payment tokens is generally not considered to be a deposit business subject to authorization if the balance transferred solely for secure safekeeping, is held (directly) within the DLT (individual allocation) and can

[35] *See also Sections 2.4 and 7.4.11 DLT Report.*

[36] *Authorization pursuant to art. 1b Banking Act.*

[37] *Art. 5 para. 3 let. c Banking Ordinance.*

[38] *Art. 6 Banking Ordinance.*

[39] *By contrast, a trading account in cryptocurrencies is likely to fall under the Banking Act and require a bank-ing license, unless it can be demonstrated that the trading activity is not comparable to that of a currency dealer (see FINMA Circular 2008/3, Section 16.2).*

be attributed to and at the disposal of the individual client at any time,[40] which also means that such payment tokens are segregated in the event of service provider bankruptcy.[41] However, segregation in the event of bankruptcy no longer automatically means that licensing is not required. Indeed, collective custody of certain digital assets (as at today's date, of payment tokens only)[42] in itself already requires a fintech license at the very least, provided that such activity is conducted on a professional basis.

– Financial Institutions Act (FinIA)

In relation to the safekeeping of digital assets (custody), the main relevant licensing category under the FinIA is that of a securities firm. Anyone who trades on a commercial basis[43] in their own name for the account of clients with digital assets classified as securities (in principle, most asset tokens, as well as hybrid tokens featuring asset token characteristics) needs to obtain an authorization as a securities firm.[44]

By contrast, activities involving pure custody (safekeeping) of digital assets which are characterized as securities or derivatives, the delivery thereof from the custodian to the client and / or the transfer by the custodian to a third party on behalf of the client (e.g., delivery-versus-payment transactions) would not in and of themselves constitute trading in securities and, hence, this company would not require a securities firm license under the FinIA. However, if the custodian is involved in the execution of transactions in securities in a causal manner (e.g., executing an order to buy or sell digital assets on an exchange), activities such as these exceed pure safekeeping and could trigger the requirement for authorization as a securities firm.

– Financial Market Infrastructure Act (FinMIA)

The FinMIA governs the organization and operation of financial market infrastructures and the rules of conduct for financial market participants in securities and derivatives trading. In this respect, it will only be potentially relevant for digital assets that can be characterized as securities or derivatives (to the exclusion of pure payment tokens, cryptocurrencies and utility tokens).

FinMIA regulates stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, payment systems and trade repositories as financial market infrastructures.[45]

From the point of view of custody as part of the digital asset value chain, the principal infrastructure license which may be relevant is that of a central custodian, which requires a central securities depository (CSD) license.[46] A central custodian is an entity for the centralized custody of securities and other financial instruments based on standard rules and procedures.

The introduction of a CSD to a generally decentralized concept like DLT is counter-intuitive. However, it may be desirable, e.g., for the purpose of safeguarding settlement or system stability, to use a CSD in certain implementations of integrated trading and settlement platforms. In this situation, the requirement for authorization as a CSD would present a high barrier to market entry.[47]

This potential issue has been addressed with the inclusion of a new DLT-based trading facility in the FinMIA, which allows for integrated trading and settlement infrastructures, so that the same infrastructure may perform custody and post-trade settlement services for token-based securities.

– Financial Services Act (FinSA)

The FinSA applies only to digital assets that are characterized as financial instruments. Typically, payment tokens and utility tokens would not fall within this definition. Only asset tokens and hybrid tokens with an asset token component could possibly qualify as financial instruments.

In a scenario where the digital assets under custody are indeed

[40] *See Section 6.3.2.1 DLT Report; art. 242a para. 2 let. a DCBA and art. 16 para. 1bis let. a BA.*
[41] *See art. 242a para. 2 let. a DCBA and art. 16 para. 1bis let. a and 37d BA.*
[42] *Art. 5a BO.*
[43] *Art. 65 Financial Institutions Ordinance (FinIO).*
[44] *Art. 41 FinIA.*
[45] *Art. 2 para. 1 FinMIA.*
[46] *Art. 61 FinMIA.*
[47] *See Section 6.4.6 c) DLT Report.*

financial instruments, the FinSA would not apply to providers of custody services, provided that their service is restricted exclusively to custody,[48] insofar as such services do not constitute financial services under the FinSA.

c) Individual Custody

Under current laws, the safekeeping of payment tokens is generally not considered to be a deposit business subject to authorization if the balance transferred solely for secure safe-keeping[49] is held (directly) within the DLT (individual allocation) and can be attributed to the individual client at any time,[50] which also means that such payment tokens are segregated in the event of service provider bankruptcy.[51] In other words, a Model 2 custody solution with individual allocation of digital assets does not require authorization by FINMA, provided the above-mentioned requirements are complied with.

No further specific requirements apply to individual custody models based on Model 2-type custody solutions in addition to the generally application requirements referred to in III.C.3.2b) above.

d) Collective Custody

Since the entry in force of the DLT Act on August 1, 2021 the collective safekeeping of payment tokens (cryptocurrencies) qualifies for segregation treatment in the event of bankruptcy both for banks and non-banks, provided that (i) the digital assets are held at the client's disposal at all times; and (ii) the individual allocation to a particular client is clearly established (e.g., custodian's internal ledger).[52]

However, the mere custody of certain types of digital assets, namely payment tokens kept in collective custody, will nonetheless and irrespective of their off-balance sheet treatment require at least a fintech license[53] and the amounts of payment tokens kept in collective custody for clients by banks may be limited in quantitative terms by FINMA.[54]

e) Intermediated Securities

Personal or corporate rights of a fungible nature vis-à-vis an issuer credited to a securities account held with a bank or another financial institution (qualified custodian)[55] could qualify as intermediated securities (*"titres intermédiés"/"Bucheffekten"*) in accordance with articles 2 and 3 Swiss Intermediated Securities Act ("ISA").

Before the entry in force of the first part of the DLT legislation on February 1, 2021, only whole issuances of uncertificated securities registered in the main register by a qualified custodian were eligible to become intermediated securities under the ISA.[56]

Now, thanks to the DLT Act, all or part of an issuance of ledgerbased securities[57] are also eligible to become intermediated securities, simply when they are credited to a securities account and immobilized by a qualified custodian.[58]

By default, irrespective of the manner in which the qualified custodian holds the ledger-based securities for its clients (it is likely that a collective custody model will be applied by default, similar to traditional intermediated securities), it will be assumed that these ledger-based securities belong to the custodian's clients, and will be segregated from the custodian's assets.[59]

Only those ledger-based securities which are directly held by the qualified custodian within the relevant DLT and credited by the custodian to its clients' securities accounts become intermediated securities. This does not affect the remainder of the issue of such ledger-based securities which can continue to be held and traded in a disintermediated environment. This flexible treatment allows market participants to benefit both from existing intermediated distribution and custody channels, which are favored by some investors, and to leverage and have access to new issuance possibilities and direct offerings to investors in a disintermediated manner, while maintaining the ability to seamlessly switch from one form to another.

[48] *See Section 6.6.3 DLT Report.*

[49] *By contrast, a trading account in cryptocurrencies is likely to fall under the Banking Act and require a bank-ing license, unless it can be demonstrated that the trading activity is not comparable to that of a foreign ex-change trader (see FINMA Circular 2008/3, Section 16.2).*

[50] *See Section 6.3.2.1 DLT Report; art. 242a para. 2 let. a DCBA and art. 16 para. 1bis let. a.*

[51] *Art. 242a para. 2 let. a DCBA and art. 16 para. 1bis let. a and 37d BA.*

[52] *Art. 242a para. 2 let. b DCBA and art. 16 para. 1bis let. b and 37d BA.*

[53] *Art. 1b para. 1 BA; art. 5a BO.*

[54] *Art. 4sexies BA.*

[55] *See definition in art. 4 ISA.*

[56] *Art. 6 para. 1 let. c and para. 2 ISA.*

[57] *Meaning rights issued as such pursuant to art. 973d CO (art. 5 let. h ISA).*

[58] *Art. 6 para. 1 let. d and para. 3 ISA.*

[59] *Art. 17 ISA.*

4. Investor Protection and Treatment in the Event of Bankruptcy

4.1 Self-Custody (Non-Custodial Wallet and Infrastructure Solutions)

By definition, in a self-custody model, the custody infrastructure solution provider does not control or have access to PKs on an exclusive basis. Without exclusive control by the infrastructure provider, the respective digital assets, irrespective of their characterization, will not fall within the provider's bankrupt estate.[60] Consequently, the bankruptcy of a non-custodial wallet and infrastructure provider has no legal bearing on the client assets held via this kind of wallet or infrastructure.

The same applies to any situation where the custody solution provider only has access to and control over one of many security elements (e.g., in a multisignature or MPC solution implementation).

4.2 Third-Party Custody Solutions

a) Individual Custody

As indicated above, the individual safekeeping of payment tokens is generally considered to be off-balance sheet and segregated in the event of bankruptcy if: (i) the balance is transferred solely for secure safekeeping; (ii) held (directly) on the DLT (individual allocation); and (iii) can be attributed to and is at the disposal of the individual client at any time.[61]

Failure to comply with these requirements means that the balance of payment tokens (cryptocurrencies) held with the custodian will be a purely contractual claim against the bankrupt custodian, and treated as an ordinary claim in the event of their bankruptcy. However, the situation is potentially different for payment tokens that represent a claim or right against a third party (counterparty payment tokens).

With regard to counterparty payment tokens, utility and asset (investment) tokens, the situation depends on the legal characterization of the individual tokens. If the general provisions of art. 401 CO or, in respect of the banking sector, art. 16 and 37d BA, are met, these tokens will be segregated in the event of bankruptcy in accordance with the procedures applicable under the DCBA or the BA.

b) Collective Custody

Since the entry in force on August 1, 2021 of the DLT legislation, cryptocurrencies and other payment tokens are also segregated in the event of custodian bankruptcy as well as in the event of collective custody (pooling) of digital assets, both in the banking and non-banking sectors, provided that: (i) the digital assets are held at the client's disposal at all times; and (ii) individual allocation to a particular client is clearly established (e.g., custodian's internal ledger).[62]

Counterparty payment tokens (i.e., claims against third parties), as well as utility and asset (investment) tokens, would typically fall under the definition of "custody assets" already in accordance with the previous version of art. 16 BA, respectively the general provisions of art. 401 CO, and therefore have been and continue to be eligible for segregation in the event of bankruptcy in accordance with the procedures applicable under the DCBA or the BA.

c) Intermediated Securities

As mentioned above, irrespective of the manner in which a qualified custodian holds ledger-based securities for its clients (most likely in a collective custody), it will be assumed by default that ledger-based securities belong to the custodian's clients, and will be segregated from the custodian's assets.[63] In principle, from a legal point of view, the fact that intermediated securities were created from ledger-based securities does not affect their

[60] *ATF 110 III 87, 90; see Section 4.1.2.1 DLT Act Dispatch.*

[61] *See Section 6.3.2.1 DLT Report; art. 242a para. 2 let. a DCBA and art. 16 para. 1bis let. a.*

[62] *Art. 242a DCBA and art. 16 para. 1bis BA.*

[63] *Art. 17 ISA.*

legal treatment in the event of custodian bankruptcy; in other words, the type of underlying used to create intermediated securities is irrelevant.

The critical point, however, to be considered and addressed when intermediating ledger-based securities, in particular at governance and technical levels, is the ability of the qualified custodian or bankruptcy estate administrator to actually bring about the segregation and to effectively transfer the respective portion of the ledger-based securities to the account holders as required under ISA.[64]

5. Financial Market Infrastructures

5.1 Overview

The FinMIA governs the organization and operation of financial market infrastructures, and the conduct of financial market participants in securities and derivatives trading. As mentioned in section III.C.3.2b), the main financial market infrastructure which is specifically relevant for the custody of ledger-based securities is the central securities depository (CSD). However, other than when trading through an exchange or multi-lateral trading facility (MTF) a CSD would not be absolutely necessary for the trading and settlement of ledger-based securities transactions.[65]

Beyond mere custody, financial market infrastructures are crucial for the smooth operation of financial and capital markets. These infrastructures drive the standardization, automation and acceleration of the various steps required in the securities value chain in order to process securities transactions (trade, clearing and settlement). In doing so, market infrastructures make a key contribution to the efficiency and stability of the financial system as a whole, something which goes hand in hand with a level of regulation and requirements in terms of the conduct of market participants.

Today's financial market infrastructures are based on the principles of centralized infrastructures, intermediated market access via regulated securities firms or similarly organized regulated entities and the segregation of various infrastructures (i.e., one entity may only operate a single market infrastructure).[66] This approach faces various hurdles when dealing with ledger-based securities and tokens in general, due to the tension between the current centralized paradigm and the decentralized nature of DLT, in particular: (1) access to and participation in the infrastructure by non-regulated participants (including individual investors), and (2) the simultaneous nature of trading and settlement within a DLT infrastructure.

In this context, among the three forms of trading facilities that currently exist, namely, the two regulated trading venues, stock exchanges and multilateral trading facilities (MTFs), and the indirectly regulated organized trading facilities (OTFs),[67] only some implementations of OTFs are suitable for the trading and settlement of ledger-based securities (unless converted to intermediated securities)[68] and can be accessed directly by non-regulated persons. Indeed, regulated trading venues are limited to securities trading only, to the exclusion of any post-trade services, and, for this reason, are not permitted to hold either securities accounts or to be involved in the actual settlement;[69] in terms of admitting participants, they are limited to regulated companies only. However, OTFs also present drawbacks, in the sense that in the absence of a bank or securities firm network of interconnected OTFs, the facility's depth of liquidity will be limited, and the trading of ledger-based securities will be restricted to the application of discretionary trading rules, leading to unwanted uncertainties.

Given the practical significance of a functioning financial market infrastructure for the economy and in addressing the abovementioned limitations, a new form of trading venue has been proposed, the so-called DLT-based trading facility. The relevant legal and regulatory framework governing the same entered in force on August 1, 2021.

5.2 DLT-Based Trading Facility

The new DLT-based trading facility (DLT-MTF) is based on the

[64] *Art. 17 para. 4 let. c ISA.*

[65] *See also Iffland / Ben Hattar, Central Securities Depositaries in the Age of Tokenized Securities, in Caplaw-2020-05.*

[66] *Art. 10 FinMIA, with the only exception that securities exchanges can also operate MTFs.*

[67] *OTFs are not regulated as such, but may only be operated by a company authorized as a bank, securities firm or trading venue.*

[68] *Indeed, any ledger-based securities converted into intermediated securities can be admitted for trading at any stock exchange or MTF, with settlement through a CSD.*

[69] *For a more detailed overview see Section 6.4.4 DLT Report and Poskriakov, op. cit., III. D. 2.*

concept of an MTF, which allows for the multilateral trading of securities based on non-discretionary rules, but distinguishes itself from an MTF by means of the following requirements:

- the DLT-MTF is authorized to admit only DLT-based securities for trading. These are defined as including all ledger-based securities within the meaning of art. 973d CO, as well as all other DLT-based assets, which should typically include all forms of tokens, including utility and payment tokens, based on certain conditions[70] (it is understood that a DLT-MTF will also, in theory, be entitled to operate an OTF for the discretionary trading of any (traditional) securities and non-discretionary trading of financial instruments, but would not be permitted to offer custody or settlement services for transactions in securities);[71] and
- the DLT-MTF needs to either admit non-regulated participants, or provide post-trade settlement or central custody services.[72]

This new regulated trading venue designed specifically for DLT-based securities and other assets should facilitate the emergence and development of new business models, but may need to be further adjusted to take requirements in practice into account once actual trading venues begin operation. The range of product offering could be significantly expanded – new asset classes will be created and investors will also gain access to non-bankable and otherwise illiquid assets on a fungible and tradeable basis. A DLT-MTF provides for the opportunity to expand the potential range of clients to the corporate and even retail sector. In particular, small- and medium-sized companies could use this new access to the capital markets in order to issue refinancing products.

However, the new DLT-MTF as proposed is not an exclusive regime for trading DLT-based securities, but simply adds flexibility, by introducing an additional type of regulated trading venue intended for business models tailored toward DLT. There is no need for conversion into intermediated securities like in the traditional setup. This may prove to facilitate the operational side.

However, securities exchanges, MTFs and OTFs can also list or admit DLT-based securities for trading, within the limitations of the requirements and restrictions specific to each of those trading facilities. In cases where the issuer wishes to issue a hybrid (parts of the securities designed as traditional securities, parts as DLT-Securities), MTFs and OTFs would be in a position to offer both types of securities.

Finally, a DLT-MTF may help to address issues regarding public deposits arising from cryptocurrency brokerage and provide an additional set of benefits for the following reasons: a DLT-MTF constitutes a natural basis for the function of an (authorized) payment system which also permits the management of accounts for participants. Most likely there are fewer issues with regard to deposits / custody, whereas the traditional exchange / CSD setup and respective licenses do not entail any payment system functionalities and for this reason, do not provide for ancillary account operations.

D. Conclusion and Outlook

The current legal and regulatory framework in Switzerland provides legal certainty and protection for investors with regard to the storage and custody of their DLT-based assets, regardless of whether they have sufficient technological skills to use a self-custody solution, or rely on a professional custody solution provider. Beyond mere custody, the legal and regulatory framework in Switzerland adequately addresses all of the requisite key aspects of the entire value chain starting from issuance, through custody to trading and the secure settlement of transactions and for this reason, consolidates the basis for a trusted custody (T3).

The next challenge could be represented by the emergence of fully distributed (peer-to-peer) trading platforms for DLT-based securities, provided that these emerging solutions successfully resolve the issues related to the basic elements of trust, including in the admission of DLT-based instruments for trading, order-matching rules, pretrade and post-trade transparency, as well as controls and rules governing the conduct of market participants.

[70] *Art. 2 para. bbis FinMIA.*

[71] *Certain limitations will apply, including a prohibition on trading in certain assets designated by FINMA (such as privacy coins) and permission to only admit derivatives without any temporal component or leverage (art. 58f FinMIO).*

[72] *Art. 73a FinMIA.*

IV. T4

The Trust Element of Transaction

Authors:

Harald Baertschi, Patrick Salm, Gino Wirthensohn

Contributors:

Rolf Guenter, Bruno Pasquier, Gian Pfister, Orkan Sahin, Michael Svoboda

A. Introduction

One of the main challenges in using an ecosystem based on DLT is how to achieve coherence between technical and legal considerations. The technical transfer of tokens needs to be legally recognized, unless there are specific circumstances justifying an intervention by the legal system in order to overrule the technical predominance of the DLT system.

In this Whitepaper, we discuss the transfer of tokens both from a technical and legal perspective. The legal analysis considers the recent amendments to Swiss law in the field of distributed electronic ledgers, which entered into force at the beginning of February 2021 and beginning of August 2021, respectively. Subsequently, we present a number of general use cases and conclude with a brief outlook.

B. Technical Context

1. General Technical Description

The focus of this section is on the technical aspects relating to the transfer of tokens on open, public blockchains. Many blockchains are in existence today, of which the most well-known are Bitcoin and Ethereum. Bitcoin has a very limited scripting language that makes it less suitable for executing complex logic or programs. By contrast, Ethereum is a computing infrastructure that enables developers to build decentralized applications ("DApp") with builtin economic functions. These applications are called smart contracts. A token is a standardized smart contract called by a transaction. All smart contracts in Ethereum are ultimately executed because a transaction is initiated from an address.

A transaction for ledger-based securities raises two main questions:

(i) Ownership governance: who owns the rights to the security?
(ii) Asset feature: how are rights represented and in the case of financial instruments, how are potential cash flows distributed?

While these questions are not related per se to the technological elements of a transaction, this section provides an overview of technical standards and practical implementations related to the transfer of ledger-based securities on the Ethereum blockchain. To avoid doubt and unless otherwise stated, in this section, the term "owner(ship)" does not necessarily refer to legal ownership, but to the technical authority to interact with a token smart contract (some-times called "administrative privileges").

Section 2 describes tokens and the interaction with smart contracts, the transfer of ledger-based securities and finality with focus on the issuance side. Section 3 then describes the asset itself in more detail.

2. Elements of a Transaction

2.1 Tokens and Smart Contract Governance

The recent amendments to the Swiss Code of Obligations define certain requirements to the register that are relevant for ledger-based securities. A key requirement is that the register provides the creditor (token holder or owner of the right), but not the debtor (token issuer), with the technical means to transfer and dispose of the tokens. This means that the full power of disposal (*"Verfügungsmacht"*) remains with the token holder. Until recently, most security token standards, which are described in more detail below, provided the issuer with extensive intervention rights and / or allowed the issuing party to change the functionality of the token at a later point in time.

2.1.1 Token

A token is a representation of something in the blockchain. This can be money (*payment token or stable coin*), access to a platform (*utility token*), a piece of art (*asset-backed token*) or shares in a company (*security token or asset token*). A token that represents something is nothing more than a smart contract, which allows other smart contracts to interact with it, exchange it, create, or destroy it. In fact, everything in Ethereum is either a smart contract or an address (sometimes called "externally owned

account"). For tokens qualifying as ledger-based securities, this means that it is possible that the token "holder" is not a person and the register does not indicate actual persons, but addresses. Although one or more persons can be behind them, it is not necessarily required. Addresses can equally be linked to other registers or any other smart contracts, so that a potentially extensive chain of addresses is created until an address controlled by one or more persons is reached.

Although the concept of a token is simple, it has a variety of complexities in its implementation. The Ethereum community has developed various standards, called improvement proposals or "EIPs".[73] If the proposed standard is related to the application level, they are called "ERCs".[74] In essence, the goal of these standards is to establish how a contract can interoperate resp. interact with other contracts.[75]

(i) **ERC20:** the most widespread token standard for *fungible assets.* It is the "lowest common denominator" of all standards albeit somewhat limited by its simplicity.

(iii) **ERC721:** the de-facto solution for *non-fungible tokens* (NFTs), often used for collectibles.

(iv) **ERC1155:** a relatively new standard for multi-tokens, allowing a single contract to represent multiple fungible and non-fungible tokens, along with batched operations for increased gas efficiency.

(v) **ERC14xx** family (referred to as "security token" standards such as ERC1404[76], ERC1450[77], or ERC1462),[78] these are advanced token smart contracts that have specific access and intervention rights attached (see following section for more details).

2.1.2 Access Control

a) Overview

Access control to a smart contract is the mission-critical governance layer that defines "who is allowed to do what" (sometimes called "administrative privileges"). In its simplest form, there is one owner of a token contract and that is the account that deployed the smart contract. It has the sole power of disposal over and full access to the deployed token.

Unfortunately, in the real world, things are not as simple as that and different levels of authorization are often required. This could be driven by regulatory / compliance requirements or industry practice. "Role-based access control" offers flexibility in this regard. For those interested, OpenZeppelin provides in-depth information on the potential access functions of a contract.[79]

In the following section, we focus on administrative functions that could be relevant for the transfer of tokens. These privileges, referred to as "capabilities", must be well-specified and fully disclosed in the legal documentation (e.g., token terms, registration agreement, etc.). It could be an intrusion to the decentralized nature of digital assets. Therefore, these functions shall only be invoked in clearly defined circumstances and in the public's legitimate interest to prevent fraud, collusion, coercion, obstruction, criminal or illegal activities or other actions that result in a violation of applicable law or harm to protected rights or property.

We group the capabilities into three categories to make a logical distinction in order to assign them to a certain group of individuals in a company (for more information, see section on segregation of capabilities). As the name implies, supply driven capabilities may be associated with the finance or operations department, compliance driven capabilities with the legal and compliance department, and technical capabilities with the IT department.

b) Supply Driven Capabilities

i) Mintable

The minter role can mint tokens to other accounts. Minting tokens increases the total supply of tokens and the balance of the account that the tokens are minted to. In the context of ledger-based securities, this can be the primary issuance

[73] *EIPs: https://eips.ethereum.org*

[74] *ERCs: https://eips.ethereum.org/erc*

[75] *For more information on smart contracts, see https://ethereum.org/en/developers/docs/smart-contracts*

[76] *Simple restricted token standard https://erc1404.org*

[77] *EIP-1462: A compatible security token for issuing and trading SEC-compliant securities https://eips.ethereum.org/EIPS/eip-1450*

[78] *EIP-1462: Base Security Token https://eips.ethereum.org/EIPS/eip-1462*

[79] *OpenZeppelin – Access: https://docs.openzeppelin.com/contracts/3.x/api/access*

of equity (e.g., incorporation of a new entity) or a capital increase of an existing company. Furthermore, it can be a conversion from simple uncertificated securities (*"einfache Wertrechte"*, art. 973c CO) into ledger-based securities (*"Registerwertrechte"*, art. 973d CO). Clear governance rules must be applied for this role (see segregation of capabilities below).

ii) Burnable

Burner roles can either destroy tokens from other accounts or send tokens to an address for which nobody possesses the PIK. Burning tokens decreases the total supply of tokens and the balance of the account the tokens are burned from. This could contravene the new law in several ways (for a discussion on the discrepancies between ledgers and the legal situation, see Section IV.C.1.3e) below).

c) Compliance Driven Capabilities

i) Whitelistable

There are two common whitelisting approaches. The first is a simple (binary) form of white-listing an address (yes / no); while the second is an array of different whitelists (e.g., for different categories such as investor type, jurisdictions, etc.). In this case, the whitelister roles can configure whitelist rules and add / remove accounts from whitelists. For example, the ERC1404 simple restricted token[80] allows for a total of 255 whitelists, each with the ability to restrict transfers to all other whitelists. When a transfer is initiated, the restriction logic will first determine the whitelist that both the source and destination belong to. Then it will determine if the source whitelist is configured to allow transactions to the destination whitelist. If either address is on whitelist 0, the transfer will be restricted. The transfer will also be restricted if the source whitelist is not configured for sending to the destination whitelist. Administrators can modify a whitelist beyond the default configuration in order to add or remove outbound whitelists.

ii) Blacklistable

Blacklister roles can add or remove accounts from blacklists. Blacklisting means an address will no longer be able to receive or send tokens (this is sometimes called a "freeze"). Payment tokens such as USDC often have this functionality enabled.

iii) Revocable

Revoker roles can revoke tokens from any account. Revoking tokens has no effect on the total supply, it increases the balance of the account revoking the tokens and decreases the balance of the account the tokens are revoked from. The revoke function can be used (amongst other solutions) to recover lost tokens (for details, see Section 2.1.5 below).

d) Technical Capabilities

i) Pausable

This is the ability to implement an emergency stop mechanism that can be triggered by the pauser role to halt or resume the contract (this is why the function is sometimes called a "circuit breaker"). When the contract is paused, *all* transfers will be blocked.

Pausing a contract may contravene the provisions of the new law as the token holder can no longer transfer the tokens freely, and for economic reasons, it is difficult to justify initiating a pause. However, there are reasons for pausing a contract as halting all transactions can be beneficial for token holders. This is discussed further in Section 2.1.4 below (upgrade token contract).

ii) Proxiable

If the contract is upgradeable and uses the Universal Upgradeable Proxy Standard (UUPS[81]), the administrative role allows updating the contract logic while maintaining the contract status. Often, this role is assigned to the owner of the smart contract (see Section 2.1.4 below).

[80] *See Github repository https://github.com/tokensoft/tokensoft_token#whitelists*

[81] *EIP-1822: Universal Upgradeable Proxy Standard (UUPS): https://eips.ethereum.org/EIPS/eip-1822*

iii) Ownable

Owner accounts can add and remove other account addresses to all roles, including themselves. This means that any owner can remove restrictions, thus turning the contract into a regular ERC20, upgrade the contract logic or switch blacklists and whitelists on / off. Owners are superadmins that have the authority to reverse any inappropriate action taken by any other admin role listed above. Furthermore, owner accounts can transfer tokens to any valid address, regardless of whether they are whitelisted or even blacklisted.

2.1.3 Segregation of Capabilities

i) Operational Governance

The segregation of duties is a wellknown concept in risk management with the goal of reducing the risk of fraud and minimizing organizational weaknesses. In terms of smart contract governance, there are various possible strategies for segregation.

For example, an issuer could segregate all roles (minter, burner, pauser, revoker, etc.), meaning that for every administrative function, only one designated signer (person) can perform the task. While this is technically possible, it is inefficient and can cause increased operational overhead (e.g., in case the person is absent, a deputy must be appointed to ensure business continuity, etc.).

Another example: if a rogue employee of an equityissuing company has been assigned minting and burning roles, they could issue or destroy as many tokens as possible but cannot do anything else with them. If this rogue employee also had been assigned whitelisting roles (assuming the tokens have a transfer restriction), they could whitelist their account, mint token to this account and sell them immediately, causing financial and reputational damage to the issuer.

The above examples demonstrate the trade-off between usability and operational governance. A solution could be to segregate the duties along the lifecycle of a token. Our suggestion is to at least separate the grouped capabilities (supply, compliance, technical) in order to achieve acceptable usability with the best security possible.

ii) Ownership Governance

Another key aspect is ownership governance. As an owner has super-admin powers, it is of the upmost importance to segregate this capability from other administrative roles. It goes without saying that segregation alone is not sufficient and that additional protective measures must be put in place.

One of the most common protection measures is assigning multiple addresses to the ownership of the token smart contract. In Ethereum, multiple signatures refer to a smart contract (referred to as a "multisig contract") that defines the required number of signers from a list of addresses authorized to sign a transaction (e.g., a 3-of-5 multisig means that five addresses can sign, but only three are required to do so to generate a valid transaction). Several multisig "standards" exist (depreciated multisig standards such as Mist or Parity are not listed below):

- Gnosis Ethereum Multisignature Wallet[82] – the industry standard
- BitGo Ethereum MultiSig Wallet Contract[83] – widely used, but limited to a 2-of-3 signature scheme
- Simple MultiSig[84] using the EIP712 format[85]– a simple and gas-saving multisig contract

iii) Key Generation Governance

The segregation of capabilities is equally important in a key generation event (sometimes called "secret generation" or "key ceremony"). The CMTA provides a platform for creating open industry standards such as the Digital Asset Custody Standard (DACS)[86] for issuing, distributing, and trading ledger-based securities. DACS consists of requirements and recommendations for the generation of cryptographic secrets for technology solutions enabling the custody and management of ledger-based securities.

[82] *Gnosis Ethereum Multisignature Wallet: https://github.com/Gnosis/MultiSigWallet*

[83] *BitGo Ethereum MultiSig Wallet Contract: https://github.com/BitGo/eth-multisig-v2*

[84] *Simple Multisig: https://github.com/christianlundkvist/simple-multisig*

[85] *EIP-712: Ethereum typed structured data hashing and signing: https://eips.ethereum.org/EIPS/eip-712*

[86] *CMTA Digital Asset Custody Standard – Secrets Generation (Section 3.3), https://www.cmta.ch/content/389/cmta-digital-assets-custody-standard-v-12-final-october-2020.pdf*

2.1.4 Upgrade Token Contract

A token contract is not only capable of interacting with other smart contracts, it can also be upgraded. While this could be essential for an issuer to ensure future regulatory compliance, major trust compromise required: the immutability of the contract. A strong governance strategy is required as part of an upgradeable strategy, such as the segregation of capabilities. Adherence to best practice and applying the latest standards are essential. The following standards allow for upgradeable contracts in a transparent and therefore usable way:

- EIP-1822: Universal Upgradeable Proxy Standard (UUPS)[87]
- EIP-1967: Standard Proxy Storage Slots[88]

While these standards have been widely adopted by the community with no reported security issues thus far, they still have some drawbacks, such as storage limitations and forward compatibility. The latter especially is a real threat because the network is due to undergo some critical upgrades in the near future (e.g., EWASM / Ethereum 2.0)[89] that will prevent proxy contracts from working. Currently deployed upgradeable contracts will not be able to call the proxy contract once these changes have been implemented.

For the above reasons, it is still advisable to make a token contract "pauseable" so that it can be upgraded safely should unexpected issues occur during the network upgrade.

2.1.5 Lost Keys

The handling of lost tokens (private keys) reflecting ledger-based securities is governed by art. 973h CO (cancellation, *"annulation", "Kraftloserklärung";* see Section C.1.3 e) ii) below). The traditional way of dealing with lost securities (e.g., paper-based shares and physical certificates) is to call the competent court and to have the shares or certificates declared invalid so that the company can issue replacements. While a situation could be envisaged whereby a judge declares the token invalid (which can then be flagged as "lost"), there are better solutions that make use of the programmability of blockchain technology. The law expressly allows these kinds of alternative cancellation procedures. From a technical point of view, there are two common approaches to recovering lost tokens.

The first approach is a "centralized mechanism" through the freeze and revoke capability outlined earlier in this document. Again, clear governance must be implemented in order to avoid any misuse of the functions. The Swiss Blockchain Federation provides useful recommendations for administrative privileges in its Tokenized Equity Circular.[90]

The second approach uses smart contracts in a more decentralized manner. The token contract can have a function to permit anyone to declare tokens as lost and claim them at the risk of losing a collateral in case the claim turns out to be false. For those interested in understanding how this kind of a recovery mechanism works in practice, there is a good explanation in the code repository of Aktionariat[91], including a smart contract example called "ERC20Recoverable"[92] that is akin to other Swiss start-ups issuing tokenized equity, such as Alethena[93] or ServiceHunter.[94]

2.2 Transfer of Tokens

Distributed ledger technologies like blockchains are decentralized networks of computers (so-called "nodes") maintaining a publicly verifiable and immutable record of (historical) transactions. The network needs a trust element in order to function.

[87] *EIP-1822: Universal Upgradeable Proxy Standard (UUPS) https://eips.ethereum.org/EIPS/eip-1822*

[88] *EIP-1967: Standard Proxy Storage Slots: https://eips.ethereum.org/EIPS/eip-1967*

[89] *Ethereum 2.0: A Complete Guide. Ewasm: https://medium.com/chainsafe-systems/ethereum-2-0-a-complete-guide-ewasm-394cac756baf*

[90] *Swiss Blockchain Federation, Circular 2019/01 - Tokenized Equity, http://blockchainfederation.ch/wp-content/uploads/2019/12/SBF-Circular-2019-01-Tokenized-Equity-4.pdf), no. 3.6.*

[91] *Aktionariat Recovery Mechanism: https://aktionariat.com/documentation/smart-contracts/recoverable.html*

[92] *Aktionariat ERC20 Recoverable: https://www.cmta.ch/content/389/cmta-digital-assets-custody-standard-v-12-final-october-2020.pdf*

[93] *Alethena Equity (ALEQ) token contract: https://etherscan.io/address/0xf40c5e190a608b6f8c0bf2b38c9506b327941402#code*

[94] *Draggable ServiceHunter AG Shares (DSHS) token contract: https://etherscan.io/address/0x414324b0aba49fb14cbfb37be40d8d78a2edf447#code*

Traditionally, intermediaries such as banks or other regulated infrastructure providers have long been responsible for providing these trust elements. In a peer-to-peer network where all participants are equally privileged, trust must be established by the network itself.

The transfer of tokens can occur in various contexts. We group them into the following use cases which differ in terms of technical, regulatory and other legal and compliance requirements:

- Peer-to-Peer Transaction (see Section 2.2.1 below)
- Transaction on a Marketplace (see Section 2.2.2 below)
- Shares with Restricted Transferability (see Section 2.2.3 below)
- Whitelisting Ruleset Applied to Transfer Restrictions (see Section V.A.2 below [Use Cases])

The above-mentioned use cases will be described in more detail in the following sections. While regulatory and legal aspects of both private and corporate law must be considered when transferring tokens, the focus of this section is on how they can be achieved from a technical point of view.

2.2.1 Peer-to-Peer Transaction

a) Introduction

A blockchain-based token can essentially represent everything. Aside from the simple transfer of a stablecoin or payment token, it would therefore also be possible to transfer non-fungible tokens ("NFTs") (e.g., art) or security tokens, which are ledger-based securities. Within this section, a peer-to-peer transaction refers to the direct exchange of tokens between two parties that know each other. Section 2.2.2 below describes the use case if the parties do not know each other (for more information with regard to the legal context for token transfers, see Section C.1.3 below).

A P2P transaction of a ledger-based security is essentially a token transfer between two addresses. As mentioned earlier, addresses can be controlled by various forms of entities and ultimately, the owner of an address can be one or more natural persons as well a legal person that provides custodial or other services. Although a natural or legal person has the ultimate ownership of a token, it is possible to have large numbers of "technical owners" in between.

b) Anti-Money Laundering Aspects

The type of transferred security and additional restrictions that could arise from regulations and/or the token issuer's Articles of Association can also have an impact on how a transfer on a DLT infrastructure would have to be technologically structured from a legal and regulatory perspective. If what is referred to as a Virtual Asset Service Provider (VASP), such as an exchange, an ATM operator, or a wallet provider is involved in a transaction that contains a cash element (fiat currency or stablecoin), the same stringent AML/KYC requirements as traditional financial institutions are applied.

Although the "FATF travel rule" does not apply to the securities leg because shareholders are not clients and the issuance of ledger-based securities is not a financial intermediation[95] (see also "Anti-Money Laundering Regulations" in Section C.2.2 below), the rule applies to a potential secondary transaction, such as the clearing and settlement of the security token. The FATF travel rule which requires information on the sender and receiver of a transaction to "travel" alongside the transferred funds can technically be implemented via "decentralized SWIFT" messaging services. OpenVASP[96] is an open-source initiative that implements a P2P communication protocol on top of the Ethereum blockchain called "Whisper".[97]

c) Transfer Restrictions

As already indicated above, another important aspect that must be taken into consideration is the type of the security that is being transferred. This is especially important since certain types of securities may be subject to transfer restrictions that also have to be enforced on the blockchain. While for debt instruments, certain transfer restrictions may apply, the issuing company's

[95] *Swiss Blockchain Federation, Circular 2019/01 - Tokenized Equity, http://blockchainfederation.ch/wp-content/uploads/2019/12/SBF-Circular-2019-01-Tokenized-Equity-4.pdf, no. 4.3 ("… rules formulated in the Anti-Money Laundering Act are not applicable to the direct issuance of security tokens …").*

[96] *OpenVASP an open protocol to implement FATF's travel rule for virtual assets: https://github.com/OpenVASP*

[97] *Go implementation of the Whisper specifications: https://eips.ethereum.org/EIPS/eip-627*

Articles of Association could also limit the transfer of the membership rights associated with equity instruments. Such provisions in the Articles of Association may limit shareholder rights, such as voting rights or the entitlement to receive dividends, and may make it necessary for these rights to be held by the previous shareholder until the new shareholder has completed registration with the issuing company and has been approved by the necessary governing bodies within the issuing company (for more information on the legal context, see Section IV.C.1.3c) below).

If the Articles of Association do not impose a transfer restriction on the issuer, the transfer of the ledger-based security is straightforward, and the transfer of the ownership is final when the token is transferred.

Finally, an important aspect to be considered from a private law perspective is that the transfer of DLT-based securities should ideally be conducted without the involvement of the issuer as defined above and therefore no whitelisting should be enabled. Nevertheless, it may be necessary to limit transfers of ledger-based securities based on investor type or jurisdictions in order to comply with regulatory requirements. In this case, whitelister roles could configure whitelist rules and add / remove accounts from corresponding whitelists. The ERC1404 simple restricted token standard, for instance, allows for such whitelisting restrictions to be implemented and managed accordingly.

2.2.2 Transaction on a Marketplace

This section describes the use case of transactions between two parties that do not know each other. Various types of marketplaces exist. In traditional finance, securities are traded on centralized exchanges. Blockchain-based assets, however, can be traded on decentralized markets.

a) Introduction to Uniswap

The concept of decentralized exchanges has been pioneered by Uniswap, an open-source automated market maker (AMM) protocol for trustless token swaps on the Ethereum blockchain. Uniswap is powered by an automated market maker algorithm ("constant product formula")[98] and is implemented in the form of a system of non-upgradeable smart contracts on Ethereum.[99]

The main difference between transactions taking place via AMM protocols, compared to their counterparts on traditional centralized exchange structures, is that most AMM protocols do not rely on order books, and are rather based on liquidity pools. Each liquidity pool is made up of reserves of two ERC20 tokens and managed by a smart contract. The liquidity within these liquidity pools can essentially be provided by anyone since Uniswap is a completely permissionless protocol and the price of the assets being traded on Uniswap's decentralized exchange is determined according to the ratio between the two assets within the underlying liquidity pool. This approach differs substantially from centralized exchanges, where transactions happen off-chain and a matching engine matches corresponding buy and sell orders from an order book (see Section C.2.1 for more information on the regulatory aspects for DLT trading facilities).[100]

b) Role of Smart Contracts and Custodianship

The design of these decentralized exchange protocols heavily impacts how token transfers look like compared to transactions occurring on centralized exchanges or simple peer-to-peer transfers. This is due to the fact that rather than a buy or sell order being matched with a corresponding counterpart order being placed by another market participant, a user of an AMM protocol like Uniswap V2 interacts with the smart contract governing the liquidity pool. When a Uniswap user executes a token swap, tokens are therefore sent from the user's wallet address to a smart contract and vice versa.

Decentralized exchanges also differ from centralized exchanges with regard to custody. Since tokens are always kept in the user's self-custodied wallet, exchange protocols such as Uniswap never assume control over the user's asset and are

[98] *https://uniswap.org/docs/v2/protocol-overview/glossary/#constant-product-formula*
[99] *https://uniswap.org/docs/v2/protocol-overview/how-uniswap-works*
[100] *https://uniswap.org/docs/v2/core-concepts/pools*

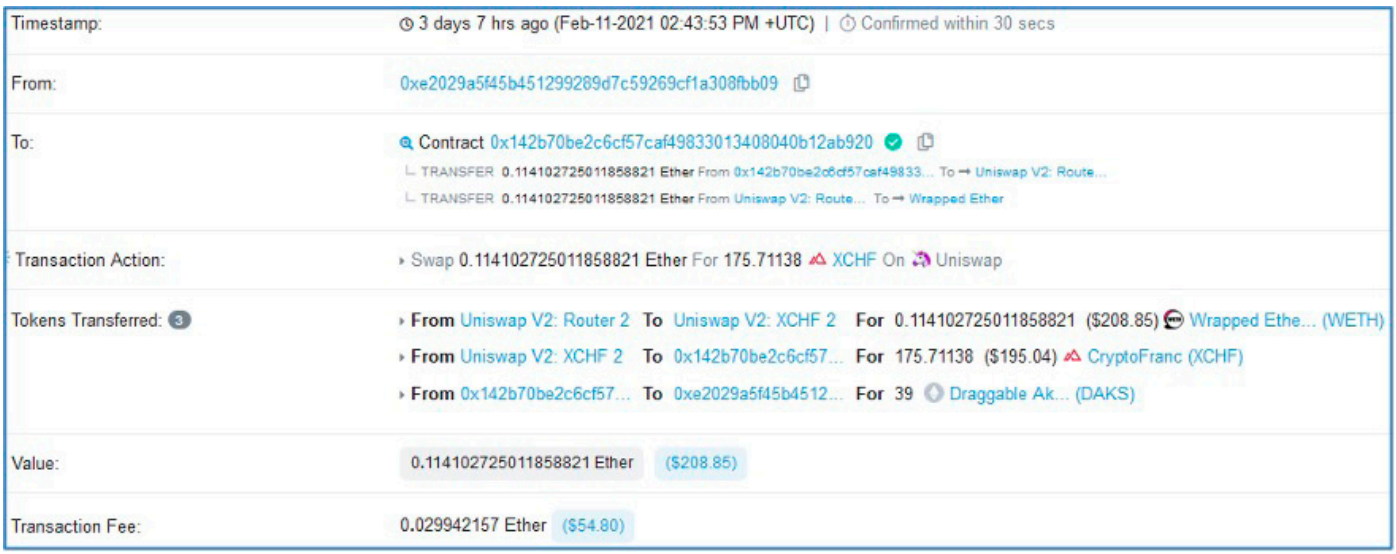
generally referred to as being non-custodial. Centralized exchanges on the other hand also hold client assets in custody (and hence are in control of the private keys).

c) Transfer of Equity Tokens

How the transfer of a blockchain-based equity tokens could be structured from a technical perspective, considering the need to account for possible transfer restrictions, is described in more detail below. This section does not provide any further details on transfers on centralized marketplaces.

As a permissionless protocol, Uniswap lacks KYC mechanisms entirely. Moreover, Uniswap is limited to the exchange of Ether (ETH) and ERC20 tokens. This is why NTFs (e.g., ERC721 or ERC1151) or security token standards that allow for certain restrictions (e.g., ERC1404 tokens), cannot currently be exchanged via Uniswap's V2 protocol. Nevertheless, there some equity tokens which are being traded on Uniswap as ERC20 representations. We have dedicated a more detailed outline of the transfer of an equity token from a Swiss-based company in Section V.A.1 below ("Use Cases Related to Capital Market Activities Trading a Swiss Equity Token on Uniswap"). It is important to note that in terms of corporate law, ERC20 tokens do not carry any shareholder rights (e.g., voting rights or entitlement to dividends). Therefore, a shareholder holding a "wrapped"[101] ERC20 representation of the share has to exchange the wrapped version for an unwrapped version of the token and complete the registration with the company in order to exercise membership rights (this is in line with the Tokenized Equity Circular from the Swiss Blockchain Federation).[102]

However, a transfer could involve a much greater number of smart contract interactions, regardless of whether it takes place directly between two wallets, or whether it is an interaction between a wallet with a smart contract-governed liquidity pool. One example is the Aktionariat token representing shares of Aktionariat AG. If an individual wishes to buy the equity token with Ethereum, the following happens on-chain:



[101] *Transaction Details: https://etherscan.io/tx/0x8d3a5898a3eb80c764b5ca5e26e88a76d99f328bea074b0080a4416195bf3f80*

[102] *Swiss Blockchain Federation, Circular 2019/01 - Tokenized Equity, http://blockchainfederation.ch/wp-content/uploads/2019/12/SBF-Circular-2019-01-Tokenized-Equity-1.pdf, no. 2.1 ("[…] Swiss law allows the separation of the securities registry [Wertrechtebuch] from the shareholder registry with the information on the beneficial owners [Aktienbuch], it is possible to tokenize registered shares and still keep the personal data of shareholders off-chain […]").*

1. UniswapV2Router02 smart contract will be called and ETH will be converted into Wrapped ETH (WETH). This is a "technical" step because in simplified terms, ETH is not "ERC20 compatible".
2. WETH then "acquires" Crypto Francs (XCHF), a Swiss franc-pegged ERC20 token (sometimes called "stablecoin"). This is necessary because Aktionariat is a Swiss entity and according to the current Swiss Code of Obligations, shares may only be issued at their nominal value of minimum 0.01 Swiss franc. The XCHF acts as proxy for the Swiss franc.
3. XCHF will then finally be "swapped" with the Aktionariat share token at the predefined price, before being executed by a smart contract.

Another example for non-trivial interaction of token contracts is described in the following use case.

d) Conclusion

Based on the explanations above, a Uniswap-style AMM protocol seems be a technically feasible means of transferring ERC20 representations of equity tokens between two parties that are unknown to each other. Nevertheless, most AMM protocols (including Uniswap) are permissionless and have no KYC processes in place. In order to enable issuers to comply with transfer restrictions potentially arising from investor type or jurisdiction, there is a high likelihood of the emergence of decentralized marketplaces with more advanced KYC mechanisms. Additionally, Uniswap V2 only supports the exchange of Ether (ETH) and ERC20 tokens. It is likely that more tightly regulated marketplaces with stricter KYC requirements will move toward supporting security token standards that allow for restrictions such as whitelisting or blacklisting (e.g., ERC14xx).

2.2.3 Shares with Restricted Transferability

As outlined above, the Articles of Association of a company issuing a ledger-based security can include provisions limiting the transfer of the membership rights and, in particular, make it necessary for the Board of Directors (or similar governing body) to approve of a new shareholder. This further exemplifies why not every share token transfer has to lead to a corresponding change in the company's share register (see Section 2.2.2).

Separating the technical aspect of the token transfer and the shareholder registration as out-lined in Section 2.2.2 allows for a fast technical transfer without formal registration, thereby mitigating some of the issue. Nevertheless, implementing a potentially necessary approval of the Board of Directors directly on the blockchain is preferable. From a technical perspective, one way to achieve this would be a multisig contract that controls the token contract of the equity token and prevents a token transfer from reaching finality until the required number of signatures has been given, for example two, i.e., the signature of the sender of the tokens as well as of the Board of Directors (indicating acceptance of the new shareholder), as described in Section 2.1.3 above ("Ownership Governance"). A similar multisig setup could also be applied on top of the wrapping contract used to convert a potentially wrapped version (without shareholder rights) to the actual security token.

Technically, the conversion from one token to the other and vice-versa can be achieved either by a *"transferAndCall"* function[103] to transfer token A and call the *"onTokenTransfer"* function on the receiving side to notify the transfer has occurred (e.g., used by Chainlink and DAI) or by the *"approveAndCall"* function to approve the transfer, and call the *"receiveApproval"* function on the receiving end to notify it can *"transferFrom"*. The basic problem lies in the architecture of the Ethereum ecosystem whereby tokens are somehow viewed as "second class" from the perspective of the protocol. The ability for users to interact with the network without holding any ETH has been a long-standing goal and is subject to several ERCs / EIPs:

- ERC777 Token Standard[104]
  This contains advanced features for interacting with tokens such as operators to send tokens on behalf of another address (contract or regular account) and send / receive hooks to offer token holders more control over their tokens.
- EIP-2771: Secure Protocol for Native Meta Transactions[105]
  A contract interface for receiving meta transactions through a trusted forwarder.

[103] *ERC: transferAndCall Token Standard #677: https://github.com/ethereum/EIPs/issues/677*

[104] *EIP-777: ERC777 Token Standard: https://eips.ethereum.org/EIPS/eip-777*

[105] *EIP-2771: Secure Protocol for Native Meta Transactions: https://eips.ethereum.org/EIPS/eip-2771*

3. Servicing of Securities: Dividends or Interest Payment Transactions

Ledger-based securities facilitate a truly digital representation and transfer of rights and obligations. This kind of native digital representation simplifies trading substantially – especially when it can be settled using a digital representation of cash or assets. For this reason, it is an essential step toward digitizing the financial value chain from end to end.

Nevertheless, the trading of securities is only one part of its lifecycle. Financial instruments such as debt or equity usually also distribute interest or dividend to investors. The processing and servicing of such instruments can also be greatly improved using DLT-based technologies.

In order to better understand this potential, we will illustrate it using the example of a debt security that is issued as a token on Ethereum. The token itself represents the security register. Under Swiss law it also needs to link to a registration agreement as well as to additional information on the instrument itself. Usually, this information is stored off-chain. Therefore, the token is just a link or pointer to the instrument itself which exists in traditional systems – ranging from core banking solutions to Excel.

3.1 New Paradigm for Asset Servicing

Nowadays, each party involved in the financial value chain maintains and updates its own ledger. The data needs to be synchronized and reconciled across all parties and systems, including term sheet information, corporate actions or net asset value calculations. These are well-established processes for traditional securities and can also be used for ledger-based securities. For example, an ISIN can be linked to the security and information made available through the existing rails and providers. Or existing fiat payment rails can be used to distribute interest to investors.

But DLT introduces a new paradigm: instead of replicating data and logic across all parties involved, a single and trusted source of truth can be made available to all parties on a shared ledger. And further, the same infrastructure can be used to distribute dividend or interest payments directly to investors. This will allow parties involved to service securities faster, cheaper and in a more transparent manner. The following sections will outline how a DLT infrastructure can facilitate corporate actions such as interest or dividend payments.

3.2 Know Your Asset (KYA) Concept

In the Blockchain Act of Lichtenstein, tokens are compared to shipping containers that can contain all kinds of (financial) claims. A token makes it easy to "ship" securities over the internet, but it provides the investor with very little information about the value which the token represents. If an investor or service provider wishes to understand what kind of cash flows are backing the debt token, they need to extract this information manually in a cumber-some way from the natural language legal document or term sheet.

A first step toward making the processing of securities faster, more efficient, and transparent is to attach the machine-readable 'freight' documents to the container itself. In the case of a debt token, the following data could be attached: issuer, instrument, jurisdiction, issue / maturity date, interest rate, interest cycles, day count conventions, etc. This digital representation of the product becomes the single source of truth for all parties.

Players are enabled to derive all kinds of information directly from the token itself such as the assets' terms, its status, future cash flows, etc. This would greatly facilitate a more auto-mated pricing, reporting and listing of such securities. Further efficiency could be increased, reconciliation efforts minimized and errors prevented.

To unlock these efficiency gains, the industry needs to collaborate and start adopting shared standards to create ledger-based securities (containers) and encode the related information in a structured form (machine-readable freight documents). Plug-and-play securities like these would greatly facilitate straight-through processing.

There are different ways in which machine-readable data can be tied to a debt token on Ethereum:

(i) Data is stored off-chain (external storage like Cloud services or IPFS)
(ii) Data is attached to transaction as call or event data (immutable and verifiable)
(iii) Data is stored on-chain (expensive but smart contracts can verify and use data)

Each of these has its own trade-offs in terms of gas cost, reliance on third parties and availability for onchain processing.

Independently of how and where the data will be stored, it is crucial that parties agree on standardized ways to describe financial instruments and their reference data. If every party reinvents the wheel and defines them in their own way, many of the potential benefits of a DLT infrastructure will be cancelled out by interoperability challenges. The industry would need a lot of adapters to plug this kind of a financial infrastructure together.

Fortunately, there are a number initiatives that have been addressing these challenges – it is up to the parties to adopt them. Worth mentioning are e.g., the highly comprehensive ACTUS financial contract standard which is currently being explored by the F.D.I.C. in the U.S. to simplify reporting by the 4,000 banks it regulates. Also, the work carried out by the ISDA on their common domain model for derivatives and the ISO 10962 asset-type classification. In Switzerland, the Capital Market Technology Association (CMTA) is working with industry members on several blueprints and the InterWork Alliance Group is promoting standardization on an international level together with support from the Swiss Digital Exchange (SDX).

3.3 Servicing Corporate Actions On-Chain

Based on the available reference data, a debt token can be serviced in a very transparent and verifiable manner. The issuer / servicer can derive the next interest payments directly from the attached data and subsequently record an updated status for the instruments once interest has been distributed, thus, providing all parties with accurate and timely information on the performance of the security.

Either the issuer themselves or a servicer can use the DLT infrastructure to distribute the interest in the form of a payment token (i.e., a stablecoin or representation of cash). Especially for cross-border setups, this is a very fast and convenient way compared to traditional fiat payment rails. At the defined date of distribution, the issuer / servicers send the interest amount directly to the wallets of the investors in proportion to their holdings.

A precondition for this is that the issuer must be able to batch-process the distribution to all investors. And investors or their service providers must be able to process and convert the tokenized cash back into fiat.

3.4 Making Tokens Smart and Intermediaries Optional

In the future, participants can unlock further benefits by embedding the servicing functionality directly on-chain in the form of smart contracts. For example, an on-chain calculation agent can be queried by all parties to derive the event schedule for our debt security and obtain more information on the next interest payment. On the corresponding date, the issuer or servicer will send the interest amount to an on-chain paying agent which verifies the amount, distributes it and updates the status of the debt instruments.

This is in contrast to the outlined batch-processing by the issuer above. If the paying agent functionality is embedded in the token, the issuer simply sends the entire interest amount to the token contract. The token then holds the interest amount and investors can withdraw the amount they are entitled to. The token itself takes care of recording who is entitled to which amount and who has already withdrawn which amount. One example of this kind of implementation is the Funds Distribution Token (ERC-2222) which is used by some Decentral Autonomous Organizations (DAO), such as the LexDAO to distribute funds between its members on Ethereum. Thus, parties do not need to rely on an intermediary to assume

responsibility for it and to ensure everything is handled as agreed. Furthermore, parties have a continuous and transparent audit trail of cash-flow distributions.[106]

As outlined above, a token would not only represent the register, but also have additional servicing logic embedded, thus creating a smart token that can take care of its own life cycle. Parties would not need to replicate data and logic across all their systems because the security is serviced using a mutual and trusted execution infrastructure based on DLT.

DLT infrastructure provides the opportunity to overcome today's "walled-garden" approach and simplify the financial stack. The common areas of the servicing of securities are implemented using a shared DLT infrastructure. For this reason, parties can focus on the areas that are different and do not need to use the same functionality repeatedly.

This will be a gradual evolution from the off-chain to on-chain processing of securities since there are several challenges that need to be overcome on a step-by-step basis, one of which being interoperability challenges. Without reasonable standardization efforts, the servicing cost of securities on a DLT infrastructure will increase exponentially. Furthermore, participants and their custody solutions need to be able to handle such securities, integration with existing systems needs to be addressed and finally, the cost and efficiency of serving securities on-chain needs to improve in the years to come.

C. Legal Context

1. Civil Law

1.1 Scope

a) Transferability of the Tokens

Using the DLT infrastructure to transfer assets requires such transfers to be recognized by the legal system and for discrepancies between the technical control over the tokens and the legal position to be minimized. This section focuses on the legal aspects relating to the transfer of the tokens. We assume that the respective tokens – reflecting the relevant rights, if any – are operational and technically transferable. This means that we have excluded the preparatory stages of a token project. At an early stage of the preparation of a token-generating event, the intended allocation of the tokens may already be reflected in the protocol; however, the (future) tokens themselves may not yet be transferable (wallet data could be transferable off-chain). In addition, (preoperational) tokens may technically be transferable via the protocol, but not yet grant the intended rights.

b) Transfer of Tokens on Contractual Basis

In the following, we discuss the transfer of tokens based on a *contractual agreement* concluded between the transferor and the transferee. The legal situation depends on whether or not the tokens to be transferred represent any legal rights. Contractual agreements are not the only basis for a change in the holder of tokens. For instance, the tokens may belong to an estate of a deceased person where all assets belonging to the estate are automatically acquired by the heirs in accordance with the law ("universal succession"). Some court judgments modify the legal relationships directly instead of merely instructing a party to transfer assets. In this case, there are no doubts about the legal recognition of the transfer. However, the challenge is to ensure that the DLT infrastructure (ledger) correctly reflects the revised own-ership situation and that the acquirer has access to the tokens and is able to dispose of them. It may be necessary to cancel existing ledger-based securities in order to create new positions or to allow the enforcement of the rights outside the register.

c) Overcoming the Written Declaration of Assignment

Prior to the recent amendment to the Swiss law which entered into force at the beginning of February 2021, it was less clear how to link tokens with legal rights, such as claims or the membership of shareholders. Under existing Swiss civil law (art. 165 para. 1

[106] *See: https://github.com/ethereum/EIPs/issues/2222; https://medium.com/lexdaoism/lexdao-engineering-year-review-2020-1-950c56f3af81*

and art. 973c para. 4 CO), the transfer of claims and of (simple) uncertificated securities generally requires a written declaration of assignment signed by the existing creditor and holder of the right (transferor). An authenticated electronic signature combined with an authenticated time stamp is deemed equivalent to the handwritten signature (art. 14 para. 2bis CO). Due to this formal obstacle, the technical transfer of tokens has not guaranteed the assignment of the underlying rights to date.[107] The creation of the ledger-based security by the Swiss legislator largely filled the gap and increased the legal certainty for transactions based on a DLT infrastructure.

1.2 Transfer of Payment Tokens

a) Description of Payment Tokens

In this first category, we discuss pure payment tokens (i.e., cryptocurrencies). They may represent significant economic value, but do not grant any rights to their holders, i.e., neither any rights vis-à-vis a counterparty (namely the issuer of the tokens) nor any rights *in rem.*

b) Legal Situation

The lack of an underlying right which needs to be transferred to a third party facilitates the legal situation somewhat. The technical means, i.e., the payment token, does not have to be linked to the legal concept of the right. Hence, the Swiss government takes the view that there is no need to adapt Swiss civil law in order to regulate the transfer of cryptocurrencies.[108]

c) Implications

However, the predominance of the technical sphere excludes interventions by the legal system to a large extent (*"Code is Law"*). For example, it is difficult, if not impossible, to restore stolen or lost payment tokens. Heirs who obtained from the decedent payment tokens as part of an estate cannot possess the assets if they do not have the necessary technical access to the tokens. The bona fide acquirer of payment tokens will not be protected. This legal gap and uncertainty are unsatisfactory.

The new Swiss DLT legislation clarifies the treatment of crypto-based assets – which include cryptocurrencies – in the event of bankruptcy (art. 242a et seq. Swiss Debt Enforcement and Bankruptcy Act, art. 37d BA). However, the provisions governing ledger-based securities do not apply to pure payment tokens. This narrow scope of the DLT legislation has been criticized.[109] There is an equivalent need for rules governing the transfer of payment tokens. And the classification of tokens is not always clear, which makes it difficult to determine the scope of the DLT legislation.

In light of this, it is recommended that the parties contractually agree the essential elements of the transfer of the payment tokens.

1.3 Transfer of Ledger-Based Securities

a) Characteristics of Ledger-Based Securities

i) Description of Ledger-Based Securities

The amended legislation in Switzerland provides for ledger-based securities (registered uncertificated securities, *"droits-valeurs inscrits"/"Registerwertrechte"*). A ledger-based security is a right which – pursuant to a Registration Agreement of the parties – has been registered in a ledger and which can only be asserted or transferred through such ledger (see art. 973d para. 1 CO). The ledger technically grants the (factual) power of disposal over the rights to their holders ("creditors"), in a similar way to the possession of a physical certificate for securities.

The ledger-based securities include rights vis-à-vis a counterparty, as expressed in the term *"counterparty tokens"*. The rights can have a wide variety of forms in terms of content, such as the right to demand a payment, the delivery of goods or the provision of services, or shareholder membership rights. The technical basis of the ledger-based securities is the ledger (uncertificated securities register). Each token transfer must be initiated through and reflected in the ledger.

[107] *Cf. Swiss LegalTech Association, Regulatory Task Force Report, p. 47 et seq.*

[108] *See Dispatch of Swiss Federal Council on DLT legislation dated November 27, 2019, Federal Gazette 2020, p. 242 and p. 259 (German version).*

[109] *Swiss Blockchain Federation, Circular 2021/01, p. 10 et seq., no. 4.*

ii) Different Types of Shares

A company may use different technical possibilities to reflect the shares: traditional certificates in printed form, simple uncertificated securities (*"droits-valeurs simples"/"einfache Wertrechte"* in terms of art. 973c CO), ledger-based securities or intermediated securities. The technical and legal solutions must be consistent, and the different concepts must not be commingled. It is not possible to create tokens reflecting ledger-based securities and simultaneously provide for transfers of such tokens without the use of the DLT infrastructure; neither is it possible to create simple uncertificated securities that are (exclusively) transferable through the DLT infrastructure.

Irrespective of the form of the shares used by the company, initially, such shares need to be *formally issued* in a traditional manner, i.e., at incorporation or for a capital increase, based on written subscription declarations by the shareholders and a provision in the Articles of Association. The newly issued shares do not exist before the relevant entry in the commercial register has been published in the Swiss Official Gazette of Commerce (art. 936a para. 1 CO. Tokens intended to represent shares depend on the existence of such underlying shares in accordance with company law. In sum, shares issued as ledger-based securities require a valid creation according to company law and, in addition, they need to be registered in the ledger. Without registration in the ledger, the shares cannot qualify as ledger-based securities, but they could still exist as simple uncertificated securities. The issuer (company) should ensure that all shares that are part of the company's share capital are registered in the ledger or have been issued as uncertificated securities or printed as share certificates.

iii) Harmonization of Registers

The question arises as to how the company should proceed if the aggregate number, or the allocation, of the tokens is not consistent with the aggregate number, or the allocation, of the shares. The owner(s) of shares that have been validly issued and are reflected in the ledger, but not allocated to a certain (token) holder, should be determined according to the initial subscription for such shares. In the event of a firm commitment underwriting agreement, owing to the lack of an ultimate shareholder, these shares would be owned by the financial institution or any other intermediary that formally subscribed to the shares as commissioner. A proportional (formal) reduction of the number of allocated shares or, as the case may be, of allocated tokens may be necessary if it is not possible to detect a specific holder of redundant tokens or shares.

iv) Intermediated Securities

Claims and membership rights credited to a deposit account held with a bank or another financial institution (custodian) might qualify as intermediated securities (*"titres intermédiés"/"Bucheffekten"*) in terms of the relevant Act (see art. 2 and 3 Swiss Intermediated Securities Act [ISA]). It is permissible to create intermediated securities on the basis of DLT securities which have been transferred to a DLT trading system or another custodian and booked to an account held with the custodian. During the existence of the intermediated securities, ledger-based securities are to be *immobilized* (art. 6 para. 3 ISA). Such immobilization requires that the securities can no longer be transferred without the involvement of the custodian.

The transfer of intermediated securities occurs outside the (DLT) ledger in accordance with the requirements set out in art. 24 ISA: The transferor must *instruct the financial institution* to transfer the securities. The transfer becomes effective as soon as the acquirer's financial institution has credited the securities to the acquirer's deposit account, subject solely to the restrictions on the transfer of registered shares.

b) Transfer

i) Requirements for Transfers

The transfer of the ledger-based securities is initiated by the holder (transferor) or its representative, basically without any central intermediary. As indicated above, the holder ("creditor") or its agent is expected to have the (sole) power of disposal over the rights. By contrast, the issuer ("debtor") should not have such power of disposal.[110]

Swiss law does not specify the requirements for a transfer of ledger-based securities. Art. 973f para. 1 CO merely stipulates that the transfer is subject to the provisions of the Registration

[110] *See Dispatch of Swiss Federal Council on DLT legislation dated November 27, 2019, Federal Gazette 2020, p. 279 (German version).*

Agreement. Hence, the Registration Agreement should refer to the protocol and the relevant rules governing transfers on the DLT infrastructure. A general reference to well-known protocols (such as tokens issued according to the ERC20 token standard on the Ethereum blockchain) should be sufficient; otherwise, further details on the characteristics of the transfer should be provided.[111] This means that the execution and (legal) effectiveness of the transaction mostly depend on the ledger's technical features and rules. When the applicable consensus rules have been complied with and the transfer completed, the acquirer should obtain the technical power of disposal over the rights through the ledger. The transfer needs to be recorded in the DLT infrastructure.

A transfer of ledger-based securities outside the ledger ("off-chain"), for instance, based on a written assignment declaration or the disclosure of the private key, would not be effective, unless provided for by the law (as in case of inheritance) or stipulated by a court order. It is, however, possible to update the register afterwards and to register off-chain transactions (or at least the outcome of such transactions) subsequently. These transactions become legally effective upon registration in the ledger. The acquirers must be able to verify the integrity of their registration (art. 973d para. 2 no. 4 CO). In the interest of technological independence, the law does not expressly refer to the blockchain technology or DLT. However, the characteristics of the ledger-based securities imply the application of such technology. The law would not exclude the use of a central ledger. A central ledger fulfilling the legal requirements does not exist for the moment.

ii) Details of Transfer

The Registration Agreement between the issuer ("debtor") and the token holders ("creditors") must stipulate that the ledger-based securities are registered in the ledger and that they may only be transferred or asserted through this ledger (art. 973d para. 1 CO). Such minimum Registration Agreement content could be included in subscription forms. It is, however, advisable to address further details regarding the transfer of tokens in the complementary data of the register or in separate regulations. Apart from referring to the underlying protocol and explaining the requirements as well as the essential features of the transfer of tokens and its validation, the issuer should clarify the *point in time* when the transfer of tokens can no longer be revoked by the transferor and when the transaction becomes effective, i.e., when the acquirer legally receives the tokens ("finality"). The relevant rules should be consistent – and interpreted consistently – with the technical features of the ledger.

In the event of *bankruptcy* involving a creditor following the transfer of ledger-based securities, the transfer becomes legally effective (which means that the tokens do not belong to the transferor's bankruptcy estate) if the transaction (i) has been executed (i.e., authorized) by the creditor prior to the declaration of bankruptcy, (ii) is irrevocable for the creditor pursuant to the applicable rules of the ledger or the trading system, and (iii) has in fact been registered (i.e., validated) in the ledger within a period of 24 hours (art. 973f para. 2 CO).

Furthermore, the issuer should specify the procedure applied to forks in the blockchain system and to *changes* in the Registration Agreement, for instance in the event of a technical update of the ledger, and determine the *applicable law* governing, inter alia, the transfer of tokens.[112]

The holders of ledger-based securities should at least tacitly accept the Registration Agreement and the further rules governing the tokens. This also applies to first holders of newly issued tokens as well as to any subsequent acquirers of tokens. The Registration Agreement and further rules can be integrated in or linked with the Terms and Conditions of issuance (in case of bonds) or reflected in regulations adopted by the Board of Directors or management of the issuer. The issuance of shares in the form of ledger-based securities as such has to be mentioned in the Articles of Association (art. 622 para. 1 CO). The rules governing the tokens play a similar role as the Terms and Conditions of traditional contracts. Consequently, a court could consider non-standard clauses as not binding, unless they are specifically red-flagged. Such an outcome may result in a problematic discrepancy between the legal rules and the technical features of the protocol.

[111] *Swiss Blockchain Federation, Circular 2021/01, p. 10, no. 3.2.*

[112] *Swiss Blockchain Federation, Circular 2021/01, p. 10, no. 3.2; Swiss LegalTech Association, Regulatory Task Force Report, p. 20 et seq.*

Changes to the Registration Agreement or to the implementing rules governing the tokens do not necessarily require the consent of all holders (creditors) or a unanimous resolution. Rather, the rules could – and usually should – provide for appropriate majority rules. The modification of provisions integrated in the Articles of Association would be subject to the quorum required by company law. Changes to regulations adopted by the Board of Directors or the management of the issuer do not require the involvement of the token holders.

iii) Interoperability with Other Protocols

Potential interconnections between different ledgers poses an additional technical and legal challenge. The rules specifying the tokens should clarify the requirements for such "qualified" transfer of tokens leaving the current ecosystem. Interoperability may apply from the beginning or be introduced later. Should the rules governing the tokens not yet provide for this kind of interoperability, the aforementioned conditions for changes to the Registration Agreement or to the implementing rules would apply.

By contrast, the replacement of the issuer ("debtor") of the ledger-based securities would require the involvement of all parties, including the new debtor. Creditor and debtor would change concurrently. The situation would be similar to a bank transfer to an account held with another bank. Where tokens represent claims, the holder ("creditor") is required to accept the new debtor. It would be possible to obtain the approval of the creditors in advance by way of a power of attorney. To be legally effective, this transfer may require additional formal procedures, such as a capital decrease by the previous debtor and a subsequent capital increase by the new debtor.

c) Acquisition of Ownership

i) Register of Shareholders and Beneficial Owners

The acquisition of ledger-based securities must comply with applicable legal requirements. In the case of shares, Swiss company law provides for the registration of the acquirer in the share register. It is advisable to at least provide for a technical connection between the ledger and the share register. It is also possible for the ledger to constitute the share register, provided the ledger or its complementary data contain the information required by law. The registration in the share register must include the names and addresses of the owners and usufructuaries (art. 686 para. 1 CO).

Furthermore, companies limited by shares (*"société anonyme"/"Aktiengesellschaft"*) and limited liability companies (*"société à responsabilité limitée"/"Gesellschaft mit beschränkter Haftung"*) are legally required to register the beneficial owners of shareholders holding at least 25 percent of the share capital or voting rights (unless the shares qualify as intermediated securities or are listed on a stock exchange; art. 697l and art. 790a para. 5 CO). The shareholders should be enabled to fulfill their respective reporting obligations directly by using the DLT infrastructure. Issuers that are not subject to the anti-money laundering legislation are generally not required to verify the identity of the shareholders. Technically, the ledger may, but does not necessarily have to exclude transfers before or without observing the applicable reporting obligations. Legally, the exercise of the membership rights by shareholders does not depend on the entry in the share register, provided that the ledger sufficiently establishes the position of the shareholder. By contrast, any breach of the obligation to notify the company of the beneficial owner results in the suspension of the voting and financial rights of the respective shareholder as a matter of mandatory law (art. 697m CO). The law expressly states that the Board of Directors is responsible for ensuring that none of the shareholders exercises any rights in violation of their reporting obligations relating to beneficial ownership.

ii) Transfer Restrictions

Transfer restrictions, such as the requirement of an *approval by the Board of Directors* of the issuer set out in its Articles of Association (art. 685a para. 1 CO), should be technically implemented in the ledger to avoid transfers which are subsequently declined or otherwise impeded (see Section B.2.2.3 above). Swiss corporate

law allows for objections to transfers by companies without listed shares in the following circumstances: (i) with good cause, provided that the Articles of Association specify the particular reasons given (such as the economic independence of the company), (ii) accompanied by an offer of the company to acquire the shares from the transferor at their real value, or (iii) where the transferees do not expressly declare that they will acquire the shares in their own name and for their own account (art. 685b CO). An implied consent is assumed after three months following receipt of the application if the company does not object. The DLT infrastructure should be consistent with the legal situation where a transfer of tokens has not (yet) been approved by the Board of Directors: The ownership and shareholder rights remain with the transferor. Hence, the ledger should technically exclude successful transfers of tokens without or prior to the necessary approval.

iii) Causal Nature of Disposal

Pursuant to the Swiss government and the prevailing view expressed by the legal doctrine, the effectiveness of the transfer of ledger-based securities depends on the legal validity of the underlying contractual agreement. This position corresponds to a causal rather than an abstract understanding of the connection between the disposal of the assets and the underlying contract, such as the sale or donation.[113] In the event that a court declares the underlying contract to be invalid, for example, due to a material error or fraud, the ledger must be adapted and the respective number of ledger-based securities must be reallocated to the transferor.

By contrast, in the event that *intermediated securities* are transferred in accordance with the ISA, pursuant to the major legal doctrine, the disposition is *abstract,* i.e., independent of the validity of the underlying contract.[114]

iv) Acquisition in Good Faith

The acquisition of a ledger-based security from a creditor without power of disposal, but duly registered in the ledger, is legally protected, unless the acquirer acted in *bad faith* or with *gross negligence* (art. 973e para. 3 CO). The legal protection of the acquirers implies that the previous legitimate holders of the rights lose their entitlement; they can prosecute the transferors for acting without power of disposal (e.g., a hacker), if it is not possible to prevent the acquisition in good faith by cancelling the ledger-based securities before the transaction with the acquirers has been executed.

The *objections* which the debtor could raise against the new creditor are legally restricted (see art. 973e para. 4 CO). In the event of a dispute between a bona fide acquirer of a ledger-based security and a bona fide acquirer of a traditional security paper, the latter shall prevail (art. 973f para. 3 CO).

d) Creation of Security Interests

Instead of transferring ownership, counterparty tokens may be transferred to create a security interest in the tokens. Technically, the transfer of the tokens remains the same. The acquirer obtains full factual control over the tokens. The limited purpose of the transfer and the restricted legal position of the acquirer result from the underlying contractual arrangement.

Alternatively, security interests can be established by merely designating the relevant ledger-based securities in the ledger as security and ensuring that the security holder is solely entitled to dispose of the ledger-based securities in the event of default (art. 973g para. 1 CO; see the similar mechanism in art. 25 ISA). It is recommended to agree on further details on the procedure and the rights of the parties in the security agreement or the Registration Agreement.

e) Discrepancies Between Ledger and Legal Situation

i) Manual Rectifications and Adjustments

There are several instances in which the legal system may require an intervention and correction of the ledger. Some examples, such

[113] *Dispatch of Swiss Federal Council on DLT legislation dated November 27, 2019, Federal Gazette 2020, p. 286 (German version); STEFAN KRAMER/URS MEIER, Tokenisierung von Finanzinstrumenten, GesKR 1/2020, p. 60–77, p. 68; HANS CASPAR VON DER CRONE/FLEUR BAUMGARTNER, Digitalisierung des Aktienrechts – Die Ausgabe von Aktien als Registerwertrechte, SZW 4/2020, p. 351–364, p. 358.*

[114] *See PATRICK HÜNERWADEL/ROLAND FISCHER, in: Heinrich Honsell/Nedim Peter Vogt/Rolf Watter (ed.), Wertpapierrecht, Basler Kommentar, Basel 2012, Preliminaries of art. 24–26 no. 22 et seq.*

as the rescission of or challenge to the agreement or the cancellation of the ledger-based securities, have been mentioned above or will be discussed below. It is justified that the Registration Agreement or the "Terms and Conditions" of the register entitle the issuers or authorized representatives to manual interventions or amendments to the ledger in exceptional circumstances, subject to precise conditions to be specified, unless corrections occur automatically, for example, due to integration in a smart contract. The potential measures include suspending the whole ledger, whitelisting (i.e., the necessary release of addresses to which tokens can be transferred), freezing certain addresses and restoring lost tokens.[115] Manual interventions may correct an inappropriate allocation of tokens or even a fraudulent use of the ledger, but at the same time, they enable potential abuses by the issuer or its representatives. In any event, the issuer has to meet the legal requirement of art. 973d para. 2 no. 1 CO which constitutes the main principle: The ledger shall grant power of disposal to the holders ("creditors"), but not to the issuer ("debtor"). Serious restrictions of the power of disposal of a token holder would require an order by the competent authorities.

ii) Cancellation of Ledger-based Securities

The previous holders ("creditors") of ledger-based securities who lost the private key are entitled to request the cancellation (*"annulation", "Kraftloserklärung"*) by the *court,* provided that they succeed in furnishing prima facie evidence of their former power of disposal and their loss of it (art. 973h para. 1 CO). A call for presenting the lost security within six months has to be published in the Swiss Official Gazette of Commerce (cf. art. 983 et seq. CO). Upon completion of the cancellation procedure, the previous ledger-based securities are nullified, and the holders of the lost ledger-based securities can exercise their rights out-side the ledger (by way of simple uncertificated securities) or to request the allocation of new ledger-based securities. The technical features of the ledger should enable the issuer to effectuate and implement such cancellation within the system ("kill switch", "forced transfer", etc.; for the technical implementation of the cancellation, see Section B.2.1.5 above).

The official cancellation by way of a court procedure does not exclude an optional, less formal – as well as cheaper and faster – *private cancellation* set out in the Registration Agreement or in other regulations (art. 973h para. 2 CO).[116]

1.4 Transfer of Ownership Tokens

a) Description of Ownership Tokens

Ownership tokens represent rights in rem, i.e., rights which allocate (movable or immovable) properties, intellectual property and similar objects in an absolute and exclusive manner to their owners, protected against any third parties (*"erga omnes"*). There is no "debtor" of the ownership token. The membership rights of a shareholder are not a possible content of ownership tokens, but could be part of ledger-based securities (see previous section).

b) Legal Situation

Basically, Swiss DLT legislation does not apply to ownership tokens.[117] At present, it is not legally possible to link tokens directly with the right of ownership to property. This means that it is not enough to transfer the token in order to transfer ownership unless movable property is in the possession of a third party (depository) that can be contractually instructed – without moving the property – to hold possession for the acquirer or, alternatively, the transferor holds possession for the acquirer ("tiered" possession). Otherwise, the ownership of the property would have to be transferred to the acquirer of the token separately and in fulfillment of the applicable formal requirements, such as the transmission of the legal possession (*"mise en possession", "Übergang des Besitzes"*) or a public deed for the purchase of real estate.

However, documents of title to goods (*"titres représentatifs de marchandises", "Warenpapiere"*, art. 1153 et seq. CO) may represent a contractual claim for return and consequently be issued as ledger-based securities (art. 1153a para. 1 CO). In addition, it is possible to collect financial means for the acquisition of property and to issue ledger-based securities reflecting the relevant bond, i.e., the debt claim of each token holder against the issuer, without granting any direct entitlement to the property to the

[115] *Swiss Blockchain Federation, Circular 2021/01, p. 4 et seq., no. 2.2.2.*

[116] *Swiss Blockchain Federation, Circular 2021/01, p. 11, no. 5.*

[117] *See Dispatch of Swiss Federal Council on DLT legislation dated November 27, 2019, Federal Gazette 2020, p. 277 (German version).*

token holder. Furthermore, the law provides for the issuance of securities relating to real estate (see art. 842 et seq. Swiss Civil Code [*mortgage certificate / "cédule hypothécaire" / "Schuldbrief"*] and art. 875 Swiss Civil Code [*bonds secured by mortgage right / "titres fonciers" / "Anleihenstitel mit Grundpfandrecht"*]).

2. Regulatory Aspects

2.1 Financial Market Infrastructure

a) Transactions Outside Regulated Financial Market Infrastructures

The operation of centralized trading platforms for tokenized assets must be distinguished from distributed peer-to-peer (person-to-person) platforms. Centralized trading platforms are usually operated by an individual legal entity and rely on a private infrastructure to match supply and demand, which is managed internally within their own technical infrastructure. By contrast, peer-to-peer platforms bring buyers and sellers together and connect users directly and also operate autonomously through self-executing smart contracts (i.e., escrows that work without a trusted third-party). Unlike centralized trading platforms, buyers and sellers can settle trades based on their own terms. This paradigm shift from centralized to peer-to-peer platforms triggers additional legal and regulatory questions. In this regard, the Swiss Federal Council acknowledged the fact that the operation of peer-to-peer platforms has not been subject to any authorization requirements pursuant to the FinMIA so far, irrespective of whether the transactions brokered on the platform are related to securities.[118] Also, platforms used to publish purchase and sale interests without a contract being concluded based on defined platform rules (also called bulletin boards)[119] can be operated without the need for authorization.

b) Regulated Financial Market Infrastructures

The simultaneous exchange of bids between multiple participants and the conclusion of contracts within non-discretionary platform rules are typically reserved for trading venues, thus requiring an authorization under the FinMIA. Trading venues are either stock exchanges or multilateral trading facilities (art. 26 FinMIA). Both types of trading venues only accept supervised financial institutions as participants (art. 34 FinMIA). Thus, individual clients or unregulated legal entities must act through supervised intermediaries (such as banks or securities firms) as eligible participants to access trading venues. Unregulated participants only have direct access to organized trading facilities which allow for multilateral trading in securities on a discretionary basis. As a result, the existing authorization types did not cover the combination of direct access by unregulated participants to multilateral trading in securities based on non-discretionary rules.

c) The DLT Trading Facility as a New Type of Financial Market Infrastructure

The new type of financial market infrastructure called "DLT trading facility" bridges this gap. A DLT trading facility is a commercially operated institution for the multilateral trading of DLT securities for the purpose of simultaneously exchanging bids between multiple (regulated and unregulated, i.e., retail) participants and concluding contracts based on non-discretionary rules. In addition, to qualify as a DLT trading facility, one of the following requirements must be met: (a) admission of legal entities other than supervised financial institutions or individual clients as participants (participation only in own name and for own account); (b) provision of central custody of DLT securities based on uniform rules and procedures; or (c) provision of clearing and settlement for transactions in DLT securities based on uniform rules and procedures.

d) Two Types of Service Offerings for DLT Trading Facilities

A DLT trading facility can be grouped into two categories[120] based on the services it offers: a) trading and b) in addition to trading, custody as well as clearing and settlement services. As a result, DLT trading facilities do not require the services of a separate CSD (art. 61–73 FinMIA), such as MTFs and stock exchanges for custody and settlement purposes. If counterparty risks are generated by the type of trading system used, a central counter-

[118] *Federal Council, Legal framework for distributed ledger technology and blockchain in Switzerland, p. 99.*
[119] *FINMA Circular 2018/1 Organised trading facilities, no. 10.*

party (art. 48–60 FinMIA) is still required. Its functions cannot be assumed by the DLT trading facility.[121] The services provided by a DLT trading facility in the area of post-trading is functionally comparable with that of central securities depositories and, as such, similar regulatory requirements must be met.[122] This includes, inter alia, capital adequacy and liquidity requirements. On the other hand, DLT trading facilities are subject to certain requirements which apply to trading venues (art. 73b FinMIA), such as, inter alia, requirements regarding self-regulation, organization of trading (including provisions that ensure effectual transaction finality), trading transparency and other organizational requirements. In the trading area, the DLT trading facility is more comparable to a multilateral trading facility than to an exchange. In particular, a "listing" in the sense of art. 2 let. f FinMIA cannot be provided.

e) Assets Tradable on a DLT Trading Facility

A DLT trading facility may admit DLT securities and other assets. For both types of tradable objects, corresponding regulations must be implemented (art. 73d para. 2 FinMIA). The admissibility of derivatives structured as DLT securities is limited to products without current value or leverage component (art. 58f para. 2 of the Financial Market Infrastructure Ordinance – FinMIO). DLT securities and other assets that significantly impede the implementation of AML provisions (e.g., "privacy coins") or which could impair the stability and integrity of the financial system are not allowed (art. 58f para. 3 FinMIO). FINMA may specify such non-admissible assets.

A DLT security is a security established in the form of a ledger-based security (art. 973d CO) or other uncertificated securities that are held in distributed electronic registers and ful-fill the additional requirements of art. 2 letter b^{bis} FinMIA.

If the distributed electronic register is not operated by the DLT trading facility itself (which is typically expected to be the case), prior to admission and at least on a yearly basis, it must verify if the distributed ledger meets the necessary requirements (art. 58g para. 2 FinMIO).

As with traditional securities, DLT securities are subject to prospectus obligations and requirements set out in art. 35–57 Financial Services Act (FinSA). The DLT trading facility must provide its participants with the relevant prospectuses (or the key information documents) for the DLT securities it has admitted to its facility (art. 58i para. 1 FinMIO).

f) Easing of Requirements for Small DLT Trading Facilities

A DLT trading facility can be further divided into standard and small DLT trading facilities. As small DLT trading facilities are deemed to pose a lower risk to financial market participants and to the proper functioning and stability of the financial system, they benefit from easing of requirements. To qualify as small DLT trading facility, it must not exceed any of the three thresholds[123] regarding a) trading volume, b) volume of assets under custody and c) clearing and settlement volume. Such small DLT trading facilities benefit from the following easing of requirements (see art. 58l para. 1 FinMIO): 1) reduced governance requirements; 2) no additional capital and liquidity requirements for the provision of ancillary services (however, additional organizational measures can still be imposed); 3) ease of business continuity management requirements if the operations can be transferred to another DLT trading facility; 4) no independent bodies are required for (self-)regulatory tasks; 5) no appeal body is required; and 6) no internal audit function is required.

In addition, if no custody or clearing and settlement services are provided by a small DLT trading facility, no capital adequacy and liquidity requirements according to art. 66 and 67 FinMIA apply (art. 58l para. 2 FinMIO). However, small DLT trading facilities are not permitted to grant loans (art. 58o FinMIO).

Small DLT trading facilities also benefit from lower minimal capital requirements, which depend on whether custody, clearing and/or settlement services are being offered (art. 58n FinMIO). This differentiation is also reflected in the minimal capital

[120] *Ordinance of the Federal Council on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology, Explanatory Report on the opening of the Consultation Procedure, p. 18.*

[121] *Dispatch of Swiss Federal Council on DLT legislation dated November 27, 2019, Federal Gazette 2020, p. 311.*

[122] *Ordinance of the Federal Council on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology, Explanatory Report on the opening of the Consultation Procedure, p. 25.*

[123] *The relevant thresholds have been specified by art. 58k FinMIO.*

requirements for regular DLT trading facilities (art. 13 para. 1 let, f and g FinMIO).

Small DLT trading facilities are required to inform their clients on the less strict requirements that it avails of (art. 58m FinMIO).

g) Settlement on DLT Trading Facilities

Depending on the scope of the services offered, the DLT trading facility also settles transactions. A common way of settling securities is delivery versus payment ("DvP"). While in the traditional financial world, DvP involves a cash leg (payment) for the delivery, DLT trading facilities may use digital means of payment (such as cryptocurrencies) for immediate settlement, thus reducing counterparty risks. As regular cryptocurrencies are volatile, effective settlement can be achieved by using so-called stablecoins (e.g., pegged to a fiat currency, thus minimizing the volatility of the stablecoin). Completed proof of concepts using Central Bank Digital Currency (Project Helvetia)[124] or private-sector initiatives issuing stablecoins (such as DCHF)[125] have demonstrated the added value of stablecoins for settlement purposes.

2.2 Anti-Money Laundering Regulations

Centralized trading platforms usually hold tokenized assets for their clients in their own wallets (i.e., they have power of disposal over third-party assets), and maintain an order book as well as bring the supply and demand together by means of automated matching. If the trading platform accepts money or cryptocurrencies from clients and transfers them to other clients, the trading platform is acting as financial intermediary according to art. 2 para. 3 letter b Swiss Anti-Money Laundering Act (AMLA) (in a trilateral relationship).[126]

A payment transaction service as defined in art. 2 para. 3 letter b AMLA exists in particular if the financial intermediary facilitates the transfer of tokenized assets to a third party provided that a permanent business relationship is maintained with the contracting party or the financial intermediary has the power of disposal over the tokenized assets (i.e., the ability to release or stop transactions or control the private keys) and it does not provide the service exclusively to appropriately supervised financial intermediaries (cf. art. 4 para. 1 letter b Swiss Anti-Money Laundering Ordinance [AMLO]). This applies, for example, to trading platforms that are not in possession of the customers' private key, but enable the transfer of virtual currencies by means of a smart contract over which they have control. It also covers wallet providers that have the power of disposal over the private key to which they have access, and which must be used to sign the transaction before it can be successfully executed. With increasingly decentralized models of tokenized asset transfer, the financial intermediary no longer has sole power of disposal over the tokenized assets in all business models. Therefore, the criterion of sole power of disposal may not be appropriate to emerging decentralized business models.[127]

On a global level, the Financial Action Task Force (FATF) has raised concerns about peer-to-peer platform operators – stating that it is now "looking closely at peer-to-peer transactions that involve a Virtual Asset Service Provider (VASP)". According to the FATF, the lack of explicit coverage of peer-to-peer transactions via private or so-called "unhosted wallets" gave cause for concern for certain jurisdictions. It was noted that transfers to an unregulated peer-to-peer platform could present a leak in tracing illicit flows of virtual assets. This may provoke preventive measures, such as a ban on or rejection of the licensing of platforms if they permit unhosted wallet transfers, the introduction of transactional or volume limits on peer-to-peer transactions or the requirement that transactions be carried out using a VASP or financial institutions.[128] The FATF conducted a second 12-month review of countries' Travel Rule frameworks in June 2021, which also assessed the need for further updates to its standards.

[124] https://www.bis.org/publ/othp35.htm

[125] https://www.insights.sygnum.com/post/sygnum-bank-launches-digital-chf-token

[126] *Federal Council report – Legal framework for distributed ledger technology and blockchain in Switzerland, 14 December 2018, p. 138.*

[127] *Ordinance of the Federal Council on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology, Explanatory Report on the opening of the Consultation Procedure, p. 7.*

The Travel Rule originates from Recommendation 16 of the International Standards Combating Money Laundering and the Financing of Terrorism & Proliferation issued in 2012 and updated in June 2019 ("FATF Recommendations"). As for traditional bank transfers, information on the originator and the beneficiary must be transmitted with transfers of tokens (with the exception of transfers from and to unregulated wallet providers).

FINMA issued guidelines to clarify the Swiss approach with respect to the Travel Rule, respectively blockchain-based payments.[129] Art. 10 AMLO-FINMA requires that information about the client and the beneficiary be transmitted with payment orders. The financial intermediary receiving this information needs to check the name of the sender against sanction lists, etc. Unlike the FATF standard, this common practice applies in Switzerland without the exception for unregulated wallets and is therefore more stringent than in other jurisdictions. Where a business is considered to be a VASP, a pragmatic (SWIFT-like second layer protocol) solution needs to be implemented in order to comply with the Travel Rule. Promising approaches in Switzerland consist of second layer messaging protocols which use cryptography to authenticate the participating VASPs (via open-source initiatives, such as OpenVASP[130] or TRISA[131]).

2.3 Data Protection

a) Background

There has been a lot of focus on data protection in recent years. It is clear that in the digital age, the exchange and marketing of personal data are becoming increasingly important. Several new regulations have been adopted to better protect the rights of individuals. In the EU, the General Data Protection Regulation (GDPR) in force since 2018 is expected to be completed by a new ePrivacy Regulation in due course. In Switzerland, following extended discussions, the Parliament adopted a total revision of the Swiss Data Protection Act at the end of 2020.

It is clear that, in the context of transactions, personal data may be stored on the blockchain. This may be the case for DLT securities, for example. If the blockchain is public, the block-chain addresses of persons involved in transactions is visible to anyone who consults the blockchain. Although these public addresses do not directly reveal the identities of the data subjects, public addresses may be classified as personal data if said addresses can be linked to particular data subjects – resulting in the classification as personal data.[132] Hence, it is important to take the data protection regulations into account.

b) Data Protection Compliance for Public Blockchains

Public blockchains often provide higher transparency and security than centralized information transfer systems. However, the unalterable character of the blockchain seems at first glance incompatible with rights arising from a breach of privacy. The question arises as to how the erasure (right to be forgotten) and rectification rights as well as the proscription of data processing can be implemented in a public blockchain. Indeed, no network participant (node) can modify or erase the information recorded on the blockchain. The legal literature proposes several solutions to resolve this issue. For example, the use of chameleon hash functions allows entries in earlier blocks to be changed. The storage of personal data off chain with only a cryptographic – and thus anonymized – representation "on-chain" is another way to solve the problem.

More generally, it may seem difficult to adhere to certain ideas and principles of data protection when using blockchain technology. A central principle in data protection is proportionality, from which the idea of data minimization is derived. The principles of privacy by default and privacy by design are also very important. In this context also, there are a number of solutions to take these principles into account. For example, it is preferable not to record personal data directly on a public blockchain,

[128] *FATF Preparing Regulation for P2P Crypto Trading Platforms. Available at: 12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (fatf-gafi.org), p. 14 et seq.*

[129] *FINMA Guidance 02/2019, Payments on the blockchain, 26 August 2019. Available at: https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg*

[130] *OpenVASP Association: https://openvasp.org*

[131] *Travel Rule Information Sharing Alliance (TRISA): https://trisa.io*

[132] *CMS, The tension between GDPR and the rise of blockchain technologies, January 2019, p. 4. Available at: https://iapp.org/resources/article/the-tension-between-gdpr-and-the-rise-of-blockchain-technologies*

but, if the use case permits it, to record only an identifier that allows access to personal data. The technique of pruning can also be of interest in this context. Certain modern blockchains provide for transaction data that is no longer required to be automatically deleted after a certain time in order to save space. This seems to be compatible with the data minimization principle, according to which personal data must be deleted when the storage is no longer required.

c) Enforcement of Rights and Sanctions

It remains to be seen whether and how the courts will decide these issues. In Switzerland, the individuals protected by data protection regulations have so far made very little use of their rights arising from a breach of privacy, such as the right to erasure (right to be forgotten) or to claim damages. The few judgments on these issues have essentially been initiated by recommendations of the Federal Data Protection and Information Commissioner. In addition, the fines of up to CHF 250 000 under the new Swiss Data Protection Act, well below the fines possible in the EU or in the United States, do not seem to have a strong dissuasive effect.

D. Conclusion and Outlook

The amended Swiss legislation in the field of distributed electronic ledgers improves the legal certainty of tokenization and the transfer of tokens and increases the attractiveness of Switzerland as a place to operate DLT trading facilities which provide for the transfer of tokens.

The Swiss Code of Obligations does not specify the details of the transfer. It is up to the issuer of ledger-based securities to clarify in advance the terms governing a transfer of tokens as well as the conditions justifying an intervention by the system and its operator, respectively, in order to correct the ledger. According to the view expressed by the Swiss government, pure payment tokens and tokens representing rights in rem are not subject to the new legal framework since they do not qualify as ledger-based securities.

The DLT trading facility allows for the participation of individual clients (acting for their own account) to trade DLT securities on a multilateral platform based on non-discretionary rules.

Time will tell how the new DLT legislation will be implemented in practice and whether there are some additional aspects which could require regulation.

V.

Use Cases

Authors:

Harald Baertschi, Patrick Salm, Gino Wirthensohn

Contributors:

Rolf Guenter, Bruno Pasquier, Gian Pfister, Orkan Sahin, Michael Svoboda

A. Selected Examples of Use Cases Related to Capital Market Activities

1. Trading a Swiss Equity Token on Uniswap

The first use case refers to the technical Section IV.B.2.2.2 ("Transaction on a Marketplace"). The question raised is how a ledger-based security can be traded on a decentralized exchange. As mentioned in the respective section, there are equity tokens that are currently traded on Uniswap, one of them being CRES.

While CRES is an ERC20 token, the CRES token contract is governed by a compliance layer.[133] Consequently, the CRES token carrying this additional governance layer to enable voting for registered shareholders is "heavier" and consumes more gas when being transferred.[134] The wrapped ERC20 version on the other hand is a simple ERC20 token and optimized for fast and cheap transferability.[135] This aspect is primarily relevant in the context of secondary market trading on decentralized marketplaces (e.g., Uniswap), since any smart contract interaction on the Ethereum blockchain incurs a cost in the form of gas fees.

a) Price Determination for ETH/wCRES Swap

To better understand what occurs when a user initiates a Uniswap transaction, let us dive into the example of an ETH/wCRES swap[136]: If a user wants to swap 10 ETH for the corresponding amount in wCRES, the user's wallet calls the smart contract managing the liquidity pool containing the ETH/wCRES reserves. The contract consequently checks the available reserves to determine the current price based on the ratio of reserves in the pool. Nevertheless, relying on this price information only makes the trade vulnerable to frontrunning by a bad actor, which could potentially cause an economic loss for the user. This requires the smart contract to have access to information about what a "fair" price for the trade would be. To achieve this, oracles[137] can be used to feed external off-chain data into smart contracts.[138] If the current price is close enough to the "fair" price, the token swap is executed and the 10 ETH are deposited in the liquidity pool, while the corresponding amount in wCRES is with-drawn from the liquidity pool and transferred to the user's wallet, thereby also changing the ratio of the reserves in the liquidity pool.[139]

b) Exercise of Shareholder Rights

Nevertheless, the wCRES holders are not yet be able to exercise their shareholder rights. This is due to the fact that from a legal point of view, the transfer of a share token (not qualifying as a duly established ledger-based security) to a new address does not necessarily transfer the shareholder rights simultaneously. Similar to the transfer of traditional securities, the new shareholders must inform the issuer of the transaction and demand entry into the shareholder registry in order to exercise their shareholder rights.

Such a decoupling of the technical transfer and the transfer of shareholder rights has the benefit of enabling shortterm trading on decentralized market infrastructures as outlined above, while still ensuring that longterm shareholders are incentivized to register accordingly. Consequently, not every token transfer led to a change in the shareholder registry of the issuing company.[140] As described above, it is possible to achieve this separation by using a secondary ERC20 contract to wrap an existing ERC20 contract (CRES), creating a technically different token (wCRES), representing the underlying token.

2. Whitelisting Ruleset Applied to Transfer Restrictions

Another use case with practical importance is how transfer restrictions can be implemented in a smart contract. Besides the use case mentioned in the technical part of T4 – The Trust Element of Transaction (Section IV.B.2.2.3 ["Shares with Restricted Transferability"]), this could be relevant if the issuance of securities is subject to certain regulatory limitations within a specific jurisdiction (cross-border rules). Furthermore, transfer restrictions could arise from an investor protection point of view. We therefore propose implementing a whitelisting framework such as the ERC1404 simple restricted token standard[141] to deal with the various transfer restriction requirements.

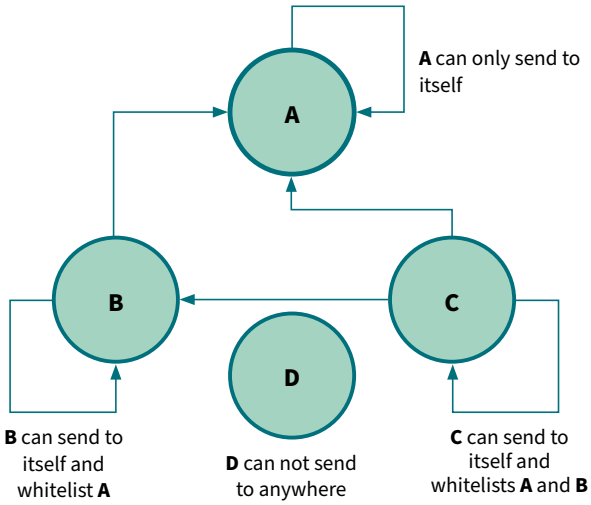
[133] *C-Layer contract: https://github.com/c-layer/contracts*
[134] *https://github.com/crescofin/cres-token*
[135] *https://medium.com/crescofin/creating-defi-equity-tokens-1ca82cbb7dba*
[136] *https://info.uniswap.org/pair/0xf650233ec6ea1c6717ac4f409f09e6c9ebc8c4d2*
[137] *https://www.seba.swiss/research/Oracles-The%20Internet-of-Blockchains*
[138] *See https://uniswap.org/docs/v2/advanced-topics/pricing*
[139] *https://uniswap.org/docs/v2/core-concepts/pools.*
[140] *https://github.com/aktionariat/contracts/blob/master/doc/shares.md*
[141] *ERC-1404 - An open-source standard for security tokens: https://erc1404.org*

Generally, any whitelist can be configured to have multiple outbound whitelists. When a transfer is initiated, the restriction logic will first determine which whitelist the source and destination address belong to. Subsequently, it will determine whether the sending account's whitelist is configured to allow transactions to the destination wallet's whitelist. If the sending account's whitelist is not configured to send to the destination address's whitelist, the transfer will fail.

Moreover, if whitelisting restrictions are enabled, an address that is not whitelisted can neither send, nor receive the token that has these restrictions on its governing smart contract. In addition, there often is a "0" whitelist, which also prevents addresses contained in it from interacting with the token's smart contract. Hence, if either address is on "0" whitelist (restricted from transferring tokens), the transfer will fail.

With regard to cross-border restrictions arising from the investor's jurisdiction, this kind of a whitelist setup would enable country-specific whitelists with corresponding transfer restrictions between them (see illustration below). As mentioned earlier, the ERC1404 token standard, for example, allows for a total of 255 different whitelists, which enables an issuer to maintain an extensive whitelist setup and distinguish between a large number of investor groups / segments (e.g., according to country). In the case of the ERC1404 standard, each address can only be a member of one whitelist at any one point in time. If an admin adds any address to a new whitelist, it will no longer be a member of the previous whitelist (if any has been previously configured).

Analogously, a whitelist setup as described above would allow transfer restrictions to be enforced based on investor type. It is important to note that this approach therefore requires investors to be onboarded and complete KYC verification.



– Whitelist A is only allowed to send to itself.
– Whitelist B is allowed to send to itself and whitelist A.
– Whitelist C is allowed to send to itself and whitelists A and B.
– Whitelist D is not allowed to transfer to any whitelist, including itself.

B. Selected Examples of Use Cases Outside Capital Markets

1. Introduction

We are at the transition from Web2 to Web3. Business models and processes are increasing in significance in business ecosystems and are no longer restricted to bilateral business relationships.

Web2 allowed us to surface the internet with significantly increased web-page functionality, which not only enabled social media applications, but also online marketplaces. With the widespread use of smart phones, Web2 development could be

used anywhere, anytime. The shift from traditional, physical, retail to e-business processes is an important example of this development. The result of this is the de facto power of central entities (e.g., Google, Amazon or Facebook), which manage participants' data and also have the power of disposal over it. Controlling the use of data and identities obviously became a major challenge.

Web3, as the next generation of the internet, is changing the data structure in the background of the internet, allowing us to keep data decentralized in networked systems and not necessarily on centralized database entities. Blockchain technology allows data to no longer be copied uncontrollably, but access to data can be controlled, making it available in a decentralized manner.

Drivers of today's business processes are data. With Web3 applications, technical solutions are made possible in which business ecosystems based on the internet infrastructure can operate on significantly more advanced, automated process flows and transaction models. Blockchain technology is an important cornerstone in this.

Whenever a large number of parties are involved in business processes and fragmented data exists among different participants, blockchain technology enables automated, traceable and secure data transfer within such ecosystems.

2. Car Administration

A specific use case exists in the mobility industry with Cardossier (www.cardossier.ch), where digital access to all data and information on a vehicle is made available on the basis of a permissioned blockchain (Corda). Consequently, among others, insurers, car importers, garage owners and, of course, the owners themselves have access to all data on the lifecycle of the vehicle at any time.

3. Real Estate Management

A comparable project is DIGIM, with which a digital real estate dossier was developed on the same technological basis as part of a research project. In Finland, the real estate market has been digitized using a blockchain-based platform (www.dias.fi).

4. Insurance Industry

The insurance industry is already familiar with fully automated insurance offers that have been realized on public blockchain applications in the field of flight delays or crop failure insurance. Premiums as well as claims payments in the event of loss can be made with cryptocurrencies. The conclusion of an insurance contract as well as claims processes can be fully automated using smart contracts.

5. Healthcare

Healthcare, with its numerous stakeholders around the affected individuals, i.e., the patients, lends itself to blockchain-based technologies. For example, a digital patient record has been explored by MIT graduates (https://medrec.media.mit.edu/). However, blockchain technology would also be an excellent fit for a globally available digital immunization registry.

6. Neighborhood Assistance

A potential application as part of a civil society initiative commenced implementation in 2021. The KISS Foundation is an organization that offers neighborhood assistance in the form of time credits through regionally based KISS cooperatives and associations in communities and regions. Time as a unit of value is made available through neighborly care by a time-giving person to a receiving person. The time-giving person is not compensated in money, but in the form of time credits. In the future, the time-giving person is entitled to spend these credits by using neighborhood assistance as the receiving person. Creating the time credits constitutes a supplementary money-free old-age provision. With the support of the TEZOS Foundation and on the

TEZOS blockchain infrastructure, the project aims to network the decentralized KISS cooperatives to ensure that the recording, storage and transfer of time credits is transparent, secure and traceable at all times. The possibility of using “time tokens” in the concept is being considered.

7. Verification of Diplomas

ODEM, a company based in Zug, carried out an ICO in 2018. ODEM offers various services in the field of education. Its platform provides access to courses and other services. On a broader level, ODEM’s platform connects educational institutions, educators, students, as well as employers.

The service most closely related to the blockchain is to permit educational institutions to issue certificates on the blockchain. The usefulness of the blockchain in this area is recognized. Indeed, this technology prevents the falsification of diplomas. Moreover, storage on the blockchain allows subscribers to have a copy of the diploma that does not depend on the institution which issued the diploma or the educator. Even if these institutions cease their activity, the student can have a copy stored on the blockchain “for life”.

The Odem Ecosystem

The process involves the following steps and outcomes:

1. An “issuer” which can be an independent educator or educational organization, either conducts a program on ODEM or uploads a student roster that are then invited to generate digital credentials on ODEM.

2. The students receive an email to return to the ODEM platform and to “claim” their certificates.

3. Upon activating this “claim”, the ODEM platform initiates a process of creating copies of the certificate. In this context, ODEM has opted for a procedure that takes data protection requirements and principles into account. Three versions of the student’s certificate are stored:

a. A blockchain-based certificate that is issued via a transaction on the Ethereum blockchain and stored on the IPFS (Interplanetary File System) blockchain. This issuance requests the student to select a passphrase to secure this certificate on IPFS and only the student then has access to this digital credential via this passphrase.

b. A server-based copy that is stored on the student’s ODEM profile for viewing by employers and institutes of higher education for consideration for employment and enrollment. This version acts as a receipt for proof of the issuance of the original certificate on Ethereum and in IPFS. This version is linked to the transaction on the Ethereum blockchain to ensure that the certificate is not falsified and corresponds to a transaction that has effectively taken place on the blockchain. The students can turn off the sharing of this version of the certificate as well as request their profile at any time, after which the certificate will be removed from the ODEM platform.

c. A downloadable copy of the digital credential that the students can store wherever they like. ODEM does not have access to this version.

Since it relates to the right to be forgotten in accordance with the FADP and GDPR regulations, ODEM has a responsibility to remove its copy (step b) above) from its server along with all account information on the student. With step a) above, the student is the full owner of the blockchain-based certificate and therefore ODEM is not responsible nor liable (nor does it even have the ability) to remove this certificate from the blockchain. With step c) above, this copy of the certificate is also owned exclusively by the student and ODEM is not responsible nor liable for deleting this material.

VI. Final Words

The new legislation on the issuance of ledger-based securities is appropriate and suitable to achieve the goal of increased legal certainty for DLT-based transactions and to increase the attractiveness of Switzerland as a leading global hub for digital innovation. However, it must also be stated that the use of DLT places high demands on all parties involved. From the issuer's point of view, in particular, careful configuration of the smart contracts used is required in order to bring the characteristics of the shares issued as ledger-based securities into line with the requirements of Swiss company law. From the shareholder's point of view, the risk of loss or theft of the private key and the difficulties associated with such a case in regaining legal power of disposal places increased demands on self-responsibility in dealing with electronic data and passwords.

In this Whitepaper we have defined the technical and legal framework to establish a secure, interoperable and reliable DLT infrastructure with the ultimate goal of exploiting the full potential of this new technology.

The center of focus regarding T1, the trust in legally binding information, is in the synchronization of on- and off-chain information through the programmed smart contract. Only by effectively linking off-chain documents, such as the Registration Agreement to the respective DLT information, can the potential of this new technology be used efficiently in practice.

As the Whitepaper outlines, trust and scale can only be achieved provided there is (inter-) operability between protocols (T2). Ten principles have been defined, which all DLT interfaces should adhere to in order to achieve effective, secure and flawless communication. As the examples demonstrate, alignment within a protocol and across protocols should be guided by a common overarching objective and not by particularism.

There are different models in the custody of ledger-based securities: self-custody and third-party custody. In T3, this Whitepaper provides an overview of the main accounting paradigms, outlines the existing contractual relationships and discusses the applicable regulatory implications in this context.

The Swiss Code of Obligations does not specify the details with regard to the transfer (T4) of ledger-based securities. It is up to the issuer of ledger-based securities to clarify in advance the terms governing a transfer of tokens, as well as the circumstances justifying an intervention by the system and/or its operator in order to correct the ledger. According to the view expressed by the Swiss government, pure payment tokens and tokens representing rights in rem are not subject to the new legal framework since they do not qualify as ledger-based securities.

Time will tell which use cases will prevail, how the new DLT legislation will be implemented in practice and whether there are some additional aspects requiring further regulation.